DIRECTRICES SOBRE CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES

ÍNDICE.

Abril de 2026.

DIRECTRICES SOBRE CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS PERSONALES.

1.- NORMATIVA.

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental contemplado en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) que establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

Así mismo, en la Constitución Española de 1978 se consagra este derecho fundamental en el artículo 18.4 al disponer que la "ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Además, la regulación de este derecho fundamental se contiene en:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

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

- Ley 27/2006, de 18 de julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- Ley 8/2018, de 14 de septiembre, de Transparencia, Buen Gobierno y Grupos de Interés del Principado de Asturias.

- Legislación sectorial aplicable a cada tratamiento, en particular:

    - Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del

Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

- Leyes 39 y 40/2015, de 1 de octubre, de Procedimiento Administrativo Común y de Régimen Jurídico del Sector Público.
- Ley 2/1995, de 13 de marzo, sobre régimen jurídico de la Administración del Principado de Asturias.

2.- DEFINICIONES.

DATOS PERSONALES: toda información sobre una persona física identificada o identificable (el interesado). Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

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

ELABORACIÓN DE PERFILES: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

FICHERO: todo conjunto estructurado de datos personales.

ANONIMIZACIÓN: el proceso de convertir los datos en una forma en que no se pueda identificar a individuos. La anonimización genera un único conjunto de datos anónimos.

SEUDONIMIZACIÓN: tratamiento de datos personales de manera tal que sea difícil de atribuir estos a una persona específica sin requerir información adicional. La seudonimización genera dos conjuntos de datos: la información seudonimizada y la información adicional que permite revertir la seudonimización.

BLOQUEO DE DATOS: Cese de la explotación y retirada de datos de los sistemas cuando no son necesarios, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas.

RESPONSABLE DEL TRATAMIENTO: la persona física o jurídica, autoridad pública, servicio u otro organismo que determine los fines y medios del tratamiento. En nuestro caso, la Presidencia del Consorcio de Aguas de Asturias.

ENCARGADO DEL TRATAMIENTO: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. En el Consorcio serán todas las empresas que contraten con la entidad o medios propios de la Administración, cuya prestación requiera el tratamiento de datos personales.

VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES: toda operación que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

DELEGADO DE PROTECCIÓN DE DATOS: es la persona encargada de supervisar y comprobar, de forma confidencial e independiente, si se está cumpliendo con la normativa de protección de datos personales en el seno de una organización. Su función es asesorar, velar y garantizar que los responsables del tratamiento cumplan sus obligaciones de protección de datos y que los interesados estén informados de sus derechos y obligaciones.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO (RATS): cada responsable llevará un registro de las actividades de tratamiento realizadas bajo su responsabilidad, en el que conste, entre otros, los fines del tratamiento y los plazos previstos para la supresión.

3.- BASES JURÍDICAS Y PRINCIPIOS DE TRATAMIENTO DE LOS DATOS PERSONALES.

El tratamiento de datos personales sólo puede realizarse si es lícito y se cumple el RGPD.

En el caso de las administraciones públicas la base jurídica del tratamiento se encuentra en el cumplimiento de una obligación legal o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (apartados c) y e) del artículo 6 RGPD)

Sólo en supuestos excepcionales y no relacionados con las funciones y competencias del Organismo la base jurídica será el consentimiento libre e informado (apartado a) artículo 6 RGPD).

El RGPD señala un conjunto de principios que los responsables y encargados del tratamiento deben observar al tratar datos personales:

- Principio de "licitud, transparencia y lealtad", que consiste en que los datos deben ser tratados de manera lícita, leal y transparente para el interesado.

- Principio de "finalidad" que implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.

- Principio de "minimización de datos", es decir, aplicar medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento reduciendo, la extensión del tratamiento, limitando a lo necesario el plazo de conservación y su accesibilidad.

- Principio de "exactitud", que obliga a los responsables a disponer de medidas razonables para que los datos se encuentren actualizados, se supriman o modifiquen sin dilación cuando sean inexactos con respecto a los fines para los que se tratan.

- Principio de "limitación del plazo de conservación" que constituye una de las materializaciones del principio de minimización. La conservación de esos datos

debe limitarse en el tiempo al logro de los fines que persigue el tratamiento. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados, bloqueados o, en su defecto, anonimizados, es decir, desprovistos de todo elemento que permita identificar a los interesados.

- Principio de "seguridad" que impone a quienes tratan datos el necesario análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten.

- Principio de "responsabilidad activa" o "responsabilidad demostrada" que obliga a los responsables a mantener diligencia debida de manera permanente para proteger y garantizar los derechos y libertades de las personas físicas cuyos datos son tratados en base a un análisis de los riesgos que el tratamiento representa para esos derechos y libertades, de modo que el responsable pueda, tanto garantizar como estar en condiciones de demostrar que el tratamiento se ajusta a las previsiones del RGPD y la LOPDGD.

4.- MEDIDAS DE SEGURIDAD INFORMÁTICA.

Con independencia de lo señalado en la Política de Seguridad de la Información del Consorcio, en relación con la protección de datos de carácter personal, debe observarse lo siguiente:

4.1. USO DE EQUIPOS INFORMÁTICOS

1. El Consorcio facilita a los usuarios los equipos informáticos, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Por ello, los datos, dispositivos, programas y servicios informáticos corporativos sólo deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales.

2. Salvo el caso de aplicaciones de servicios compartidos de la Administración, u otras corporativas del Consorcio, únicamente el personal del Servicio de Sistemas de Información e Infraestructuras (Servicio SII) o autorizado por este podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos informáticos o de comunicaciones, especialmente en aquellos aspectos que puedan repercutir en la seguridad y privacidad de los sistemas de información del Consorcