PROTECCION DE DATOS EN LAS CORPORACIONES LOCALES

Derecho Administrativo y Compliance

Colegio Oficial de de Secretarios, Interventores y Tesoreros de la Administración Local de Madrid.

04-11-2025

INDICE

- Conceptos Fundamentales de Protección de Datos Personales
- Protección de Datos e Interacción con otras normas (Transparencia, Procedimiento Administrativo Común, ENS)
- Novedades Legislativas (RGPD)
- Seguridad en el tratamiento de los datos personales
- Novedades Legislativas
  - Gobernanza del Dato
  - Regulación europea sobre la IA
- Nuevos servicios municipales
  - Oficina del Dato
  - Centro de Excelencia de la IA
- Calidad y exactitud en el dato. Oficina del Dato
- Impacto de la nueva regulación europea sobre la IA en la protección de datos personales
- Nuevos Servicios municipales basados en IA
- Panorama actual de la IA

Conceptos Fundamentales de la Protección de Datos Personales

1. Ámbito de aplicación
- **LOPD (1999):** Solo aplicaba en España.
- **RGPD (2016):** Aplicación **europea y extraterritorial**: afecta a cualquier organización que trate datos de ciudadanos europeos, incluso fuera de la UE.
- **LOPDGDD (2018):** Adapta la normativa española al RGPD e incorpora derechos digitales.

2. Consentimiento
- **LOPD: Permitía consentimiento tácito (por ejemplo, seguir navegando implicaba aceptación).**
- **RGPD: Exige consentimiento expreso, libre, informado e inequívoco (acción clara como marcar una casilla).**
- **LOPDGDD: Mantiene** el consentimiento expreso y regula excepciones (p.ej., relaciones laborales o interés legítimo).

3. Nuevos derechos
- **LOPD:** Derechos ARCO (Acceso, Rectificación, Cancelación, Oposición).
- **RGPD:** Amplía derechos: **Acceso, Rectificación, Supresión (Olvido), Limitación, Portabilidad, Oposición**.
- **LOPDGDD:** Añade **derechos digitales** (neutralidad de Internet, desconexión digital, protección de menores en redes).

4. Delegado de Protección de Datos (DPO)
- **LOPD:** No existía esta figura.
- **RGPD:** Introduce el DPO como obligatorio en ciertos casos (administraciones públicas, tratamientos a gran escala).
- **LOPDGDD:** Detalla requisitos y sanciones por no designarlo cuando es obligatorio.

5. Principios y transparencia
- **RGPD:** Refuerza el principio de **transparencia**: información clara y comprensible sobre el tratamiento.
- **LOPDGDD:** Desarrolla este principio en España y regula brechas de seguridad y canales de denuncia.

6. Régimen sancionador
- **LOPD:** Sanciones más bajas.
- **RGPD:** Sanciones mucho más severas (hasta **20 millones € o el 4% del volumen de negocio global**).
- **LOPDGDD:** Ajusta el régimen sancionador en España conforme al RGPD.

📌 **Aspecto clave:** La LOPDGDD no sustituye al RGPD, sino que lo **complementa** en España, regulando aspectos específicos como derechos digitales y tratamiento en el ámbito laboral.

Conceptos Fundamentales de la Protección de Datos Personales

LORTAD (1992) → LOPD (1999) → RGPD (2016) → LOPDGDD (2018)

LORTAD (1992)
Fue la **primera ley española** que reguló la protección de datos personales.
Se centraba en el **tratamiento** informático de datos.

LOPD (1999)
Amplió el ámbito a **cualquier tratamiento**, no solo automatizado.
Introdujo los **derechos ARCO** (Acceso, Rectificación, Cancelación, Oposición).
Creó la obligación de **inscribir ficheros en la AEPD**.

El RGPD (2016)
Enfoque hacia responsabilidad proactiva yconsentimiento explícit o.

LOPDGDD (2018)
La LOPDGDD adapta el RGPD en España
e incorpora derechos digitales modernos.

Transformación en gestión de datos
Se pasó decontrol externo a cumplimiento interno y responsabilidad activa en datos personales.

Conceptos Fundamentales de la Protección de Datos Personales

1. Derecho a la neutralidad de Internet
Garantiza que los proveedores de servicios no discriminen el tráfico y mantengan un acceso abierto y no sesgado.
2. Derecho de acceso universal a Internet
Reconoce el acceso a Internet como esencial para la ciudadanía, promoviendo su disponibilidad y asequibilidad.
3. Derecho a la seguridad digital
Protección frente a ciberataques y obligación de adoptar medidas para garantizar la integridad de los sistemas.
4. Derecho a la educación digital
Impulsa la formación en competencias digitales y uso seguro de la tecnología, especialmente para menores.
5. Derecho a la protección de menores en Internet
Medidas para evitar la exposición a contenidos inapropiados y garantizar su privacidad en entornos digitales.
6. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral
Regula el uso de dispositivos por parte del empleador y protege la privacidad del trabajador.
7. Derecho a la desconexión digital en el ámbito laboral
Permite al trabajador no atender comunicaciones fuera del horario laboral.
8. Derecho a la intimidad frente al uso de sistemas de videovigilancia y grabación de sonidos
Prohíbe grabaciones en espacios privados y regula su uso en el trabajo.
9. Derecho a la intimidad frente a sistemas de geolocalización
Protege la localización del trabajador y limita su uso a fines laborales justificados.
10. Derecho al olvido en búsquedas de Internet y redes sociales
Permite solicitar la eliminación de enlaces o contenidos que afecten a la reputación o privacidad.
11. Derecho de portabilidad en servicios digitales
Facilita la transferencia de datos entre plataformas.
12. Derecho al testamento digital
Permite a herederos gestionar perfiles y contenidos digitales tras el fallecimiento

Conceptos Fundamentales de la Protección de Datos Personales

Testamento Digital …

Sucesión en entornos digitales se señala que este concepto es **limitado** y que sería más adecuado hablar de:

> **“Gestión post mortem de la identidad digital”**
> **“Administración del legado digital”**
> **“Derecho sobre el patrimonio digital”**

Estas expresiones reflejan mejor que no se trata solo de un testamento clásico, sino de **regular el destino de datos, perfiles y contenidos digitales tras el fallecimiento**, incluyendo acceso, conservación o supresión. [revistas.um.es], [fundacionareces.es]

Contexto normativo:

La **LOPDGDD (art. 3)** reconoce el derecho de herederos o personas designadas para gestionar cuentas y contenidos digitales del fallecido, lo que popularmente se llama “testamento digital”, pero jurídicamente se orienta hacia **gestión del legado digital**.

Conceptos Fundamentales de la Protección de Datos Personales

Facebook

Permite convertir la cuenta en **“Perfil conmemorativo”**:

Aparece la palabra *“En memoria de”* junto al nombre.
Amigos y familiares pueden publicar recuerdos.
No se puede iniciar sesión ni modificar contenido.

Se puede designar un **contacto legado** para gestionar:

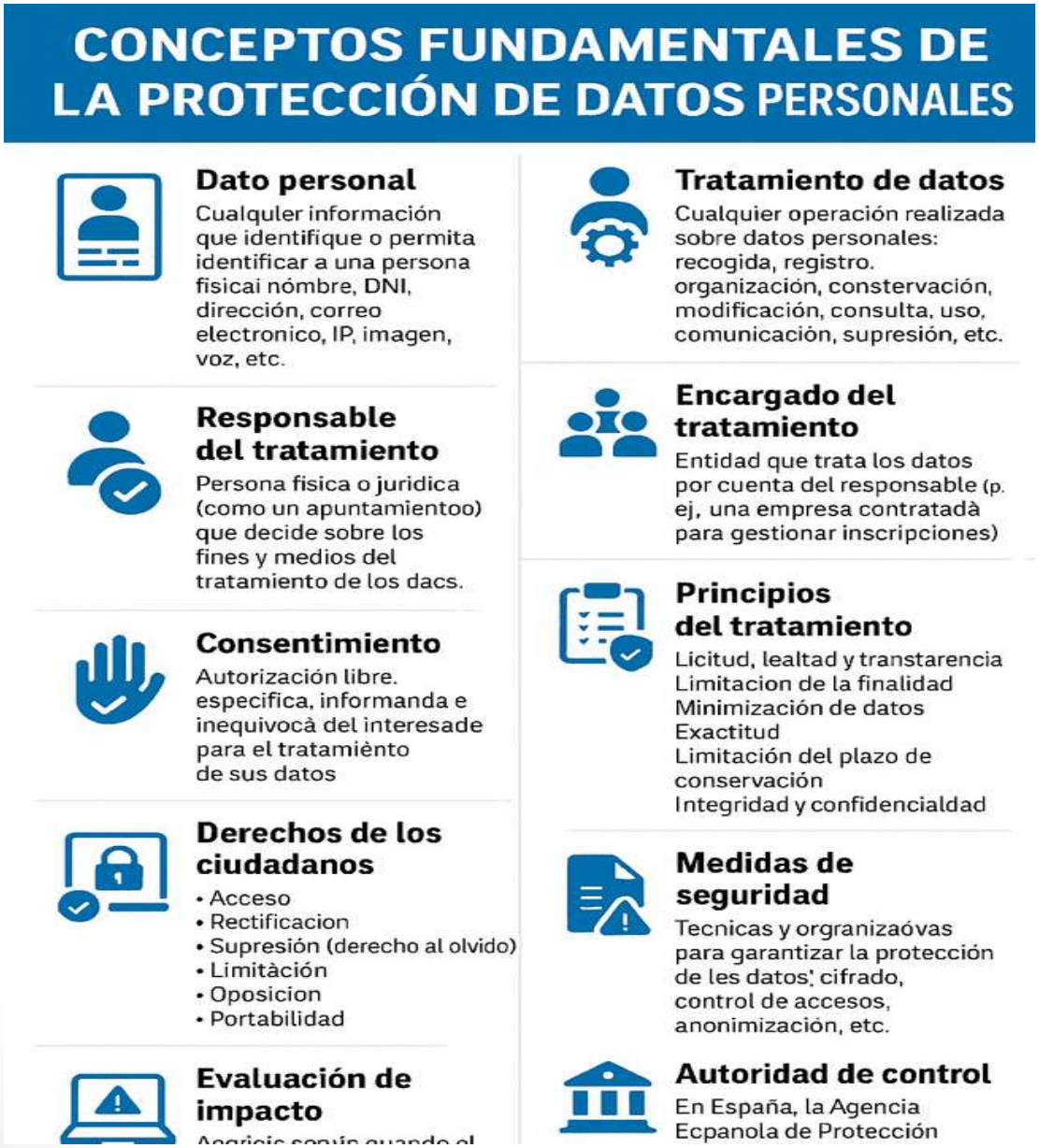
Foto de perfil.
Publicaciones de homenaje.
Descargar contenido (si el fallecido lo autorizó).
No se aceptan solicitudes de amistad

Instagram

Permite **memorializar la cuenta**:

Se mantiene el contenido, pero no se puede iniciar sesión.
No se eliminan publicaciones, pero se bloquea la edición.
Se requiere prueba del fallecimiento (certificado).

Conceptos Fundamentales de la Protección de Datos Personales



Conceptos Fundamentales de la Protección de Datos Personales

- **Dato personal**

  Cualquier información que identifique o pueda identificar a una persona física: nombre, DNI, dirección, correo electrónico, IP, imagen, voz, IMEI, etc.

- **Tratamiento de datos**

  Cualquier operación realizada sobre datos personales: recogida, registro, organización, conservación, modificación, consulta, uso, comunicación, supresión, etc.

- **Responsable del tratamiento**

  Persona física o jurídica (como un ayuntamiento) que decide sobre los fines y medios del tratamiento de los datos.

- **Encargado del tratamiento**

  Entidad que trata los datos por cuenta del responsable (por ejemplo, una empresa contratada para gestionar inscripciones).

Conceptos Fundamentales de la Protección de Datos Personales

- **Consentimiento**
  Autorización libre, específica, informada e inequívoca del interesado para el tratamiento de sus datos.

Supuestos en los que NO se requiere consentimiento

- **Ejecución de un contrato**
  Cuando el tratamiento es necesario para cumplir un contrato en el que el interesado es parte o para aplicar medidas precontractuales (por ejemplo, gestionar una póliza o un contrato laboral). [rgpd.com]

- **Cumplimiento de una obligación legal**
  Si una ley obliga al responsable a tratar los datos (por ejemplo, obligaciones fiscales, Seguridad Social, registro de huéspedes en hoteles). [aepd.es]

Base legal

- **Protección de intereses vitales**
  Cuando el tratamiento es necesario para proteger la vida o integridad del interesado o de otra persona (por ejemplo, en emergencias médicas).

- **Misión en interés público o ejercicio de poderes públicos**
  Cuando el tratamiento se realiza para cumplir una función pública (por ejemplo, elaboración de estadísticas oficiales por el INE).

Base legal

- **Interés legítimo del responsable o de un tercero**
  Siempre que este interés no prevalezca sobre los derechos y libertades del interesado (por ejemplo, prevención del fraude, seguridad de redes).

no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

Conceptos Fundamentales de la Protección de Datos Personales

Derechos de los ciudadanos

- **Acceso:** saber qué datos se tienen y cómo se usan. Ejemplo: Un vecino solicita al ayuntamiento conocer qué datos personales se han recogido en el padrón municipal y cómo se están utilizando.
- **Rectificación:** corregir datos incorrectos. *Ejemplo*: Una persona detecta que su dirección en el padrón está mal escrita y pide corregirla.
- **Supresión (derecho al olvido):** eliminar datos cuando ya no sean necesarios. Derecho de Supresión (Derecho al Olvido). *Ejemplo*: Un ciudadano solicita eliminar sus datos de una lista de difusión de actividades culturales porque ya no quiere recibir información.
- **Limitación:** restringir el uso de los datos. *Ejemplo*: Un vecino pide que sus datos no se usen para fines estadísticos mientras se resuelve una reclamación sobre su inscripción en un curso municipal.
- **Oposición:** negarse al tratamiento en ciertos casos. *Ejemplo*: Un ciudadano se opone a que su imagen aparezca en fotografías publicadas en redes sociales del ayuntamiento tras participar en un evento.
- **Portabilidad:** recibir los datos en formato estructurado. Ejemplo: Una persona solicita que los datos de su inscripción en actividades deportivas municipales se transfieran a otra entidad pública que gestiona instalaciones deportivas. Las AAPP **no están obligadas a atender la portabilidad en la mayoría de sus tratamientos**, porque normalmente actúan en el marco de **interés público** o **poderes públicos**. Solo sería aplicable en casos donde traten datos **por consentimiento o contrato**, como servicios voluntarios de actividades deportivas o culturales.

Conceptos Fundamentales de la Protección de Datos Personales

Excepciones y limitaciones al Derecho de Acceso

Solicitudes manifiestamente infundadas o excesivas

Por ejemplo, cuando son repetitivas sin justificación.

El responsable puede negarse a actuar o cobrar un canon proporcional a los costes administrativos. [aepd.es]

Cuando afecte negativamente a derechos y libertades de terceros

Si al facilitar la información se vulneran derechos de otras personas (p. ej., revelar datos personales de terceros). [aepd.es]

Cuando exista una obligación legal que lo limite

Normas que impidan revelar cierta información (p. ej., datos protegidos por secreto profesional, seguridad pública). [aepd.es]

Cuando el acceso pueda obstaculizar investigaciones o procedimientos judiciales

Por ejemplo, en procesos penales o inspecciones administrativas en curso. [aepd.es]

Conceptos Fundamentales de la Protección de Datos Personales

Excepciones y limitaciones al Derecho de Rectificación

Solicitudes manifiestamente infundadas o excesivas

Por ejemplo, cuando son repetitivas sin justificación.

El responsable puede negarse a actuar o cobrar un canon proporcional a los costes administrativos. [aepd.es]

Puede limitarse el tratamiento hasta la verificación del dato

No procede si afecta a derechos de terceros o a obligaciones legales

Conceptos Fundamentales de la Protección de Datos Personales

Excepciones y limitaciones al Derecho al Olvido

Ejercicio del derecho a la libertad de expresión e información
Por ejemplo, publicaciones en medios de comunicación amparadas por este derecho. [aepd.es]

Cumplimiento de una obligación legal
Padrón municipal, registros tributarios). **[aepd.es]**

Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos
Por ejemplo, actuaciones administrativas o judiciales. [aepd.es]

Razones de interés público en el ámbito de la salud pública
Como tratamientos relacionados con epidemias o campañas sanitarias. [aepd.es]

Fines de archivo en interés público, investigación científica o histórica, o fines estadísticos
Siempre que la supresión pueda impedir u obstaculizar gravemente esos objetivos. [aepd.es]

Formulación, ejercicio o defensa de reclamaciones
Si los datos son necesarios para procedimientos judiciales o administrativo

No procede si afecta a derechos de terceros o a obligaciones legales

Conceptos Fundamentales de la Protección de Datos Personales

- **Derecho de acceso / Derecho de rectificación / Derecho de oposición / Derecho de supresión ("al olvido") /Derecho a la limitación del tratamiento / Derecho a la portabilidad / Derecho a no ser objeto de decisiones individualizadas**
  - Ante solicitudes manifiestamente infundadas o excesivas: canon / negarse a actuar
  - En función a la complejidad y número de solicitudes: de 1 mes, se puede prorrogar a dos meses más.
  - Si no se da curso a la solicitud, se informará y a más tardar en un mes, de las razones y de la posibilidad de reclamar ante una Autoridad de Control
  - Puede que el encargado atienda la solicitud por cuenta del responsable

El **derecho a no ser objeto de decisiones individualizadas** está regulado en el **artículo 22 del RGPD** y significa que **una persona no puede ser sometida a una decisión basada únicamente en el tratamiento automatizado de sus datos**, incluida la **elaboración de perfiles**, cuando esa decisión produzca **efectos jurídicos** sobre ella o la afecte significativamente de forma similar.

formulario-derecho-de-oposicion-decisiones-automatizadas.pdf

Conceptos Fundamentales de la Protección de Datos Personales

Derecho a no ser objeto de decisiones individualizadas

Salvaguardas obligatorias GDPR

Intervención humana significativa protege derechos del interesado en decisiones automatizadas.

Medidas técnicas y organizativas

Auditorías, anonimización y supervisión aseguran seguridad y equidad en procesos automáticos.

Ejemplos prácticos locales

Asignación automática de ayudas y gestión de citas médicas mediante algoritmos precisos.

Derecho a revisión humana

Ciudadanos pueden solicitar revisión si la decisión automatizada les afecta negativamente.

Interacción con otras normas (Transparencia, Procedimiento Administrativo Común, ENS)

- **Diferenciar el derecho de acceso RGPD del derecho de acceso a la información pública** que regula la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno.

- **Diferenciar el derecho de acceso RGPD del derecho de acceso a la documentación en un procedimiento administrativo** cuando se ostenta la condición de interesado, regulado por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

- **Datos de Menores**

  Art. 8 RGPD. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de **servicios de la sociedad de la información**, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga **como mínimo 16 años**. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. **AEPD. Entre 14 y 18 años podrán otorgar el consentimiento**. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela. Salvo que una ley indique lo contrario, nunca será con menos de 13 años. >> consentimiento AEPD >> FORMA

  RGPD (Reglamento General de Protección de Datos)

  Considera a los menores como un grupo que requiere protección específica (Considerando 38 RGPD).
  Establece en el artículo 8 que: La edad mínima para que un menor pueda dar consentimiento válido es **16 años.**
  Los Estados miembros pueden reducirla, pero **nunca por debajo de 13 años**. [ineaf.es]

  LOPDGDD (Ley Orgánica 3/2018 en España)

  Fija la **edad mínima en 14 años** para que el consentimiento sea válido sin intervención de padres o tutores (art. 7 LOPDGDD). [aepd.es]. En caso contrario, el consentimiento debe otorgarlo el titular de la patria potestad o tutela.
  Además:
  La información dirigida a menores debe ser clara y comprensible.
  Se prohíbe recabar datos que revelen información sobre la familia del menor sin autorización expresa. [ineaf.es]

  Aspecto clave:

  Aunque los datos de menores no son considerados "sensibles" por el RGPD, se les otorga **protección reforzada**, especialmente en:

  - Servicios de la sociedad de la información (apps, redes sociales).
  - Marketing y elaboración de perfiles.
  - Publicación de imágenes en internet

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

- **Datos de Menores**

Sharenting (publicar fotos de hijos en redes)

La AEPD alerta sobre riesgos: ciberbullying, grooming, pedofilia y uso indebido de imágenes mediante IA.

Recomienda evitar publicar imágenes o, si se hace:

Configurar la privacidad de la cuenta.

No mostrar la cara ni elementos identificativos (uniformes, ubicación).

No compartir localización ni datos sensibles.

[newtral.es]

Conflictos entre progenitores

Si uno se opone, no se puede publicar.

Puede resolverse judicialmente.

El bienestar del menor y sus derechos (honor, intimidac imagen) prevalecen. [incibe.es]

Sanciones por incumplimiento

Ejemplo: multa de 10.000 € a un local por publicar fotos de menores en Instagram sin consentimiento.

Incluso usar emoticonos para cubrir parcialmente el rostro puede ser sancionado si el menor es reconocible.

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

✓ Datos del **canal para menores y sus familias**
Correo electrónico: canaljoven@aepd.es
Teléfono gratuito: 900 293 621
WhatsApp: 616 172 204
Web de recursos: Tú decides en Internet
Estas vías están abiertas para menores, padres/madres y personal docente. [aepd.es], [tudecidese...nternet.es]

✓ Qué se puede denunciar
Publicación de imágenes de menores sin consentimiento.
Uso indebido de datos en redes sociales o plataformas educativas.
Incumplimiento del ejercicio de derechos (acceso, rectificación, supresión, etc.).
Brechas de seguridad que afecten a menores.
[proteccion...s-lopd.com]

✓ Cómo hacerlo
Preferentemente a través de la Sede Electrónica de la AEPD:
Formulario de reclamación
Se pueden presentar denuncias anónimas o como representante legal del menor.
Plazo de respuesta: máximo 3 meses para admitir o inadmitir la reclamación.

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

[Sede Electrónica - Agencia Española de Protección de Datos - Comunicación]

[Eliminar fotos y vídeos de internet | AEPD]

https://www.aepd.es/canalprioritario

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

PROTECCIÓN DE DATOS EN VACACIONES

Disfruta de tus vacaciones y protege tus datos personales

aepd agencia española protección datos

Piensa dos veces antes de compartir

La información que publiques te puede comprometer. Piensa siempre en quién puede ver lo que compartes.

Si publicas información de otras personas, como sus fotos, **procura que sea en modo no abierto a todo el mundo y recuerda que te gustaría que a ti te preguntasen** con antelación.

Evita dar información sobre tu **localización**. Estos datos pueden ser utilizados para saber cuándo no estás en casa.

Los códigos de billetes y tarjetas de embarque contienen datos personales y del viaje. **No compartas fotos de estos documentos.**

Desconfía de las WiFis abiertas o públicas

Cuidado con el intercambio de **información sensible**, privada o confidencial.

Antes de utilizar tu servicio de banca online o de hacer compras utilizando estas redes, **piénsalo**.

No accedas a tus cuentas protegidas **mediante tu usuario y clave** si no es estrictamente necesario.

Cuidado cuando uses ordenadores compartidos

Utiliza la opción de **ventana de incógnito** del navegador.

No guardes tus contraseñas en el gestor del navegador o del equipo.

Cuando termines, **cierra todas las sesiones** que hayas abierto.

Adelántate al robo o pérdida de tus dispositivos y los datos que contienen

Utiliza un **sistema de patrón o clave** para desbloquearlos.

Haz una **copia de seguridad** de la información que contienen tus dispositivos.

¡Disfruta de las vacaciones!

Si te pasas el día pegado a tu teléfono, en Internet o mirando las redes sociales, te perderás momentos irrepetibles.

twitter.com/AEPD_es

www.aepd.es

Más información

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

RESPONSABILIDAD DE LOS Y LAS MENORES (Y DE SUS PADRES Y MADRES) POR LOS ACTOS COMETIDOS EN INTERNET

agencia española protección datos

Acosar a otras personas, intimidarlas, discriminarlas, expresar una burla o publicar contenidos sensibles a través de redes sociales y otros servicios de internet puede vulnerar sus derechos e ir contra la ley. Puede constituir **una infracción administrativa e incluso un delito**.

Padres, madres o tutores legales pueden llegar a tener que responder económicamente por las infracciones administrativas y conductas delictivas de sus hijos e hijas menores de edad, así como por los daños y perjuicios materiales y morales causados.

Supervisar y poner límites

Para evitar estas consecuencias puedes ayudarte de un software de control parental, pero no te relajes, en tu mano está la mejor supervisión. Te recomendamos acordar con tus hijos e hijas los filtros, restricciones y tiempos.

Quien difunda ilegítimamente **contenidos o información sensible de otras personas sin su consentimiento** puede incurrir en distintos tipos de responsabilidades:

Responsabilidad administrativa

La publicación sin consentimiento de información sensible de una persona (imágenes, audios, videos o información de carácter sexual o violenta que permita identificarla) a través de Internet supone una infracción de la normativa de protección de datos que, sin perjuicio de que se denuncie ante el **Canal Prioritario** de la Agencia para solicitar la retirada urgente de esos contenidos, puede terminar en una sanción económica a quien la haya publicado o contribuido a la difusión.

De la sanción económica por infracción a la normativa de protección de datos impuesta a menores de edad responden solidariamente sus padres, madres o tutores. Ejemplo de procedimiento sancionador **en el que la multa impuesta tiene que ser abonada por los padres al tratarse de un menor.**

Es una infracción tanto obtener los datos ilícitamente (imágenes, videos, audios u otros contenidos) como quien, sin consentimiento de la persona afectada, los ha difundido o publicado en Internet.

Responsabilidad civil

Los daños y perjuicios materiales y morales causados a terceros por menores de edad como consecuencia de estas conductas (delictivas y no delictivas) dan lugar a responsabilidad civil patrimonial, de la que se hacen cargo los padres o tutores.

Responsabilidad penal

Los menores de edad mayores de 14 años también responden* por los delitos tipificados en el Código Penal como el acoso, las amenazas o la difusión o el reenvío de imágenes que menoscaben gravemente la intimidad de una persona, aunque se hubieran obtenido con su permiso, aplicables en casos de sexting, ciberacoso o ciberbullying.

Las medidas en estos casos dependen de sus circunstancias: desarrollo evolutivo, antecedentes, etc., y normalmente se impone la realización de servicios en beneficio de la comunidad o tareas socio educativas, pudiendo llegar a la libertad vigilada e incluso a la privación de libertad (internamiento en centros o permanencia de fin de semana).

*Ley Orgánica reguladora de la responsabilidad penal del menor

Responsabilidad disciplinaria en el ámbito educativo

Estas conductas dan lugar a responsabilidad disciplinaria cuando se producen en los centros escolares (acoso, intimidación, humillación, ofensas graves, discriminación o violencia a otros alumnos o profesores realizadas a través de Internet). Se pueden imponer medidas correctivas que van desde la amonestación verbal o el apercibimiento por escrito a la suspensión del derecho de asistencia al centro o la expulsión del alumno o alumna.

AEPD_es · www.aepd.es · AEPD · @aepd.es

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

Actuación del coordinador/a de bienestar y protección del alumnado

ante la publicación de contenidos sexuales o violentos en internet

aepd agencia española protección datos

www.aepd.es @AEPD_es

La **Ley Orgánica 8/2021 de protección integral a la infancia y la adolescencia frente a la violencia** (LOPIVI) recoge que **todos los centros educativos donde cursen estudios personas menores de edad deberán tener un Coordinador o Coordinadora de bienestar y protección del alumnado**, que actuará bajo la supervisión de la persona que ostente la dirección o titularidad del centro. (**Artículo 35.1**)

Función del Coordinador o Coordinadora de bienestar y protección de centros educativos, entre otras:

Promover, en aquellas **situaciones que puedan implicar un tratamiento ilícito de datos de carácter personal de las personas menores de edad, la comunicación inmediata por parte del centro educativo** a las *Agencias de Protección de Datos*. (**art. 35.2. j**)

La AEPD dispone de un **Canal prioritario general** para comunicar la publicación no autorizada en internet de contenido sexual o violento (fotografías, vídeos, audios o información que identifique a personas) y solicitar su retirada de forma urgente.

El centro educativo puede denunciar la publicación en internet de estos contenidos utilizando un **certificado electrónico de representante de persona jurídica**.

Por razones técnicas, este Canal no es operativo frente a servicios de mensajería privada (WhatsApp, Telegram, Snapchat, Messenger...). En estos casos **se pueden utilizar las herramientas ofrecidas por estos servicios para bloquear o reportar usuarios**.

En cualquier caso, si la AEPD confirmara la autoría de una difusión no autorizada de datos personales, podría iniciar actuaciones para determinar una posible responsabilidad administrativa en materia de protección de datos e imponer una sanción económica.

Información general que se ha de aportar en la comunicación al Canal prioritario de la AEPD:

- Describir con el mayor detalle posible las circunstancias en las que se ha producido la publicación del contenido indicando, en su caso, que la publicación afecta a menores de edad matriculados en el centro educativo.
- Identificar al alumno/a cuyos datos se publican en abierto y además indicar que esta comunicación se realiza desde la Dirección del centro o como coordinador/a de bienestar y protección o director/a del centro educativo.
- Identificar claramente el contenido del que se solicita la retirada (vídeos, fotografías, audios, información) y el perfil social a través del que, en su caso, se está publicando, incluyendo las distintas direcciones web de acceso (http://...).
- Especificar si se ha denunciado la publicación ante Policía, Guardia Civil o Fiscalía, acompañando copia de la denuncia.
- Especificar si se ha **solicitado previamente la retirada a las redes sociales o prestadores de servicios**, incluyendo en tal caso copia de la solicitud y de la respuesta obtenida.

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

https://www.aepd.es/guias-y-herramientas/infografias?page=1

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

- **Medidas de Seguridad**
  El nuevo RGPD no distingue entre los niveles de los ficheros, sino que especifica que se apliquen medidas técnicas y organizativas de seguridad 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 los riesgos para los derechos y libertades de las personas físicas. (Artículo 25 Protección de datos desde el **diseño y por defecto**). **Bajo el principio de responsabilidad proactiva (Artículo 5.2), todos los servicios y sistemas implantados deberían conllevarlos y documentarse.**

- **Evaluación de impacto del tratamiento de datos personales**
  El RGPD establece realizar una evaluación de impacto en organizaciones que realicen tratamientos de datos de alto riesgo para los derechos y libertades de las personas físicas (víctimas, antecedentes, salud, investigaciones, **servicios sociales, actuaciones sanitarias** de emergencia, etc.)

  Análisis de riesgos: Identificar amenazas y vulnerabilidades que puedan afectar la seguridad y privacidad.
  Resultado: Medidas preventivas y correctivas (cifrado, control de accesos, anonimización).

  Evaluación de impacto (EIPD): cuando el tratamiento puede implicar **alto riesgo para los derechos y libertades** (art. 35 RGPD).
  Resultado: Descripción del tratamiento y finalidad, Evaluación de necesidad y proporcionalidad.
  Análisis de riesgos para los interesados, Medidas para mitigar riesgos.

Diferencia clave:

El **análisis de riesgos** es general y aplica a cualquier tratamiento.
La **EIPD** es más profunda y obligatoria en casos de alto riesgo.

Evalúa-Riesgo RGPD v2 | AEPD

Guía para una Evaluación de Impacto en la Protección de Datos Personales

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

- **Procedimiento de comunicación de una violación de Seguridad de DP (incluida la Autoridad).**
  Todos los usuarios incluido el responsable deben contar con una herramienta para notificar las violaciones de seguridad de los datos. Un problema de protección de datos es un incidente de seguridad, pero no todos los incidentes de seguridad son problemas de protección de datos. Hta de Soporte al CAU

Violación de la Seguridad es cualquier incidente que provoque:
Pérdida, **alteración**, **destrucción**, **acceso no autorizado** o **divulgación** de datos personales. Ejemplo: robo de dispositivos, ciberataque, envío erróneo de datos.

Obligación de comunicar

- A la AEPD:

- En un plazo máximo de **72 horas** desde que se tiene conocimiento.
- A través de la **Sede Electrónica de la AEPD**:
  Formulario de notificación de brechas

- A los afectados:

- Cuando la brecha suponga **alto riesgo para sus derechos y libertades**.
- Debe ser **clara y sencilla**, indicando:
  - Naturaleza de la brecha.
  - Datos afectados.
  - Medidas adoptadas.
  - Contacto del DPO.

Contenido mínimo de la comunicación

1. Naturaleza de la violación.
2. Categorías y número aproximado de afectados.
3. Consecuencias probables.
4. Medidas adoptadas o propuestas.
5. Datos de contacto del Delegado de Protección de Datos (DPO).

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

- **Principio de Transparencia (5.1.a)** “Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado”.

- **Minimización de datos (5.1.c)** "Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”.

- **Nuevos derechos**
  - Derecho a la transparencia de la información, (art. 12)
  - Derecho de supresión (derecho al olvido), (art. 17)
  - Derecho de limitación, (art. 18) inexactitud del dato
  - Derecho de portabilidad, (art. 20)


Artículo 18

Derecho a la limitación del tratamiento

- **Ampliación del deber de información**
  - explicar la base legal para el tratamiento de los datos
  - se debe informar acerca del periodo de conservación
  - se debe informar acerca de la posibilidad de hacer reclamaciones
  - se debe informar de los demás derechos que incorpora el nuevo reglamento.

- **Obtención del consentimiento para el tratamiento de datos**
  - el nuevo RGPD indica que para poder considerar que el consentimiento es inequívoco, deberá existir una declaración expresa del interesado que manifieste su conformidad.

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

Contenido mínimo del RAT

- **Para responsables:**
  - Nombre y datos de contacto del responsable y del DPO.
  - Finalidad del tratamiento.
  - Categorías de interesados y de datos personales.
  - Destinatarios (incluidas transferencias internacionales).
  - Plazos previstos para la supresión.
  - Medidas técnicas y organizativas de seguridad.
- **Para encargados:**
  - Nombre y datos del responsable.
  - Categorías de tratamientos realizados por cuenta del responsable.

Características

- **No se envía a la AEPD, pero debe estar disponible para inspección.**
- **Es obligatorio para:**
  - Administraciones públicas.
  - Empresas con más de 250 empleados.
  - Tratamientos que no sean ocasionales o incluyan datos sensibles.

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

Interés público como base legal

La última base legal que queda por analizar es el supuesto de la letra e) del artículo 6 apartado 1 del RGPD que legitima el tratamiento de datos personales cuando «es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos».

Se prevén dos situaciones:

1ª.- Tratamientos de datos en el ejercicio de una potestad de derecho público, que exclusivamente puede llevarse a cabo por parte de una Administración pública, en el marco de sus competencias, legalmente atribuidas.

Las facultades atribuidas a las Administraciones públicas no son ilimitadas, así, estas deben servir con objetividad a los intereses generales, actuando de acuerdo a los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y al Derecho, de acuerdo al artículo 103.1 de la Constitución.

La LOPDGDD contempla diversos preceptos en los que la causa de legitimación encajaría en el artículo 6.1.e) del RGPD, a saber:

- Tratamientos de datos en el ámbito de la función estadística pública (artículo 25).
- Tratamientos de datos con fines de archivo de interés público por parte de las Administraciones públicas (artículo 26).
- Tratamientos de datos relativos a infracciones y sanciones administrativas (artículo 27).

2ª.- Tratamientos de datos personales para el cumplimiento de una finalidad o misión de interés público, que puede llevarse a cabo tanto por entidades públicas como privadas.

La LOPDGDD contempla varios supuestos que encuentran encaje en el artículo 6.1.e) del RGPD, a saber:

- Tratamientos con fines de videovigilancia (artículo 22).
- Sistemas de exclusión publicitaria (artículo 23).
- Tratamiento de datos para la protección de las personas que informen sobre informaciones normativas (artículo 24).

Conclusión

Esta base legal debe interpretarse con cierto grado de flexibilidad para garantizar la gestión de las Administraciones públicas, instituciones y organismos públicos, pues éstas no tienen la posibilidad de alegar como base legal para justificar un tratamiento de datos personales el interés legítimo.

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

- **En el caso de la actividad de las AALL será muy habitual que la base jurídica de los tratamientos** sea el cumplimiento de una tarea en **interés público** o el ejercicio de poderes públicos. Tanto el interés público como los poderes públicos que justifican el tratamiento deben estar **establecidos en una norma**.
- **Encargado de tratamiento**. Puede ser el **responsable de recopilar y operar el dato**.

  También puede ser el responsable de atender los derechos en materia de protección de datos.
- El **consentimiento** del artículo 28.2. de la Ley 39/2015, de 1 de octubre. Según el citado apartado 2 del artículo 28 de esta Ley, "Los interesados no estarán obligados a aportar documentos que hayan sido elaborados por cualquier Administración, con independencia de que la presentación de los citados documentos tenga carácter preceptivo o facultativo en el procedimiento de que se trate, siempre que el interesado haya expresado su consentimiento a que **sean consultados o recabados** dichos documentos. Se presumirá que la consulta u obtención es autorizada por los interesados salvo que conste en el procedimiento su oposición expresa o la ley especial aplicable requiera consentimiento expreso".
- **Tratamiento de categorías especiales de datos**

  El interés público habilita el tratamiento de datos de salud por los servicios sociales de ámbito municipal, cuya prestación esté reconocida por una **norma de rango legal**.

Novedades Legislativas RGPD

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

- **Identificación del empleado público con el DNI**
  De este modo, la inclusión del DNI podría no ajustarse al artículo 5 del RGPD, en relación con el principio de minimización de datos, salvo que tal dato fuese exigido por una norma especial.
  En todo caso, es recomendable la utilización de un sello del órgano correspondiente, sin necesidad de que
  aparezca la identificación del funcionario que realiza esta labor.

- **Notificación de actos administrativos**. Se impide N+A+DNI . Si se debe publicar N+A + *D*N*I*, si la notificación es por medio de **anuncios**, únicamente el DNI.
- **Publicación de datos en Portal de Transparencia**, Actas de JGL, Actas de Pleno. [video actas]
- **Metadatos.** Metaolvido
- **Abuso de posición dominante** de estas empresas, relacionados con la imposición de ciertos productos y con el uso que hacen de los datos que recaban. También puede ocurrir en las AAPP. Cuando la tecnología es difícil de sustituir los expertos hablan de el *cognitive lock-in* (bloqueo cognitivo) y el *vendor lock-in* (dependencia a los proveedores).

Seguridad en el tratamiento de datos personales

Reglamento General de Protección de Datos
RGPD y LOPDGDD

Artículo 32

Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que en su caso incluya, entre otros:

(a) la seudonimización y el cifrado de datos personales;

(b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

(c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

(d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

573 *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.

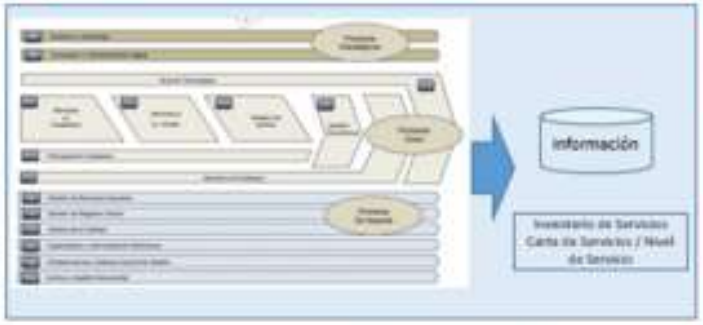
En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

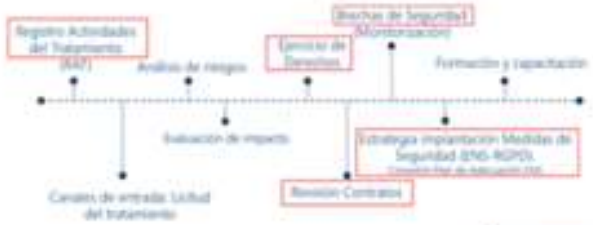
ENS Cadenas de Suministro

Seguridad en el tratamiento de datos personales

07 Sistema de Gestión de Seguridad de la Información y Protección de Datos

Extracto de la estrategia de Implantación ENS / RGPD





Medidas de Seguridad

Seguridad en el tratamiento de datos personales

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

¿Cómo encaja dentro del procedimiento Administrativo?

Desde la entrada en vigor de la Ley 39/2015, de Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de Régimen Jurídico del Sector Público, ambas de 1 de octubre, (que derogaron la Ley 11/2007, de Acceso de los ciudadanos a los Servicios Públicos), el ámbito de aplicación subjetivo del Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad (ENS), es coincidente con el señalado en la Ley 40/2015: el Sector Público, tal y como se encuentra definido en el art. 2 de dicha norma.

ENI /ENS

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha ampliado el ámbito de aplicación del ENS a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, señalando al ENS como instrumento fundamental para el logro de dichos objetivos en su artículo 156.

Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en el artículo 13 incluye el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

En desarrollo de las dos leyes anteriores, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, concreta en diferentes preceptos la obligación del cumplimiento de las medidas de seguridad previstas en el ENS, como los referidos al intercambio electrónico de datos en entornos cerrados de comunicación, los sistemas de clave concertada y otros sistemas de identificación de las personas interesadas, el archivo electrónico único o los portales de internet, entre otros.

Derecho de acceso por medios electrónicos con todas las garantías de seguridad

Seguridad en el tratamiento de Datos Personales

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

Para facilitar el proceso de adecuación al ENS, el CCN pone a disposición Herramientas de Gobernanza de la Ciberseguridad

ESQUEMA NACIONAL DE SEGURIDAD

Conjunto normativo que posibilita crear y mantener las condiciones necesarias de seguridad en el uso de los medios electrónicos, a través de medidas que garanticen la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, para facilitar el ejercicio de derechos y cumplimiento de deberes a través de estos medios.

Para las entidades públicas de su ámbito de aplicación, lo dispuesto en el ENS permite satisfacer los principios de actuación y los requisitos de seguridad de las Administraciones Públicas que les permitan alcanzar sus objetivos.

Para los ciudadanos, destinatarios últimos del servicio público, supone la garantía de que las entidades públicas con las que se relacionan reúnen las condiciones de seguridad necesarias para salvaguardar su información y sus derechos.

Listado de entidades del Sector Público certificadas en el ENS. 12

3% de las EELL Inés

327 sector público

41 EELL

11 nivel medio

QUÉ ES

- ✓ **Marco de gobernanza** de la Ciberseguridad

OBJETIVOS

- ✓ **Alinear el ENS con el marco normativo y el contexto estratégico** para garantizar la seguridad en la Administración Digital.
- ✓ Ajustar los requisitos del ENS para garantizar su **adaptación a la realidad** de ciertos colectivos o tipos de sistemas, entidades.
- ✓ **Reforzar la protección** frente a las tendencias en ciberseguridad con principios básicos, requisitos y medidas a adoptar por las entidades sujetas al ENS.
- ✓ **Gestión continuada de la seguridad**, la prevención, detección y corrección, para una mejor ciber-resiliencia.
- ✓ **Tratamiento homogéneo de la seguridad que facilite la cooperación** en la prestación de servicios públicos digitales
- ✓ **Proporcionar los elementos comunes** que han de guiar la actuación de las entidades del Sector Público y de sus proveedores tecnológicos en materia de seguridad de las tecnologías de la información.
- ✓ Servir de **modelo de buenas prácticas.**

Seguridad en el tratamiento de Datos Personales
Esquema Nacional de Seguridad

Los elementos principales del ENS son los siguientes:

- Los **principios básicos** en materia de seguridad (arts. 5-11).
  - Seguridad como proceso integral
  - Gestión basada en riesgos
  - Prevención, detección, respuesta y conservación
  - Líneas de defensa (org, fís, lóg)
  - Reevaluación periódica
  - Diferenciación de responsabilidades (medidas compensatorias). Principio de diferenciación e independencia

La política de seguridad de la información es el conjunto de directrices que rigen la forma en la que una organización gestiona y protege el información que trata y los servicios que presta

- **Requisitos mínimos** que permitan una protección adecuada de la información (arts. 12-27).

Política de Seguridad

- Objetivos y misión de la organización
- Marco regulatorio en el que se desarrollan las actividades
- Roles de seguridad y funciones
- Estructura y composición del Comité de Seguridad
- Estructura de la documentación del sistema de Gestión
- Riesgos que se derivan del tratamiento de datos personales

Requisitos mínimos

- Organización del proceso de la seguridad
- Análisis y Gestión de Riesgos
- Gestión del personal
- Profesionalidad
- Autorización y Control de Accesos. MP
- Protección de Instalaciones
- Adquisición de Productos
- Integridad y actualización del Sistema
- Protección almacenada y en tránsito
- Protección de sistemas interconectados
- Registro de actividad
- Incidentes de seguridad
- Continuidad de la Actividad (copias, restores)

Seguridad en el tratamiento de Datos Personales
Esquema Nacional de Seguridad

- El mecanismo para lograr el cumplimiento de los principios básicos y de los requisitos mínimos mediante la adopción de medidas de seguridad proporcionadas a la naturaleza de la información y los servicios a proteger (arts. 28, 40, 41, Anexo I y Anexo II).
- El uso de infraestructuras y servicios comunes (art. 29).
- Los perfiles de cumplimiento específicos (art. 30).

  Determinadas entidades o sectores concretos tienen perfiles de cumplimiento específicos adecuados a su análisis de riesgos para una categoría concreta
- El informe de estado de la seguridad (art. 32)
- La auditoría de la seguridad (art. 31 y Anexo III).
- La respuesta ante incidentes de seguridad (arts. 33 y 34).
- El uso de productos certificados (art. 19 y Anexo II).
- La conformidad (art. 38).
- La formación y la concienciación (disposición adicional primera).
- Las guías de seguridad (disposición adicional segunda).
- Las instrucciones técnicas de seguridad (disposición adicional segunda).

Los municipios podrán disponer de una política de seguridad común elaborada por la entidad local comarcal o provincial que asuma la responsabilidad de la seguridad de la información de los sistemas municipales

Seguridad en el tratamiento de Datos Personales
Esquema Nacional de Seguridad

µCeENS

µCeENS es una metodología innovadora que se beneficia de las novedades del Real Decreto 311/2022, de 3 de mayo, para facilitar la obtención de la **Certificación de Conformidad en el Esquema Nacional de Seguridad (ENS)** en base a un **Perfil de Cumplimiento Específico (PCE)**.

Con esta metodología se proporciona el **acompañamiento y la asistencia necesaria** para alcanzar la Certificación de Conformidad con el ENS desde la fase previa a la adecuación, hasta después de su obtención, todo ello automatizado en las herramientas de Gobernanza de la Ciberseguridad (INES-AMPARO).

2. Gobierno y Adecuación

Pinche para ampliar

Política de seguridad, establecer una estructura, determinar roles asignando responsabilidades y flujos de relación, inventario de activos, categorización, declaración de aplicabilidad e informe de riesgos.

Colaboración e impulso: Roles

Los/las Responsables de la Información y Responsables de los Servicios.
Determinan los requisitos (de seguridad) de la Información tratada y de los Servicios prestados.

Responsable de Seguridad. Determina las decisiones de seguridad para satisfacer los requisitos de la información manejada y de los servicios prestados. Nivel Supervisión.

Responsable del Sistema. Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad.

Delgado/a de Protección de Datos.
Informa y asesora a los responsables de las actividades de tratamiento. Supervisa el cumplimiento de lo dispuesto en normativa de protección de datos personales. Coopera con la AEPD y presta atención a los riesgos asociados a las operaciones de tratamiento.

Seguridad en el tratamiento de Datos Personales

Esquema Nacional de Seguridad

¿Qué es un el Plan de Adecuación? Hoja de ruta

El Plan de Adecuación es un **conjunto ordenado de acciones tendentes a satisfacer lo exigido por el ENS**. Este Plan deberá contemplar las siguientes fases:

- Disponer de una **Política de Seguridad**, incluyendo la definición de roles y la asignación de responsabilidades.
- **Categorizar** los sistemas de información, atendiendo a la valoración de la información manejada, teniendo en cuenta si incluye datos de carácter personal, y la **valoración** de la información y servicios prestados.
- **Realizar el análisis de riesgos**, incluyendo la valoración de las medidas de seguridad existentes.
- Preparar la **Declaración de Aplicabilidad de las Medidas del Anexo II del ENS** y Perfil de Cumplimiento.
- Elaborar un **Plan de Mejora de la seguridad**, sobre la base de las insuficiencias detectadas, incluyendo plazos estimados de ejecución. (Hoja de Ruta)

NIVEL BAJO

Un incidente de seguridad supone un **prejuicio limitado** [reducción apreciable de las capacidades, daño menor de un activo, incumplimiento de una regulación con carácter **subsanable**, prejuicio molesto a un individuo].

NIVEL MEDIO

Un incidente de seguridad supone un **prejuicio grave**

[reducción significativa de las capacidades, daño mayor de un activo, incumplimiento de una regulación con carácter **subsanable**, prejuicio de difícil reparación a un individuo].

NIVEL ALTO

Anulación de la capacidad de prestar un servicio y daños irreparables.

Información B	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto
...	...	...	...	...	...
Servicio X	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto

Seguridad en el Tratamiento de Datos Personales

Análisis de Riesgos y Evaluación de Impacto // Dimensiones DICAT

	BAJO	MEDIO	ALTO
	Perjuicio limitado	Perjuicio grave	Perjuicio muy grave
CAPACIDAD (Alcanzar sus objetivos)	Reducción apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose	Reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose	La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose
DAÑO ACTIVO (Protección activo)	El sufrimiento de un daño menor por los activos de la organización	El sufrimiento de un daño significativo por los activos de la organización	El sufrimiento de un daño muy grave, por los activos de la organización
CUMPLIMIENTO SERVICIO (Obligaciones diarias de servicio)	Reducción apreciable de la capacidad para cumplir con las obligaciones diarias del servicio	Reducción significativa de la capacidad para cumplir con las obligaciones diarias del servicio	Anulada la capacidad para cumplir con las obligaciones diarias del servicio
CUMPLIMIENTO LEY (Legislación vigente)	El incumplimiento formal de alguna ley o regulación, que tenga el carácter de subsanable	El incumplimiento material de alguna ley o regulación o el incumplimiento formal que no tenga el carácter de subsanable	El incumplimiento formal y material grave de alguna ley o regulación
NORMA CONTRACTUAL	Incumplimiento formal leve de una obligación contractual	Incumplimiento material o formal de una obligación contractual	Incumplimiento formal o material grave de una obligación contractual
NORMA INTERNA	Incumplimiento formal leve de una norma interna	Incumplimiento material o formal de una norma interna	Incumplimiento formal o material grave de una norma interna
CIUDADANÍA (Respeto derechos de las personas)	Causar un perjuicio menor a algún individuo, que, aun siendo molesto, pueda ser fácilmente reparable	Causar un perjuicio significativo a algún individuo, de difícil reparación	Causar un perjuicio grave a algún individuo, de difícil o imposible reparación
PÉRDIDAS ECONÓMICAS	Pérdidas económicas apreciables (no superiores al 5% del presupuesto anual de la organización)	Pérdidas económicas importantes (superiores al 5% e inferiores al 10% del presupuesto anual de la organización)	Pérdidas económicas o alteraciones financieras significativas (superiores al 10% del presupuesto anual de la organización)
REPUTACIÓN	Daño reputacional moderado con los ciudadanos o con otras organizaciones	Daño reputacional significativo con los ciudadanos o con otras organizaciones	Daño reputacional grave con los ciudadanos o con otras organizaciones
PROTESTAS	Múltiples protestas individuales	Protestas públicas (alteración del orden público)	Protestas masivas (alteración seria del orden público)
DELITOS	Favorecería la comisión de delitos	Favorecería significativamente la comisión de delitos o dificultaría su investigación	Podría incitar a la comisión de delitos, constituiría en sí un delito, o dificultaría enormemente su investigación

[DICAT]
Disponibilidad [D]
Integridad [I]
Confidencialidad [C]
Autenticidad [A]
Trazabilidad [T]

DIMENSIÓN DISPONIBILIDAD DEL SERVICIO			
IMPACTO	BAJA	MEDIA	ALTA
RTO (Tiempo de Recuperación del Servicio)	1 día < RTO < 5 días	4 horas < RTO < 1 día	< 4 horas

CATEGORÍA DEL SISTEMA	[C]	[I]	[T]	[A]	[D]
NIVEL MÁXIMO SERVICIOS+INFORMACIÓN	[M]	[M]	[M]	[M]	[M]
CATEGORÍA MEDIA[C=M, I =M, T=M, A=M, D=M]					

Seguridad en el tratamiento de datos personales

Contexto general

Contexto general

- Punto de inflexión para la incorporación a nuestra entidad de esta cultura de protección tan reglamentariamente y éticamente necesaria.
- Actual uso intensivo de las tecnologías:
  - Inmersos en un proyecto de digitalización integral.
  - Implicados en proyectos de alta tecnología (EPIU que promueve hogares saludables mediante el uso de técnicas de IA).
  - Nuestra ciudad dentro del internet de las cosas.
- Escenario de ciberamenazas y conflictos bélicos híbridos sin antecedentes
  - Obligados y comprometidos con la seguridad y protección de datos.
  - En línea con estrategias nacionales y europeas de datos y ciberseguridad.
- Nivel de uso de datos personales sin precedentes
  - Nivel inusual de datos personales que pueden poner en serio riesgo los derechos y libertades de todos nosotros, y desgraciadamente no sólo en términos de privacidad e intimidad.

Primer paso: El compromiso Inicial

Los vectores de infección / entrada.
Los "malos", simplemente tienen que encontrar una de tus muchas puertas un poco abierta
los días las tienes que cerrar...

Segundo paso: Exploración del territorio

Tercer paso: Elevación de privilegios

Cuarto paso: Consiguiendo persistencia

Quinto paso: Exfiltrando informaci

Sexto paso: Lanzamiento del cifrado

Elementos nucleares de secuestro: privación de libertad y condición para ponerlo en libertad.

Ransomware, es un secuestro de información.

Su origen: del inglés ransom, 'rescate', y ware, acortamiento de software).

Se espera que el ransomware ataque a una empresa, un consumidor o un dispositivo cada dos segundos el año 2031, frente a cada 11 segundos que ataco en 2021.

Exfiltración hacia C2:

- Tunelización a través de protocolos DNS, SMB, FTP, HTTP/S, SMTP, etc.
- Herramientas de almacenamiento en nube.
- Transferencias programadas.

Lo que se llevan, nunca vuelve:

- Información corporativa.
- Información de ciudadanos.
- Información para futuros ataques (quizás tu víctima sea un proveedor, ciudada

En seis años Los ciberataques contra las AAPP se incrementaron en un 455%

Seguridad en el Tratamiento de Datos Personales
Medidas de Seguridad Anexo II ENS

Responsabilidad Proactiva
Seguridad y Privacidad por Defecto

Controles ENS	
El Ayuntamiento de Getafe está implantando las medidas en categoría MEDIA del ENS	
MEDIDAS ENS (categoría básica en implantación MEDIA)	
§ **Marco organizativo [org]**	
- Org.1 Política de Seguridad	
Comité de Seguridad, roles y responsabilidades	
- Org.2 Normativa de seguridad	
- Org.3 Procedimientos de seguridad	
- Org.4 Proceso de autorización	
§ **Marco Operacional [op]**	
- Op.pl.1. Análisis de riesgos	
- Op.pl.2. Arquitectura de seguridad	
- Op.pl.3. Adquisición de nuevos componentes	
Control de acceso [op.acc.]	
- Op.acc.1. Identificación	
- Op.acc.2. Requisitos de acceso	
- Op.acc.4. Proceso de gestión de derechos de acceso	
- Op.acc.5. Mecanismos de autentificación	
- Op.acc.6. Acceso local	
- Op.acc.7. Acceso remoto	
Explotación [op.exp.]	
- Op.exp.1. Inventario de activos	
- Op.exp.2. Configuración de seguridad	
- Op.exp.4. Mantenimiento	
- Op.exp.6. Protección frente a código dañino	
- Op.exp.8. Registro de actividad de usuarios	
- Op.exp.11. Protección de claves criptográficas	
Monitorización del sistema [op.mon.1]	
- Op.mon.2. Sistemas de métricas	

Medidas de Protección [mp]
Protección de las instalaciones e infraestructuras [mp. if]
- mp.if.1 Áreas separadas y control de accesos
- mp.if.2 Identificación de las personas (con medidas correctivas dentro del pla
- mp.if.3 Acondicionamiento de locales
- mp.if.4 Energía eléctrica
- mp.if.5 Protección frente a incendios
- mp.if.7 Registro de entrada y salida de equipamiento
Gestión personal [mp.per.]
- mp.per.1 Caracterización del puesto de trabajo
- mp.per.2 Gestión del personal: deberes y obligaciones
- mp.per.3. Concienciación
- mp.per.4. Formación
Protección de equipos[mp.eq.]
- mp.eq.1 Puesto de trabajo despejado
- mp.eq.3 Protección de los equipos portátiles
- mp.eq.9 Medios alternativos
Protección de las comunicaciones [mp.com]
- mp.com.1 Seguridad perimetral
- mp.com.3 Protección de autenticidad e integridad
Protección de soportes de información [mp.si.1]
- mp.si.1 Etiquetado
- mp.si.3 Custodia
- mp.si.4 Transporte
- mp.si.5 Borrado y destrucción
Protección de app [mp. sw]
- Mp.sw.2 Aceptación y puesta de servicio
Protección de la información [mp.info]
- mp.info.1 Datos de carácter personal
- mp.info.2 Calificación de la información
- mp.info.4 Firma electrónica
- mp.info.6 Limpieza de documentos
- mp.info.9 Copias de seguridad
Protección de los servicios [mp. s]
- mp.s.1 Protección del correo electrónico
- mp.s.2 Protección de autenticidad y de la integridad

- Proteger credenciales
- Contraseñas privadas
- Contraseñas profesionales
- No acceso a avisos, correos de dudosa procedencia
- Síndrome del clic fácil
- Contraseñas en memoria de navegadores
- Sesiones sin cerrar
- Urgencia
- Solicitud de datos de credenciales/banco
- Certificados digitales con contraseña
- Canales seguros (ORVE, no correo)
- Faltas de Ortografía
- No operar con móviles
- Borrado Seguro
- Etiquetar dispositivos de almacenamiento
- Cifrar portátiles y dispositivos de almacenamiento
- No Sw pirata / gratuito
- Contraseñas en texto plano
- Metadatos (CSV)
- Wifis públicas

Seguridad en el Tratamiento de Datos Personales
Contexto General

La Agencia de Ciberseguridad de la Comunidad de Madrid atiende directamente a los ayuntamientos con menos de 20.000 habitantes, especialmente en materia de administración electrónica y protección digital.

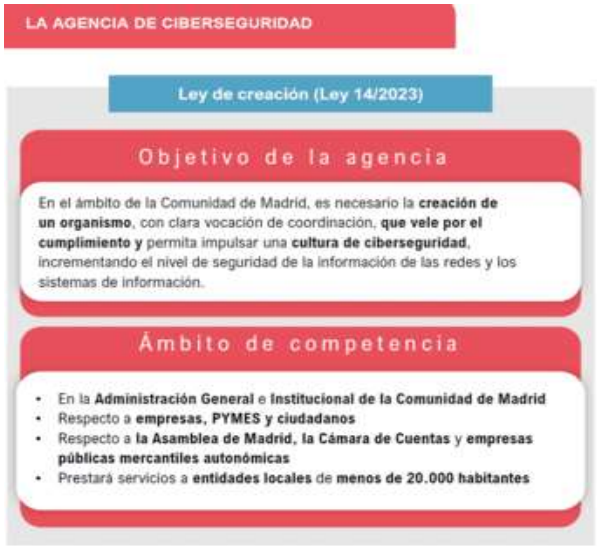
Objetivo: reforzar la ciberseguridad en municipios pequeños que no cuentan con recursos suficientes.

Servicios:

- Asesoramiento especializado.
- Implementación del Escudo Digital (prevención, detección y respuesta ante incidentes).
- Formación y concienciación para empleados públicos.

Cobertura actual: ya se ha desplegado en 60 municipios y se ampliará a 143 localidades antes de fin de año.

csirt@madrid.org



Seguridad en el Tratamiento de Datos Personales
Contexto General

Seguridad en el Tratamiento de Datos Personales
Contexto General

Estrategia de Seguridad (en línea con la estrategia Europea y Exigencias Next Generation)

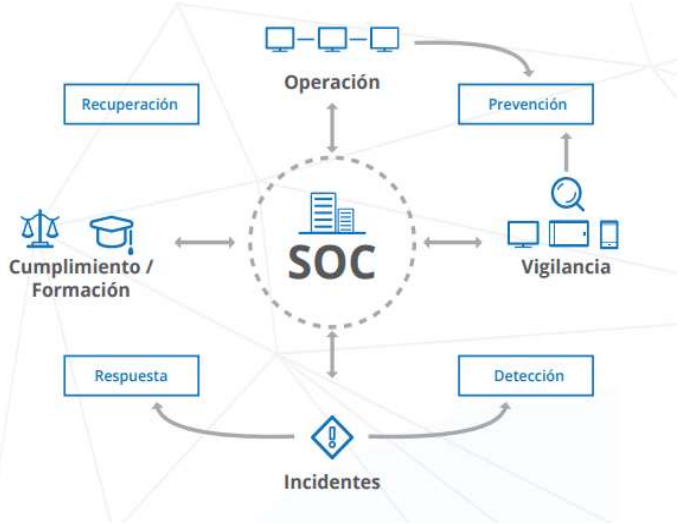
- Herramientas de Detección, Reacción, Protección y Auditoría: LUCIA, Micro-Claudia, SAT-INET, REYES. [ENS. Servicios y Productos certificados.]

- Actuaciones a corto plazo:
- Implantación de un Centro de Operaciones de Seguridad (SOC).
  - Sistemas de Alerta Temprana.
  - Seguridad en servidores y equipos de usuario (EDR)
  - Seguridad en redes. (Doble barrera)
  - Seguridad en accesos (2FA)
  - Revisión y actualización de SIs críticos.

- Actuaciones a medio plazo
  - Modernizar sistemas y equipamientos
  - Incorporar la competencia y cultura de ciberdefensa

Seguridad en el Tratamiento de Datos Personales
Contexto General

Tipos de SOC y Operativa de un SOC



Medias de Seguridad y Protección Técnicas y Organizativas

Seguridad en el Tratamiento de Datos Personales

Análisis de Riesgos y Evaluación de Impacto //Derechos y libertades

https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-nueva-guia-gestionar-riesgos-y-evaluciones-impacto

Actividad de tratamiento	FACTORES DE RIESGO		
	Factor	Desglose actividades del factor de riesgo	Valoración el riesgo inherente
MONITORIZACIÓN Y CONTROL DE SEGURIDAD TIC	Control empleados	Monitorización del puesto de trabajo	MEDIO
MONITORIZACIÓN Y CONTROL DE SEGURIDAD TIC CORREO ELECTRÓNICO CORPORATIVO		Monitorización y control del correo electrónico	MEDIO
MONITORIZACIÓN Y CONTROL DE SEGURIDAD TIC REGISTRO DE CONEXIONES EXTERNAS		Monitorización y control navegación en internet	MEDIO
ACCESO WIFI CORPORATIVO (AYTORCM) MONITORIZACIÓN Y CONTROL DE SEGURIDAD TIC ACCESO WIFI ESPACIOS MUNICIPALES	Control del acceso a Internet	Análisis o evaluación de la actividad de navegación	MEDIO
VIDEOVIGILANCIA CÁMARAS (RPAS) VIDEOVIGILANCIA CÁMARAS UNIPERSONALES POLICÍA LOCAL VIDEO VIGILANCIA DE ESPACIOS PÚBLICOS PROTEGIDOS SERVICIO DE VIDEOVIGILANCIA Y CONTROL DE ACCESOS (SIBA) GRABACIÓN DE IMÁGENES DE LAS CÁMARAS DE VIGILANCIA EN ESPACIOS PÚBLICOS EN FIESTAS PATRONALES GRABACIÓN DE IMÁGENES DE LAS CÁMARAS DE VIGILANCIA DE LOS EDIFICIOS MUNICIPALES GRABACIONES DE IMÁGENES DE LAS CÁMARAS DE VIGILANCIA DE LOS EDIFICIOS DE LA POLICÍA LOCAL	Observación	Vigilancia mediante imágenes	ALTO
PROYECTO EPIU: SISTEMA DE INTELIGENCIA ARTIFICIAL	Evaluación de sujetos/Perfilado		ALTO
CONTROL DE ACCESO AL APARCAMIENTO SERVICIO DE VIDEOVIGILANCIA Y CONTROL DE ACCESOS CONTROL DE ACCESO Y REGISTRO DE VISITAS A LA CASA CONSISTORIAL	Control físico de acceso	Control de acceso a edificios (públicos)	BAJO
CERTIFICADOS DIGITALES DOBLE FACTOR DE AUTENTICACIÓN Y APORTACIÓN DE RECURSOS PROPIOS PARA TRABAJO Y TELETRABAJO USUARIOS Y PERMISOS	Identificación unívoca	N/A	BAJO

Controles (medidas técnicas y organizativas)			
Medidas cumplimiento normativo RGPD			
Política Seguridad información y protección de datos			
Roles ENS y Delegado Protección de Datos			
Registro de Actividades del Tratamiento			
Procedimiento ejercicio derechos			
Análisis de bases de licitud			
Registro de incidentes y procedimiento gestión			
Instrucciones (información, publicaciones…)			
Procedimiento gestión prestadores			
Actualización de la información a las personas afectadas			
Procedimiento AARR e EIPD			
Análisis de riesgos			
Información y confidencialidad empleados			
Supervisiones periódicas (DPD)			
Formación en protección de datos y seguridad de la información			
Procedimientos de conservación y gestión documental			

	Impacto para personas afectadas	Probabilidad	VALORACIÓN DEL RIESGO
Pérdida de confidencialidad	Significativo	Baja	ALTO
Pérdida de integridad	Significativo	Improbable	MEDIO
Pérdida de disponibilidad	Significativo	Improbable	MEDIO
Deficiencias en la resiliencia	Limitado	Improbable	BAJO
Autenticación	Limitado	Improbable	BAJO
Trazabilidad	Limitado	Improbable	BAJO
Fallos en medidas técnicas y organizativas en el tratamiento de datos	Limitado	Baja	MEDIO
Errores en las operaciones técnicas del tratamiento	Limitado	Baja	MEDIO

Para el cálculo de probabilidad se han tenido en cuenta las medidas implantadas a la fecha así como los incidentes registrados y reclamaciones ante la autoridad de control

Seguridad en el Tratamiento de Datos Personales

Medias organizativas y técnicas

¿Qué son las medidas organizativas técnicas y medidas organizativas?

Las medidas de seguridad técnicas y organizativas son términos que se utilizan a menudo en el contexto del RGPD.

Una medida técnica podría ser el uso de software antivirus para la detección de malware en su ordenador o el uso de cámaras de video para disuadir a los delincuentes. Tanto el software antivirus como las cámaras de video pueden ayudar a una empresa a mantener un nivel adecuado de seguridad de la información personal identificable que su empresa está tratamiento.

Una medida organizativa podría ser los tratar, los procedimientos o la formación de los empleados en las mejores prácticas. Las medidas organizativas son esenciales para aplicarlas en las organizaciones menores, ya que éstas suelen disponer de menos recursos técnicos para aplicar medidas técnicas. Las medidas técnicas suelen requerir conocimientos más especializados para su aplicación adecuada.

¿Qué son las medidas "adecuadas"?

El RGPD establece que es necesario aplicar medidas organizativas técnicas y medidas organizativas "apropiadas"; en este sentido, el significado de "apropiado" es un término crucial que hay que entender para el cumplimiento del RGPD.

Sólo sabrá cuáles son las medidas adecuadas cuando haya evaluado los riesgos del tratamiento datos personales de su organización. Así que hay que hacer una evaluación de riesgos.

A partir de los resultados de sus evaluaciones de riesgo, sabrá a qué amenazas y consecuencias potenciales se enfrenta su organización. Después, es esencial mitigar estos riesgos mediante la adopción de medidas técnicas organizativas y medidas técnicas"adecuadas".

https://rgpd.com/es/reglemento/capitulo-4-responsable-del-tratamiento-y-encargado-del-tratamiento/articulo-32-seguridad-del-tratamiento/

Seguridad en el Tratamiento de Datos Personales

Instrucciones Internas, Códigos de Conducta

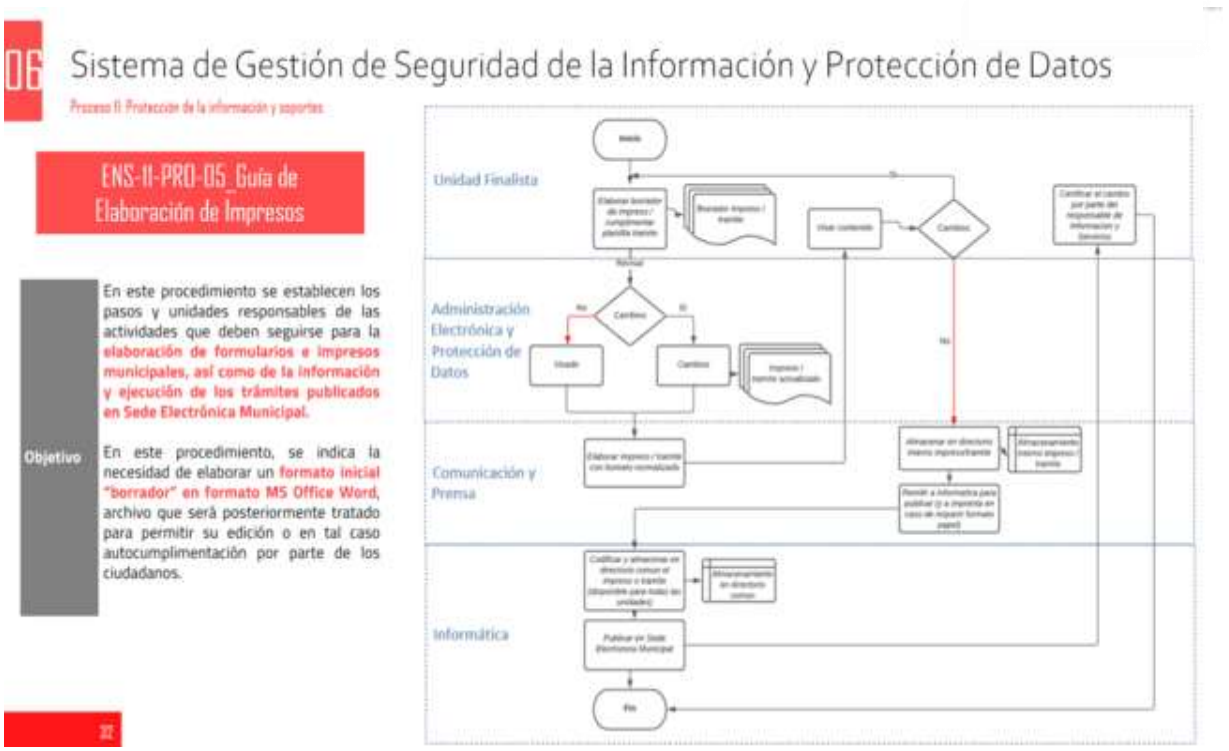
*Firma o autorización por parte de ambos **tutores** (salvo justificación por motivos de custodia).*

*Indique si la persona se encuentra en situación de **especial vulnerabilidad**. Se le requerirá documentación acreditativa*

Declaro bajo mi responsabilidad la veracidad de los datos indicados, y haber sido informado/a de la necesidad de entregar dichos datos [Acepto las condiciones de participación].

***Autorizo la captación de imágenes** e información multimedia con el fin de promocionar las actividades municipales. La imagen y/o video se difundirá en espacios y medios de divulgación municipal (página web, boletines informativos municipales)*

***Autorizo a recibir avisos** y comunicaciones (u otra finalidad) mediante: ☐ Correo ☐ Teléfono*



Información sobre Protección de datos de carácter personal:

*Los datos recabados serán incorporados y tratados por el Ayuntamiento de Getafe, como responsable del tratamiento, en la **actividad de tratamiento** **[*****]**, con la **finalidad de** **[*****]**. El tratamiento queda **legitimado por el [cumplimiento de una obligación legal o misión de interés publico]** según la Ley **[indicar referencia]**Los datos no serán cedidos a terceros salvo cuando exista una obligación legal. No se realizan transferencias internacionales de datos. Podrá ejercer sus derechos ante el Servicio de Atención al Vecino (Plaza de la Constitución, s/n, 28901, Getafe, Madrid), en la sede electrónica del Ayuntamiento. Si lo desea puede consultar a la persona designada como Delegada de Protección de Datos a dpd@ayto-getafe,org*

INFORMACIÓN ADICIONAL en sede.getafe.es- Protección de Datos La legitimación consta en el registro de actividades del tratamiento. Con carácter general, el tratamiento se legitima para dar cumplimiento a una Ley (p.e recogida de datos para el pago de tasas o impuestos) o por el cumplimiento de una misión de interés público (p.e. competencias municipales de la Ley de Base de Régimen Local) o el ejercicio de potestades públicas (p.e. tramitar un procedimiento sancionador de tráfico). El consentimiento es una legitimación residual).

Seguridad en el Tratamiento de Datos Personales

Instrucciones Internas, Códigos de Conducta

06 Sistema de Gestión de Seguridad de la Información y Protección de Datos

Proceso 8: Protección de la información y soportes

Recomendaciones para cumplir con el deber de información

Objetivo

Incluye todos los aspectos a tener en cuenta para cumplir con la normativa vigente de protección de datos durante la recogida de datos de carácter personal:

1. Información sobre protección de datos de carácter personal que debe incluirse en todos los formularios / impresos.
2. Instrucciones si en el formulario/impreso se permite que los interesados no aporten documentos de la administración (aplicación del artículo 28 de la LPAC).
3. Instrucciones para la recogida de datos de menores.
4. Instrucciones para la recogida de categorías especiales de datos.
5. El interesado debe declarar que los datos son ciertos o que acepta las condiciones de participación en una actividad/concurso.
6. Autorización para el uso de imágenes.
7. Recogida de email y/o número de teléfono para avisos y/o comunicaciones.
8. Transferencias internacionales de datos (Información sobre publicaciones en Redes Sociales)

Información sobre Protección de datos de carácter personal:

Los datos recabados serán incorporados y tratados por el Ayuntamiento de Getafe, como responsable del tratamiento, en la ***actividad de tratamiento*** **[*****]**, *con la* ***finalidad de*** **[*****]**. *El tratamiento queda* ***legitimado por el [cumplimiento de una obligación legal o misión de interés público]*** *según la Ley* ***[indicar referencia]*** *Los datos no serán cedidos a terceros salvo cuando exista una obligación legal. No se realizan transferencias internacionales de datos. Podrá ejercer sus derechos ante el Servicio de Atención al Vecino (Plaza de la Constitución, s/n, 28901, Getafe, Madrid), en la sede electrónica del Ayuntamiento. Si lo desea puede consultar a la persona designada como Delegada de Protección de Datos a dpd@ayto-getafe.es.* *INFORMACIÓN ADICIONAL en sede.getafe.es- Protección de Datos*

Extracto Punto 1 – Información que debe incluirse en todos los formularios / impresos

Seguridad en el Tratamiento de Datos Personales

Instrucciones Internas, Códigos de Conducta

06

Sistema de Gestión de Seguridad de la Información y Protección de Datos

Proceso 07. Protección de las Instalaciones

ENS-07-PRO-02 Gestión de cámaras y grabaciones videovigilancia

Objetivo

Este documento tiene por objeto definir los roles, autoridades y el conjunto de actividades que deben llevarse a cabo para gestionar el proceso de gestión de instalación y videovigilancia con cámaras fijas y móviles en vía pública, espacios públicos o espacios donde dadas las circunstancias particulares se requiera la activación de cámaras fijas, móviles o unipersonales gestionadas y administradas por policía local del municipio Getafe.
Las actividades que se detallan son:

- Identificar la **necesidad de videovigilancia** vinculada a garantizar la seguridad de personas, bienes e instalaciones.
- **Clasificar la finalidad de la videovigilancia .**
- **Consulta / autorización** de Delegación de Gobierno.
- **Inventario e instalación de cámaras.**
- **Mapa de la ubicación de cámaras** y cartelería informativa.

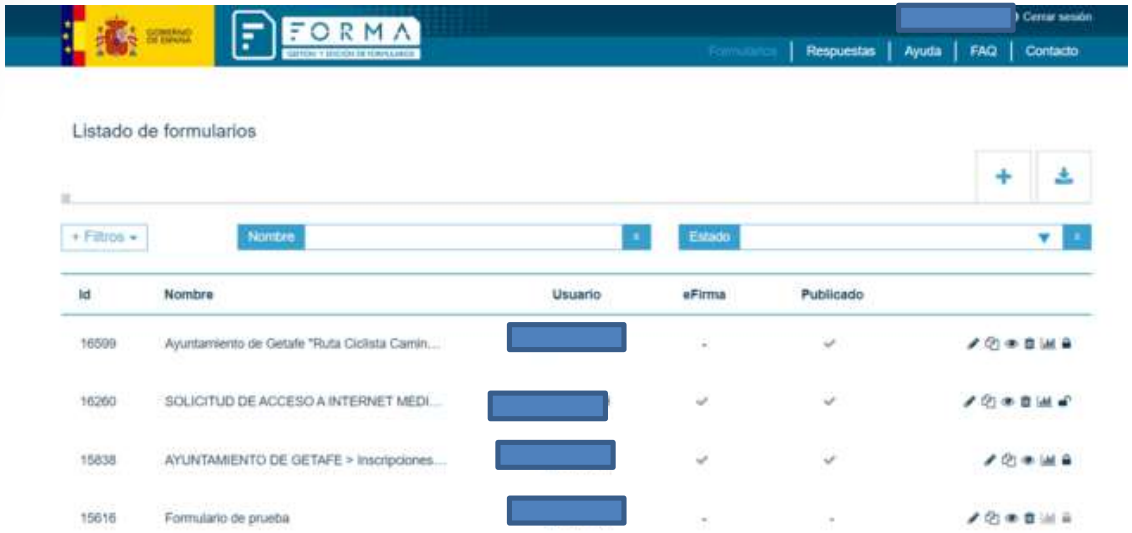
Actividad	R Realiza	A Responsable	C Consultado	I Informado
Gestión y administración de las cámaras	Policía Local	Policía Local		
Definición de la necesidad de ubicar las cámaras y solicitud de autorización a la Delegación de Gobierno	Responsable de información y servicios de Policía Local	Responsable de información y servicios de Policía Local	DPD	DPD
Gestión y mantenimiento del Inventario de Cámaras	Área de Informática	Responsable de Informática		
Adquisición de las Cámaras	Responsable de la Unidad Finalista	Responsable de la Unidad Finalista	Responsable de información y servicios de Policía Local	Responsable de Informática

Matriz RACI

Seguridad en el Tratamiento de Datos Personales

Instrucciones Internas, Códigos de Conducta

https://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=forma



DERECHOS EN MATERIA DE PROTECCION DE DATOS

Consentimiento reforzado (**custodiado** por tercera parte de confianza).
Consentimiento con **e-firma** en el caso de menores.
Gestión de derechos y preferencias de comunicación centradas en el usuario.

Seguridad en el Tratamiento de Datos Personales

Instrucciones Internas, Códigos de Conducta

AYUNTAMIENTO DE GETAFE	Guía Protección de Datos en Procesos selectivos	Identificador: ENS-00-REG-01-06 Versión: 01 Fecha: 27/06/2023 Página 1 de 21

Elaborado por:	Aprobado por:
Delegado/a de Protección de Datos	Comité de Seguridad y Protección de Datos El documento ha sido firmado por el Concejal Delegado de Hacienda, Recursos Humanos y Modernización de la Administración, D. Herminio Vico Algaba, en fecha 21 de julio de 2023.

Guía Protección de Datos en Procesos selectivos

ÍNDICE:

AYUNTAMIENTO DE GETAFE	Normativa de Uso de los Sistemas de Información	Identificador: ENS-02-NOR-01 Versión: 01 Fecha: 20/01/2023 Página 1 de 21

ÍNDICE:

Seguridad en el Tratamiento de Datos Personales

Instrucciones Internas, Códigos de Conducta

Compromisos y Pacto Digital

- ✓ Servicios Digitales donde el valor esencial sean las personas (Derechos y libertades de ciudadanas y ciudadanos).
- ✓ Ética y la lucha contra el acoso y violencia en internet
- ✓ Privacidad como un activo.
- ✓ Gobernanza del dato para la mejora de políticas públicas.
- ✓ Escenario de prueba en innovación (mejora de la calidad de vida, medio ambiente y la protección de las personas).
- ✓ Conectividad accesible e inclusiva (que fomente la igualdad de género, la protección de la infancia y de las personas más vulnerables).
- ✓ Por una tecnología que no perpetúe sesgos (no a la discriminación algorítmica por razón de raza, procedencia, creencia, religión o sexo...)

https://www.aepd.es/canalprioritario

No es por el vídeo o la foto, es por todo lo que hay detrás

Seguridad en el Tratamiento de Datos Personales

A mínimos con la seguridad

Conociéndote a ti mismo: ¿Qué medidas tenemos?

a) ¿Tienes un doble factor de autenticación (MFA)?
b) ¿Mantienes actualizados tu puesto de trabajo (S.O. y Aplicaciones)?
c) ¿Dispones de un antivirus con capacidades EDR/XDR o sólo es EPP?
d) ¿Almacenas contraseñas en los navegadores? ¿Utilizas gestores de claves?
e) ¿Cambias / Reutilizas contraseñas en diferentes servicios? ¿Patrones claves?
f) ¿Existen usuarios con privilegios para instalar aplicaciones?
g) ¿Has instalado alguna vez software "pirata"?
h) ¿Tienes una copia de seguridad "off-line" / inmutable?
i) ¿Tienes cifrado tus equipos / soportes?
j) ¿Monitorizas la actividad de tu red?
k) ¿Tenemos un plan "b"?

Contraseñas: Errores mas frecuentes

1. Crear contraseñas simples.
2. Reutilizar contraseñas.
3. Almacenar contraseñas en texto plano o en navegadores.
4. Compartir contraseñas.
5. Generar contraseñas en base a patrones.

Contraseñas: Doble Factor de Autenticación

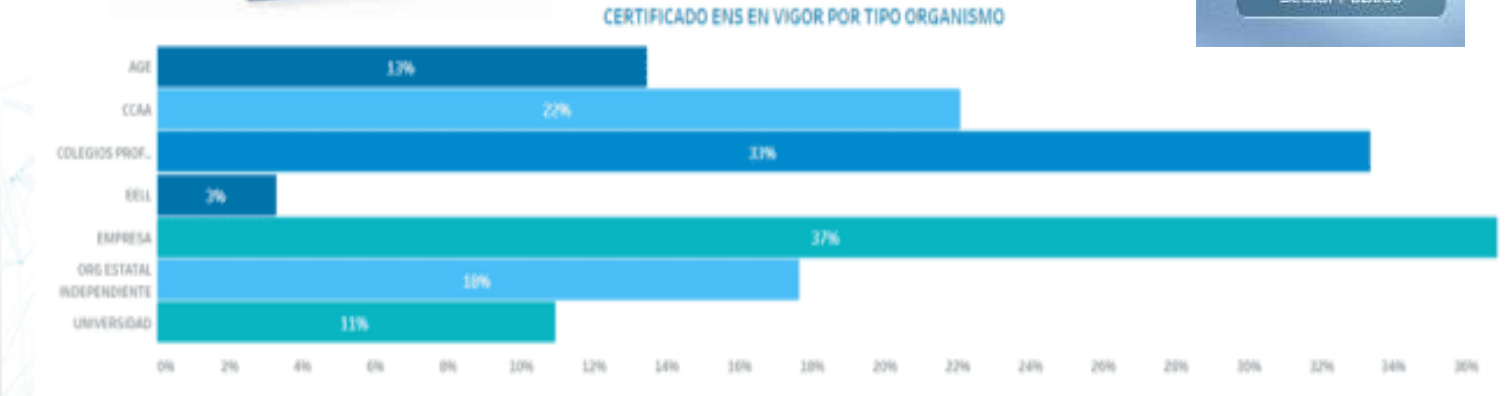
Seguridad en el Tratamiento de Datos Personales
Mecanismos de certificación

[Certificación (cni.es)]

Seguridad en el Tratamiento de Datos Personales
Mecanismos de certificación

Un mecanismo de certificación es instrumentos que permiten demostrar el cumplimiento de lo dispuesto en el RGPD, ENS y demás normativas, sistemas de gestión de seguridad, calidad, etc.

- Responsable del Tratamiento : art 24.3 señala dentro de las obligaciones relativas a su responsabilidad está la adhesión a códigos de conducta o mecanismo de certificación
- Encargado de tratamiento: art. 28.1 señala que cuando se vaya a realizar un tratamiento por cuenta de un responsable de tratamiento, éste elegirá únicamente un encargado que ofrezca las garantías suficientes para aplicar las medidas de seguridad técnicas y organizativas de manera que sea conforme con lo establecido en el RGPD.



Seguridad en el Tratamiento de Datos Personales
Mecanismos de certificación

NECESARIO APOYO POLÍTICO

- ✓ **Gobernar el dato** y la responsabilidad de su tratamiento es de la **entidad**
- ✓ **Proteger el dato** es corresponsabilidad de **todas las concejalías**

Actuaciones a desarrollar en los próximos tres meses

- Nombramiento de la figura del DPD ☑
- Desarrollo de un Diagnóstico de Situación ☑
- Formación, difusión y capacitación en el RGPD ☒
- Definir una política de privacidad unificada. ☒
- Acuerdo de confidencialidad municipal y externo ☒
- Actualización Política de Seguridad (Roles PD) ☒
- Contenidos tipo RGPD para pliegos, contratos. ☒
- Coletilla legal corporativa e inclusión en impresos. ☒
- Identificar tratamientos de datos personales "ocultos". ☒
- Revisar el uso del dato para que no sea excesivo. ☒
- Datos de menores: revisión de servicios e impresos. ☒
- Identificar datos y tratamientos sensibles ☒
- Actualizar RAT (registro de actividades de tratamiento). ☒
- Obtención del consentimiento ☒
- Renovación de Impresos, formularios y plantillas ☒
- Categorización de los datos tratados ☒
- Desarrollo de un informe de riesgos inicial ☒
- Desarrollar una evaluación de impacto inicial (víctimas, antecedentes, salud, investigaciones, servicios sociales, actuaciones sanitarias de emergencia, etc.) ☒
- Mecanismos "autenticados" ejercicio de derechos. ☒
- Sistemas de Información de soporte por tratamiento ☒
- - -

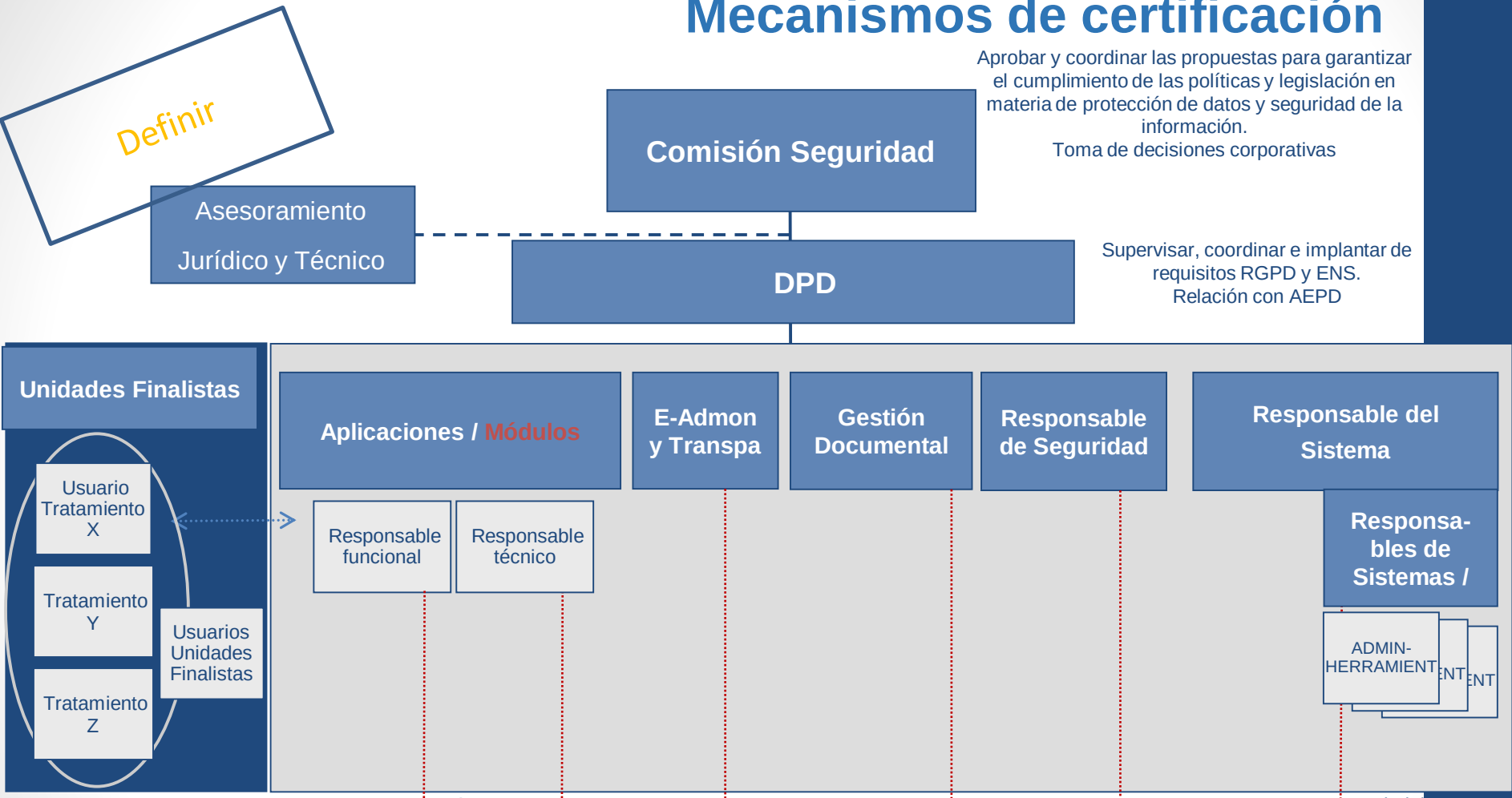
Siguientes pasos

- Medidas de seguridad técnicas /tecnológicas ☒
- Medidas de seguridad organizativas ☒
- Realización de auditorías ☒
- Proc notificación de incidentes de seguridad /Brechas ☒
- Buenas Prácticas y recomendaciones ☒
- Otras actuaciones por determinar ☒

Finalizado
En desarrollo
Pendiente

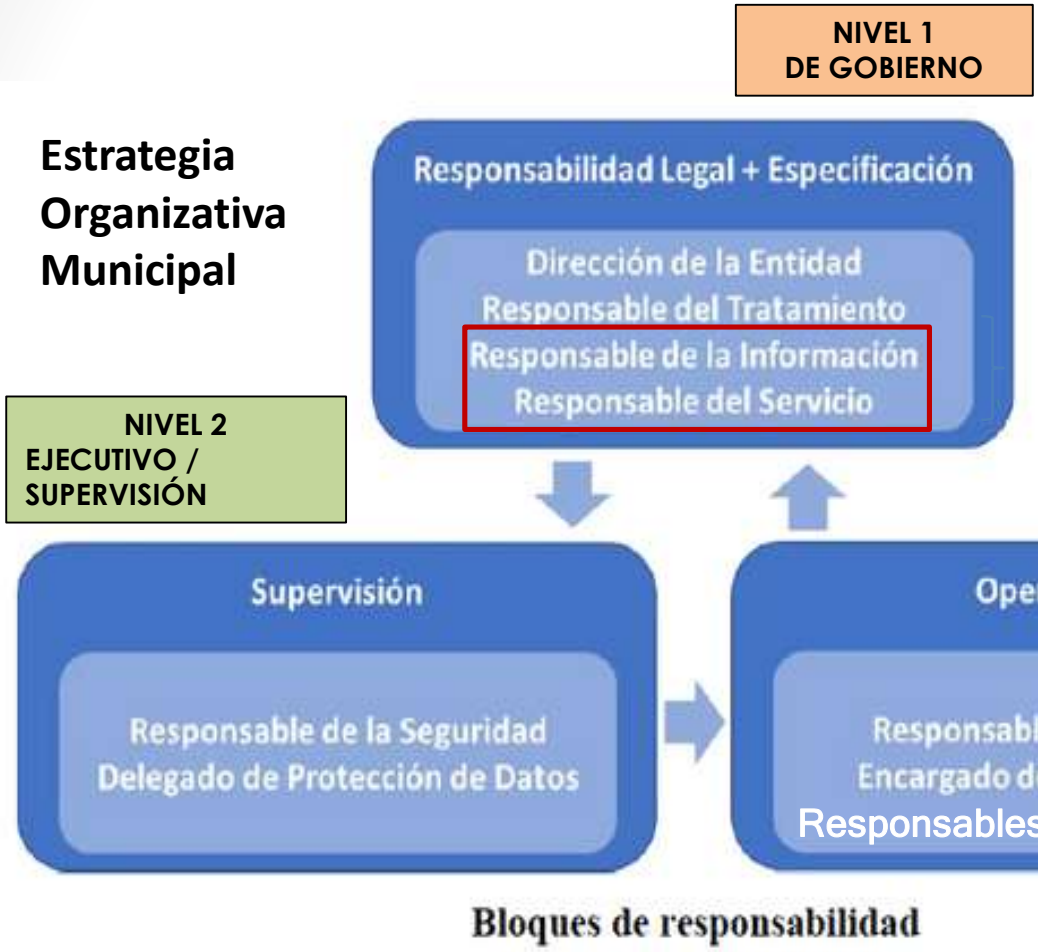
Certificación ENS en dos años

Seguridad en el Tratamiento de Datos Personales
Mecanismos de certificación



Seguridad en el Tratamiento de Datos Personales
Mecanismos de certificación

Estrategia Organizativa Municipal



Bloques de responsabilidad

Alcaldía

Determina los objetivos a alcanzar y responde de que se alcancen

Jefes y Resposables de Órganos y Unidades / Organismos autónomos, establecen los requisitos de su información / servicios

Operaciona

Se centran en una actividad concreta y **controlan cómo se hacen las cosas**.

Seguridad en el Tratamiento de Datos Personales
Mecanismos de certificación

Funciones de los Responsables de Información y Servicios

- Establecer los **requisitos de seguridad** aplicables al Servicio (niveles de seguridad del servicio) y la Información (niveles de seguridad de la información), dentro del marco ENS, RGPD.
- Dictaminar respecto a los **derechos de acceso** a información propia del Servicio.
- **Aceptar los niveles de riesgo** residual.
- Poner en comunicación del Responsable de Seguridad ENS/DPD cualquier variación respecto a la Información y los Servicios de los que es responsable.
- **Aprobación de impresos**, formularios, trámites normalizados.
- Aprobación de cambios en aplicaciones de gestión y servicios en producción (certificación del cambio).
- **Aprobación** publicación trámites, información y servicios en **Sede**.

Seguridad en el Tratamiento de Datos Personales
Mecanismos de certificación

Funciones de los Responsables de Información y Servicios

- Autorizaciones de **emisión de credenciales.**
- Autorizaciones acceso a pasarela de **intermediación de datos**.
- Incorporación de Información al Portal de **Transparencia**.
- Colaborar en el mantenimiento del Registro de Actividades de Tratamiento (**RAT**).
- Identificar los prestadores que traten datos por cuenta del Ayuntamiento y determinar los **contratos de encargados de tratamiento.**
- Dar cumplimiento tramitando, con el asesoramiento del Delegado/a de Protección de Datos, al ejercicio de los derechos de protección de datos.
- Colaborar en la gestión de **brechas de seguridad** en protección de datos cuando afecte a un tratamiento de su área de competencia, contando con el responsable de seguridad, el de sistemas y con el asesoramiento de la Delegada de Protección de Datos.

Seguridad en el Tratamiento de Datos Personales
Mecanismos de certificación

Situación actual Ayuntamiento y Ciudad

- **Actual uso intensivo de las tecnologías:**
  - Inmersos en un proyecto de digitalización integral
  - Implicados en proyectos de alta tecnología
  - Nuestra ciudad dentro del internet de las cosas
- **Escenario de ciberamenazas y conflictos bélicos híbridos sin antecedentes**
  - AAPP Centro de atención
- **Nivel de uso de datos personales sin precedentes**
  - Nivel inusual de datos personales que pueden poner en serio riesgo nuestros derechos y libertades de todos nosotros, y desgraciadamente no sólo en términos de privacidad e intimidad.
- **Incorporación a nuestra entidad de esta cultura de protección tan reglamentariamente y éticamente necesaria.**

Situación actual internacional y normativa

- **Situación Internacional**
  - Cada vez más ataques especializados, dañinos y dirigidos
  - Conflicto bélico que se torna en conflicto cibernético
  - Especial atención en las Administraciones públicas y concretamente en las entidades locales
  - Estrategias europeas de impulso masivo de las TIC (IA, IoT, 5G, Mercado Único Electrónico en la UE)
- **Situación Normativa**
  - DIRECTIVA (UE) 2019/1024 datos abiertos y la **reutilización** de la información del sector público.
  - RD-Ley 24/2021, de 2 de noviembre, de transposición de varias directivas de la Unión Europea, entre ellas 2019/1024.
  - Ley 19/2013, 9 de diciembre, de **transparencia**, acceso a la información pública y buen gobierno.
  - La Ley 39/2015, de 1 de octubre, del **Procedimiento Administrativo Común** de las Administraciones Públicas Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
  - **Esquema Nacional de Seguridad** / Esquema Nacional de Interoperabilidad
  - Reglamento General de Protección de Datos (**RGPD**). / Ley Orgánica de Protección de Datos y Derechos Digitales. / Ley de Protección de Datos relacionados con Infracciones Penales.
  - Reglamento sobre Seguridad de las Redes y Sistemas de la Información.
  - **Reglamento sobre Ciberseguridad.**
  - REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (LEY DE INTELIGENCIA ARTIFICIAL) Y SE MODIFICAN DETERMINADOS ACTOS LEGISLATIVOS DE LA UNIÓN
  - **NIS2 / E-IDAS2 /DORA**

Novedades Legislativas
Gobernanza del Dato

A nivel europeo. Data Governance Act (DGA)

Es la Ley de Gobernanza de Datos de la UE, en vigor desde 2023.

Objetivo:

- Facilitar el intercambio seguro y voluntario de datos.
- Crear un mercado único europeo de datos.
- Regular servicios de intermediación y reutilización de datos protegidos.
  Complementa la DGA, estableciendo normas para el acceso justo y uso adecuado de datos, especialmente industriales.

En España

Política de Gobierno del Dato
Publicada en el BOE (Orden INT/160/2025), en el marco de la Estrategia Europea de Datos y la Agenda España Digital 2026.

Objetivo:

- Situar los intereses de la persona en el centro.
- Garantizar derechos fundamentales y normas europeas.
- Impulsar reutilización segura de datos en el sector público

Novedades Legislativas
Gobernanza del Dato

Ley de Gobernanza del Dato

- Medidas para fortalecer la confianza en el uso compartido de datos, ya que la falta de confianza es actualmente un gran obstáculo y genera altos costes.
- Nuevas normas de la UE sobre neutralidad, que establecen la función novedosa de los intermediarios de datos como organizadores fiables del intercambio de datos.
- Medidas para facilitar la reutilización de determinados datos en poder del sector público.
- Herramientas que permiten a los europeos controlar cómo se utilizan los datos que generan. Esta facilitación y mayor seguridad aumentan la disposición de empresas e individuos a poner voluntariamente sus datos a disposición del bien común en condiciones claras.
- La ley prohíbe la vinculación de los servicios de intermediación con otros servicios como el almacenamiento en la nube o Business Analytics

Datos de calidad, disponibles y seguros

Novedades Legislativas Gobernanza del Dato

Ley de Servicios Digitales

- Regulará anuncios personalizados y a borrar contenido ilegal. Afectará a plataformas e intermediarios en línea, Twitter, YouTube, Spotify,Airbnb y otros mercados digitales (45 millones de usuarios activos mes).
- Se espera asegurar la igualdad de condiciones en el mercado y permita que las pequeñas y medianas empresas puedan tener su espacio y se marque un estándar mundial.
- Los usuarios podrán señalar contenido ilegal, y la plataforma estará obligada a notificarles cualquier decisión. También se establecerá un sistema de indicadores de confianza. Habrá reglas específicas para las grandes plataformas en línea, donde los usuarios podrán evitar el contenido personalizado y se exige más responsabilidad en la desinformación. También permitirá a los usuarios ponerse en contacto con las empresas en caso de que sus cuentas estén bloqueadas, por ejemplo.

Ley de Mercados Digitales

- Limitaciones AL USO en que algunos de estos gigantes tecnológicos pueden utilizar los datos personales de los consumidores, pero en términos de darles el control sobre su propia información personal, se queda corta“
- Los guardianes de acceso conservarán todas sus oportunidades de innovar y ofrecer nuevos servicios. La única diferencia es que no se les permitirá someter a prácticas desleales, para obtener ventajas indebidas, a las empresas y clientes usuarios que dependen de ellos (inferir datos más allá de las finalidades autorizadas, etc.).

Novedades Legislativas Gobernanza del Dato

- **Estrategia Europea de Datos**
  - Convertir a la UE en líder de una sociedad impulsada por los datos.
  - Creación de un mercado único de datos para que fluyan entre sectores, en beneficio de las empresas, investigadores y las administraciones públicas.
  - Mejores decisiones a partir del conocimiento que aportan los datos no personales, que deben estar a disposición de todos.

- **Estrategia de Seguridad Nacional 2021.**
- **Programa Europa Digital [2021-2027]**
  - Supercomputación,
  - Inteligencia artificial,
  - Ciberseguridad,
  - Competencias digitales avanzadas,
  - Generalización del uso de las tecnologías en todos los sectores.

- **NextGenerationEU más que un plan de recuperación es una oportunidad para diseñar una Europa que funcione para todos. Con lemas del tipo:**
  - tecnología 5G y la banda ancha ultrarrápida disponible en toda la UE;
  - identidad digital que te facilitará el acceso a los servicios públicos en línea y te dará un mayor control sobre tus datos personales;
  - ciudades más inteligentes y eficientes;
  - compras en línea seguras;
  - la inteligencia artificial nos ayudará a combatir el cambio climático y a mejorar la asistencia sanitaria, el transporte y la educación.

Novedades Legislativas
Gobernanza del Dato

Los **datos de alto valor** son una serie de conjuntos de datos con un gran potencial para generar “beneficios para la sociedad, el medio ambiente y la economía, en particular debido a su idoneidad para la creación de servicios de valor añadido, aplicaciones y puestos de trabajo nuevos, dignos y de calidad”.

La Directiva recoge 6 categorías de datos a considerar de alto valor: **datos geoespaciales**, de observación de la Tierra y medio ambiente, meteorológicos, **estadísticos**, de compañías y de movilidad.

En España, el rol de añadir nuevas categorías de datos de alto valor recae en la Oficina del Dato con la colaboración de los actores interesados, tanto públicos como privados, según lo especificado en el Real Decreto-ley 24/2021, de 2 de noviembre, de transposición de varias directivas de la Unión Europea, entre ellas la Directiva 2019/1024.

La Oficina del Dato nace con la misión de dinamizar la compartición, la gestión y el uso de los datos a lo largo de todos los sectores de la Economía y Sociedad.

La Economía del Dato tiene cada vez un peso, así mismo, los datos abiertos habilitan el desarrollo de nuevos productos, servicios y soluciones de alto valor socioeconómico.

La reutilización de los documentos será gratuita. No obstante, podrá aplicarse una tarifa, limitándose la misma a los costes marginales en que se incurra para su reproducción, puesta a disposición, difusión, anonimización de datos personales y las medidas adoptadas para proteger información comercial confidencial.

Novedades Legislativas
Reglamento de IA

Objetivos principales

Garantizar que la IA respete derechos fundamentales, seguridad y transparencia.
Clasificar sistemas de IA por niveles de riesgo:

- Riesgo inaceptable → prohibidos (p.ej., manipulación subliminal, puntuación social).
- Alto riesgo → requisitos estrictos (evaluación de conformidad, registro).
- Riesgo limitado → obligaciones de transparencia.
- Mínimo riesgo → sin requisitos adicionales.

Regular modelos de IA de propósito general (incluidos los modelos fundacionales).
Crear la Oficina Europea de IA y un grupo de expertos científicos independientes. [boe.es]

Calendario de aplicación

2 agosto 2024 → Entrada en vigor.
2 febrero 2025 → Prohibición de prácticas de IA de riesgo inaceptable.
2 agosto 2025 → Obligaciones para modelos de IA de propósito general y régimen sancionador.
2 agosto 2026 → Aplicación completa para sistemas de alto riesgo

Nuevos Servicios Municipales
Oficina del Dato

2015-2019	2020-2025
Objetivos LEY 39/2015 LEY 40/2015 Ley 19/2013, RD 1112/2018, Tramitación, Transparencia, accesib. y Protección de Datos (RGPD) RD 14/2019, medidas urgentes seguridad pública en materia de e-administración, **Soluciones** Certificados Dig. Dir3 / Face Registro Común Orve /Notifica	**Objetivos** Nuevos modelos de gestión primando la seguridad y protección de inf. DATA CENTRISMO EXPLOSIÓN EN EL USO INTESIVO DE LOS DATOS **Soluciones** Implementación del ENS (Esquema Nacional de Seguridad) y RGPD (Protección datos) Inteligencia Artificial Data minning (minería de datos)

Ataques a AAPP

Cultura de Protección del Dato

SITUACIÓN ACTUAL ADMINISTRACIÓN ELECTRÓNICA

- DIGITALIZACIÓN INTEGRAL
- REFORMULACIÓN DE PROCEDIMIENTOS TRADICIONALES PARA UNA ÓPTICA SIMPLIFICADORA Y ELECTRÓNICA

SITUACIÓN ACTUAL DEL DATO

- EXISTENCIA DE TRATAMIENTOS OCULTOS
- FALTA DE DISPONIBILIDAD DE DATOS DE PROVEEDORES
- ISLAS DE DATOS EN UNIDADES FINALISTAS
- DATOS PRIMARIOS QUE REQUIEREN DE VALOR AÑADIDO
- INEXISTENCIA DE CUADROS DE MANDO / INDICADORES
- NECESIDAD DE CREAR UNA “OFICINA DEL DATO”

TRANSPARENCIA

- EXISTENCIA DE PORTAL DE TRANSPARENCIA Y DATOS

POLÍTICAS Y BUENAS PRÁCTICAS

- Buenas prácticas en materia de Ética Digital [Pacto Digital]

SEGURIDAD Y PROTECCIÓN DE DATOS

- INCORPORACIÓN DE LA CULTURA DE LA PROTECCIÓN DE DATOS
- INCORPORACIÓN DE LA CULTURA DE LA SEGURIDAD TIC

Nuevos Servicios Municipales
Oficina del Dato

- DIRECTIVA (UE) 2019/1024 datos abiertos y la reutilización de la información del sector público.
- RD-Ley 24/2021, de 2 de noviembre, de transposición de varias directivas de la Unión Europea, entre ellas 2019/1024.
- Ley 19/2013, 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Esquema Nacional de Seguridad / Esquema Nacional de Interoperabilidad
- Ley de Sociedad de la Información y del Comercio Electrónico.
- Ley de Secretos Empresariales.
- Reglamento e-IDAS.
- Reglamento General de Protección de Datos (RGPD).
- Ley Orgánica de Protección de Datos y Derechos Digitales.
- Ley de Protección de Datos relacionados con Infracciones Penales.
- Protección de Infraestructuras Críticas.
- Directiva NIS / Ley de secretos oficiales.
- Ley de Seguridad de las Redes y Sistemas de la Información.
- Reglamento sobre Seguridad de las Redes y Sistemas de la Información.
- Reglamento sobre Ciberseguridad.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Ley de Conservación de Datos en Comunicaciones Electrónicas.
- Reglamento de Evaluación y Certificación de la Seguridad de las TI.
- Ley de Seguridad Privada / Directiva sobre Servicios de Pago.

Asimismo, el artículo 3.2 de la también vigente **Ley 40/2015**, de 1 de octubre, de Régimen Jurídico del Sector Público, señala: *"Las Administraciones Públicas **se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos,** que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados".*

Nuevos Servicios Municipales
Oficina del Dato

- CONSTITUCIÓN DEL DATO ÚNICO
- CONTROL DE LA EXPLOTACIÓN DEL DATO
- OBTENCIÓN DEL DATO DE SERVICIOS EXTERNALIZADOS
- CREACIÓN DE UNA ESTRATEGIA DE SISTEMAS Y DATOS DE ALTO VALOR
- CREACIÓN DE UN ESPACIO PROTEGIDO DE GESTIÓN DEL DATO
- ESPACIO DE TITULARIDAD CIUDADANA DEL DATO
- COLABORAR EN LA GESTIÓN DE LA BRECHA DIGITAL
- COLABORAR EN LA ÉTICA DIGITAL

Nuevos Servicios Municipales
Oficina del Dato

Datos disponibles:

- Crear un lago de datos procedente no solo de ERPs sino de la gestión interna de las unidades (Excel, Access, etc.)
- Obtener datos de los proveedores de servicios que puedan agregarse.

Datos de calidad:

- Disponer de una relación directa entre el dato y su tratamiento.
- Disponer de una oficina del dato que garantiza su normalización, unicidad y legitimidad jurídica.

Datos seguros:

- Nodo securizado / Transmisión y descarga securizada.
- Cifrado homomórfico / APIs de disponibilidad.

Datos de alto valor:

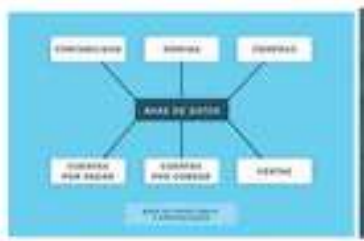
- Cruzar e inferir datos con garantías técnicas y jurídicas

Ejercicio de derechos protección de datos y su gestión centrada de el usuario:

- Exclusivo control de sus datos del interesado / afectado (fuentes autorizadas).
- Autorizacion para la legitimación uso de medios para avisos y comunicaciones
- Ejercicio de derechos de acceso, posición, cancelación, etc. on-line.

Nuevos Servicios Municipales
Oficina del Dato

Linaje de los datos



Datos ERPs | Datos de Gestión | Documentos | Datos de contratas

OFICINA DEL DATO

- Define plantillas para datos no ERP
- Garantiza minimización y calidad
- Garantiza uniformidad
- Garantiza legitimidad
- Garantiza unicidad
- Verifica el metadato
- Audita el dato

Nuevos Servicios Municipales
Oficina del Dato

Nodo Securizado de tratamiento de datos
- ✓ Conexión protegida
- ✓ Entorno protegido

Datos disponibles | Datos de calidad | Datos seguros | Datos de alto valor | Datos centrados en el usuario

- ✓ Datos sensibles
- ✓ Datos confidenciales

Cortar

- ✓ Datos de negocio
- ✓ Datos personales

Anonimizar

- ✓ Datos estadísticos

CUADRO DE MANDO INTEGRAL

Portal de Datos Abiertos

CUADRO DE MANDO INTEGRAL

DATA Y POLITICAS PUBLICAS

Cruces e inferencias de datos y geolocalización

✓ DataSets

- Formatos y datos abiertos
- Legibles por máquina (machine Learning, IA)
- Accesibles
- Fáciles de localizar y reutilizar

- Conservan los metadatos
- Licencias de uso estándar
- Nodo cifrado homomórfico

Nuevos Servicios Municipales
Centro de Excelencia de la IA

1. **Gobernanza y cumplimiento normativo**
    - El nuevo Reglamento Europeo de IA exige controles sobre sistemas de IA de alto riesgo.
    - Las entidades locales necesitan un órgano especializado para garantizar:
        - Inventario y Transparencia en algoritmos.
        - Evaluaciones de impacto en derechos fundamentales.
        - Cumplimiento con RGPD, ENS y la Ley de IA.

2. Reducción de riesgos

- Evita decisiones automatizadas sin supervisión humana (art. 22 RGPD).
- Mitiga riesgos de sesgo, discriminación y errores en servicios públicos (p.ej., asignación de ayudas, selección de personal).

3. **Optimización de recursos**

- Centraliza conocimiento y herramientas para:
    - Análisis de datos.
    - Modelos predictivos para movilidad, energía, servicios sociales.
- Evita duplicidades y reduce costes en municipios pequeños.

4. Innovación y formación

- Capacita al personal en uso ético y seguro de IA.
- Promueve proyectos piloto en áreas como:
    - Atención ciudadana (chatbots).
    - Gestión inteligente del tráfico.
    - Detección temprana de fraude.

Un centro de excelencia actúa como referente técnico y ético, asegurando que la IA se use para mejorar servicios sin vulnerar derechos.

Calidad y exactitud en el tratamiento de datos personales

GOBIERNO DEL DATO

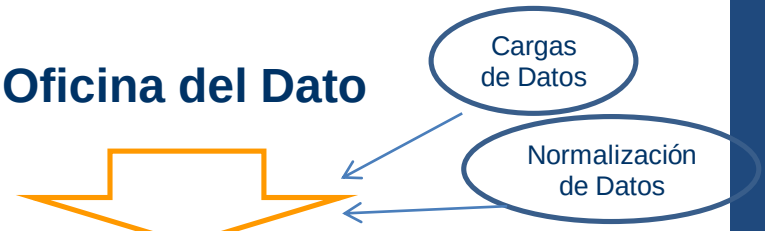
El gobierno del dato permite extraer conocimiento y potenciar el crecimiento inteligente.
Se trata de disponer de datos de calidad, uniformes y compartidos.

El gobierno del dato son las funciones, y normas para el uso eficiente de los datos, y se implementa mediante la definición de un **mapa de datos**, clave para la integración de Sistemas y su interoperabilidad, así como la creación de una unidad especializada para su tratamiento denominada la "**oficina del dato".**

Mapa Datos

Mejora en la calidad de los datos.
Ofrece comprensión compartida de los datos (360º).
Mejora la toma de decisiones.
Permite el cumplimiento normativo uniforme.
Mejora la gestión de datos.

Oficina del Dato



La unidad de Datos tiene entre sus funciones la recopilación, depuración y organización de los datos procedentes de otras entidades o generados internamente.

La gestión de datos se basa en la gestión de los requerimientos del ciclo de vida de los datos, mientras que su gobernanza es la pieza principal de conexión con otras disciplinas, como la gestión de datos maestros, calidad de datos, seguridad de datos, o la gestión de metadatos.

Impacto de la nueva regulación europea sobre la IA en la protección de datos personales

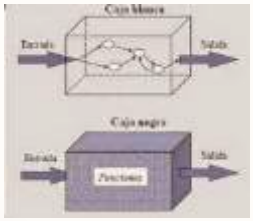
El Reglamento define Sistema de Inteligencia Artificial como aquel que opera con elementos de autonomía y que, basándose en datos y entradas obtenidos de humanos o máquinas, infiere como alcanzar unos objetivos propuestos usando para ello técnicas basadas en el aprendizaje-máquina o en lógica y conocimiento, y genera como salida contenidos, predicciones.

ETIQUETA ATRACTIVA

- **Prohibidos**: puntuación social. Scoring social
- **Alto riesgo**: reclutamiento, formación, ayudas, salud. Permitido con **declaración** de **conformidad** y afectan a la salud, la seguridad o los derechos fundamentales o ya están clasificados tales como dispositivos médicos, los trenes o la maquinaria
- **Riesgo medio**: necesidad de transparencia en el tratamiento. Permitido con req de transparencia.
- **Riesgo mínimo**: sin restricciones

- Sistema de **gestión de riesgos de IA de alto riesgo**, que contemple, en particular, los riesgos sobre la salud, seguridad y derechos fundamentales relacionados con su propósito.
- **Gobernanza y gestión de los datos de entrenamiento y prueba**, asegurando buenas prácticas en su diseño, recolección y preparación, asegurando su relevancia y corrección y sus muestras apropiadas (no sesgos)
- **Documentación técnica actualizada**, que demuestre que se cumplen los requisitos exigidos.
- Disposición de **registros de actividad del sistema.**
- **Información a los usuarios** sobre las capacidades del sistema, requisitos precisión, condiciones de utilización que pueden implicar riesgos, los sistemas para supervisión humana , etc.
- Los sistemas permitirán la **supervisión por personas cualificadas** y toma de control
- Los sistemas proporcionarán un nivel adecuado de **precisión, robustez y ciberseguridad**. Se diseñarán con tolerancia a errores o inconsistencias en su empleo, e incorporarán medidas de ciberseguridad apropiadas en particular de protección contra la manipulación de los datos de entrenamiento.

Certificar el algoritmo de IA por parte como medio para garantizar la transparencia y cumplimiento de la Legislación Europea de Inteligencia Artificial.



RGPD. Responsabilidad proactiva monitorización, auditoría, y trazabilidad de las decisiones tomadas y las acciones realizadas.
COMITÉS DE ÉTICA Y PROTECCIÓN DE DATOS

RGPD. Reidentificación, vinculabilidad, inferencia, anonimización, agrupación, ofuscación, abstracción de datos, distribución de datos, generación, perturbación, datos sintéticos, enmascaramiento

Nuevos Servicios Municipales basados en la IA

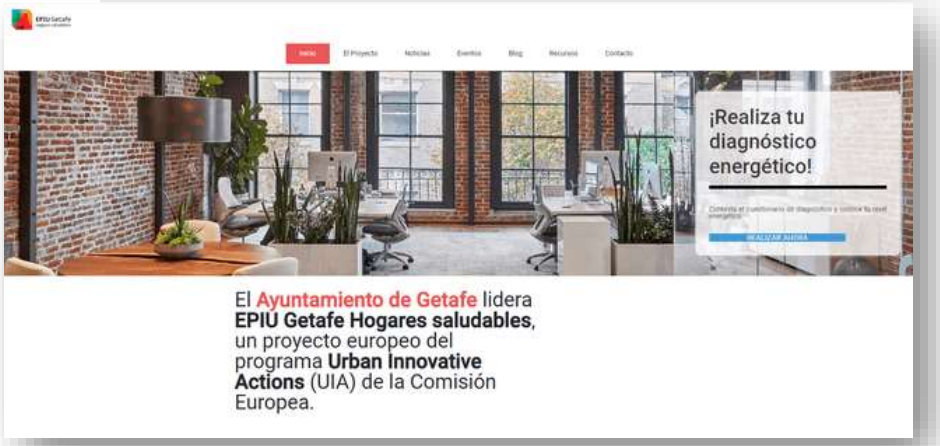
EPIU

MARCO TECNOLÓGICO

Proyecto EPIU- Hogares Saludables. [coletivos especialmente vulnerables]

Detectar necesidades de colectivos vulnerables y luchar contra la pobreza energética oculta.

- ✓ **Herramienta de IA** para detectar vulnerabilidad energética y que sirva de soporte con **supervisión humana** para actuales y futuras ayudas.
- ✓ **Volumen óptimo de datos**, recopilándose los mismos mediante encuestas, datos de tratamientos municipales de los que somos responsables, y encargados.
- ✓ **Lago de datos,** Nodo de ingesta, normalización y anonimización de datos, se encuentra **centralizado en las infraestructuras municipales.**
- ✓ Desarrollo realizado la **Universidad Carlos III de Madrid, socio tecnológico del proyecto** y miembro del cluster, y con el que el Ayuntamiento ha firmado un contrato de protección de datos que le confiere el rol de **encargado de tratamiento**, por lo que el acceso temporal a los datos para realizar el entrenamiento de la herramienta se realiza bajo el RGPD, así como los subencargos de tratamientos con sus contratas .
- ✓ **Medidas de ciberprotección** (anonimización, agrupación, distribución de datos) para evitar la reidentificación, vinculabilidad e inferencia de los titulares del dato.



Preparación del dato
Securización del Dato
Integración de tres orígenes de datos
Información a los afectados

Nuevos Servicios Municipales basados en la IA

Armonización Legislativa

EPIU

MARCO JURÍDICO

LEGISLACIÓN Y NORMAS APLICABLES

Ley 7/1985 de 2 de abril, Reguladora de las Bases del Régimen Local.
Ejercicio de las funciones en el ámbito material conforme al art .27 c) *Prestación de los servicios sociales*, promoción de la igualdad de oportunidades y la prevención de la violencia contra la mujer

Ley 11/2003, de 27 de Marzo, de Servicios Sociales de la Comunidad de Madrid
En la que se establece que corresponde a la Administración de la Comunidad de Madrid y a *sus municipios competencias similares en relación con la prestación de servicios sociales* a las personas sometidas a su ámbito de actuación, y ejerciéndose dichas competencias sobre la base de los principios generales de coordinación y cooperación.

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
En lo relativo al Artículo 141. Deber de colaboración entre las Administraciones Públicas, que indica en su apartado c) "*Facilitar a las otras Administraciones la información que precisen* sobre la actividad que desarrollen en el ejercicio de sus propias competencias o que sea necesaria para que los ciudadanos puedan acceder de forma integral a la información relativa a una materia"

La ley orgánica 6/2001, de 21 de diciembre, de Universidades, regula en su art 10 los Institutos universitarios de Investigación, como centros dedicados a la *investigación científica* y cuya creación es acordada con la Comunidad Autónoma, considerándose por tanto, una función esencial de las Universidades.
La investigación es un derecho y un deber del personal docente e investigador de las Universidades, de acuerdo con los fines generales de la Universidad, y dentro de los límites establecidos por el ordenamiento jurídico.
La investigación científica y técnica *en el ámbito público* se encuentra regulada por la **Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación y por la Ley 5/1998, de 7 de mayo, de Fomento de la Investigación Científica y la Innovación Tecnológica**

INVESTIGACIÓN Y DATOS PERSONALES

Considerando 50 RGDP
El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros.
*Las operaciones de tratamiento ulterior con fines d*e archivo en interés público, *fines de investigación científica* e histórica o fines estadísticos *deben considerarse operaciones de tratamiento lícitas compatibles.* La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior.

Nuevos Servicios Municipales basados en la IA

BINDI

MARCO TECNOLÓGICO

BINDI - UC3M4Safety

Se trata de un **wereable**, que se conecta por bluetooth al móvil. Este dispositivo permite **prevenir situaciones de riesgo** en las mujeres que lo lleven puesto.

Este proyecto es la continuación de un primer **prototipo académico**, que demostró que Bindi era una solución viable, con mejoras en la detección de aquellos episodios de activación de un estado de alerta ante una amenaza.

Bases de datos a partir de pruebas con usuarias en las que se induzca de manera eficaz **estados emocionales** relacionados con situaciones de riesgo.

El proyecto Bindi se enmarca en las iniciativas de la UC3M y Ayuntamiento de Getafe para la realización de los Objetivos de Desarrollo Sostenible; en concreto el ODS 5: Lograr la igualdad entre los géneros y empoderar a todas las mujeres y niñas; en concreto, lo que se refiere a la meta 5.2: Eliminar todas las formas de violencia contra todas las mujeres y las niñas en los ámbitos público y privado, incluidas la trata y la explotación sexual y otros tipos de explotación.

Ayuntamiento de Getafe, firma un convenio en fase **piloto con el fin de verificar la eficacia en circunstancias reales** del citado dispositivo, promoviendo, de tal modo, acciones tendentes a la posible futura implantación de nuevos dispositivos que contribuyan a la protección de mujeres víctimas de violencia de género.

- IA contra el maltrato del mayor
- IA para la protección de personas con movilidad reducida
- Soporte a la toma de decisiones ya que permiten encontrar respuestas en grandes volúmenes de políticas existentes, resumir documentos extensos o sugerir contenidos para su revisión, anonimización, bot de atención ciudadana.

Responsabilidad del Dato
Rol del Ayuntamiento en la fase de Piloto
Análisis de Riesgos y Evaluación Impacto
Cuidado con la elección de la muestra
Consentimiento muy bien informado

Nuevos Servicios Municipales basados en la IA

UITEL

MARCO JURÍDICO

LEGISLACIÓN Y NORMAS APLICABLES

Ley 7/1985 de 2 de abril, Reguladora de las Bases del Régimen Local. Ejercicio de las funciones en el ámbito material conforme al art. 25.2. e) que atribuye competencia al Ayuntamiento para la "evaluación e información de situación de necesidad y la atención inmediata a personas en situación o riesgo de exclusión social" y art .27 c) *Prestación de los servicios sociales*, promoción de la igualdad de oportunidades y la prevención de la violencia contra la mujer

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
En lo relativo al Artículo 141. Deber de colaboración entre las Administraciones Públicas, que indica en su apartado c) "Facilitar a las otras Administraciones la información que precisen sobre la actividad que desarrollen en el ejercicio de sus propias competencias o que sea necesaria para que los ciudadanos puedan acceder de forma integral a la información relativa a una materia"

La ley orgánica 6/2001, de 21 de diciembre, de Universidades, regula en su art 10 los Institutos universitarios de Investigación, como centros dedicados a la investigación científica y cuya creación es acordada con la Comunidad Autónoma, considerándose por tanto, una función esencial de las Universidades.
La investigación es un derecho y un deber del personal docente e investigador de las Universidades, de acuerdo con los fines generales de la Universidad, y dentro de los límites establecidos por el ordenamiento jurídico.
La investigación científica y técnica en el ámbito público se encuentra regulada por la **Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación y por la Ley 5/1998, de 7 de mayo, de Fomento de la Investigación Científica y la Innovación Tecnológica,** considerando que le término científico desde el punto de vista semántico implica pertenencia a una ciencia (ciencias económicas, ciencias de la información).

INVESTIGACIÓN Y DATOS PERSONALES

Considerando 50 RGDP
El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros.
Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior.

Panorama actual de la IA

IMPACTO DE LA IA EN PDP

- **Consentimiento**
- **Minimización de datos**
- **Calidad del Dato.** Los datos serán exactos y actualizados en todo el momento.
- **Privacidad.** PDD desde el diseño y por defecto. Responsabilidad proactiva.
- **Medidas de Seguridad:** ENS según RGPD / LOPDyGDD / Ley 39-40 /2015
- **Transparencia**
- **Análisis de Riesgos y Evaluación de impacto en PDP, salud, seguridad y derechos fundamentales**
- **IAs colaborativas:** cadenas de valor complejas, que implica AR si se integra con otra IA de AR.
- **Ciberataques:** envenenamiento de datos, manipulación del algoritmo-> espacios seguros, Backup datos
- **Ley Europea de Gobernanza de Datos / Ley de Datos / Estrategia Europea de Datos**

Esquema Nacional de Seguridad

Espacios Comunes de Datos y Espacios controlados de pruebas para el desarrollo de las IAs utilizadas en Europa de manera que sean seguras, transparentes, trazables, no discriminatorias y respetuosas con el Medio Ambiente

21 Marzo 2024 | Derechos humanos

Es la primera vez que la Asamblea adopta una resolución para regular este campo emergente. La resolución pide a los Estados que se abstengan de utilizar sistemas de inteligencia artificial que no puedan funcionar de conformidad con las normas internacionales de derechos humanos o los pongan en riesgo.

IAs propias

ACUERDO DE SOCIOS TECNOLOGICOS CON LA UNIVERSIDAD CARLOS III DE MADRID PARA LA CREACIÓN DE UNA OFICINA DEL DATO Y UN CENTRO DE COMPETENCIAS DE IA MUNICIPAL

ACUERDO MARCO CON LA UNIVERSIDAD CARLOS III DE MADRID PARA EL DESARROLLO DE ALGORITMOS DE IA OFRECIENDO DATOS MUNICIPALES COMO ESCENARIO DE PRUEBA

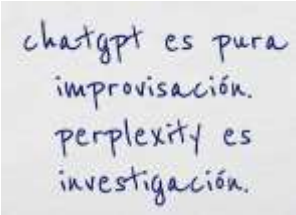
Nuestros Retos

ERRORES EN LA IA y EXCENTES CONDUCTUALES

- **Sesgo en la muestra. Errores de muestreo. Busco altura media en un equipo de baloncesto**
- **Sesgo en la inferencia. Errores de inferencia. Personas obesas tienen falta de vitamina D.**
- **Sesgo de confianza.**
- **Sesgos de persuasión blanda (cambian si les das pena o las adulas)**
- **Algoritmos / Sistemas Expertos / Redes Neuronales**
- **Redes neuronales (no saben nada y fruto del entrenamiento adquieren conocimiento).** A más entrenamiento más corrección y más optimización
- **Reevaluación continua ante comportamientos y resultados inesperados.**
- **Sesgo de conocimiento. Si el universo de prueba son elementos quirúrgicos y se le enseña un alicate, su salida puede ser unas tijeras para retirar vendajes**
- **Inteligencias colaborativas y multimodales**
- **Actuaciones imprevistas**
- **las entrenan a otras las**
- **Prompt (aprender a relacionarte con la IA y a hacerla preguntas)**
- **Alexa reza el padre nuestro / Alexa canta la canción del padre nuestro**
- **Ataques (envenenamiento de datos/ alteración del algoritmo)**
- **las ciberatacantes (no duermen, no descansan)**
- **IoT / 5G Excedentes conductuales, uso extensivo de los datos**
- **Usos previstos / Usos malintencionados (suplantación de identidad. Dime la palabra secreta)**

Nuestros Retos

Y mis dudas



- Si soy más inteligente ¿mi IA será más inteligente ?
- Que ocurre con mi IA entrenada si cambio de entidad o fallezco
- Donde guardo mis datos. Hipoteca Digital
- Con qué datos entreno mi IA
- Con quién y como comparto las IAs desarrolladas y entrenadas
- Como afecta a una IA la localización del entrenamiento
- ¿Afecta a mis resultados el idioma de base del LLM empleado para el entrenamiento en el modelo fundacional?
- ¿IAs colaborativas públicas?
- ¿Podremos obtener de los puntos de interoperabilidad datos masivos?
- ¿Si tengo menos datos de un ciudadano/a le estoy vulnerando su derecho a la igualdad de oportunidades?
- ¿Hace falta un superordenador?
- El derecho de acceso ¿Incluye saber "quién" accedió?

  El RGPD no obliga a dar el nombre individual de cada persona que accedió, pero sí:

  Categorías de destinatarios (p.ej., personal del área de tributos, empresa encargada del software).

  Si hubo cesiones a terceros (p.ej., INE, Seguridad Social).

  Algunas administraciones, por transparencia y trazabilidad, pueden informar del registro de accesos (logs), pero no es un derecho explícito en la norma.

  Excepción

  Si el acceso lo hizo personal interno en el marco de sus funciones, normalmente se informa como "personal autorizado" o "departamento responsable", no con nombres concretos.

Informe EsadeEcPol sobre IA en el sector público español
67 % de los trabajadores públicos podrían mejorar entre el 10 % y el 50 % de sus tareas con IA generativa.
9 % de ocupaciones podrían beneficiarse en más de la mitad de sus tareas.
Estimación: +9 % de productividad por trabajador en la Administración pública tras 10 años.
Valor añadido: 7.000 millones € anuales en España.
Casos de uso: reducción de carga burocrática, mejora de interacción con ciudadanos, agilización de contratación pública.

Dictamen del Comité Europeo de las Regiones (UE)
•La IA puede **aumentar considerablemente la productividad y la competitividad** en servicios públicos locales.
•Áreas clave: **eficiencia energética, transporte, educación, sanidad y atención ciudadana**.
•Subraya que la IA debe aplicarse de forma **transparente, trazable y con supervisión humana** para garantizar derechos fundamentales

¡Gracias por la atención!

EL INFITO VALOR DE LAS PERSONAS

Nuestros datos personales centro de nuestra protección

Mucho por hacer, mucho por aprender

ARÁNZAZU HERRÁEZ

pa.herraez@ayto-fuenlabrada.es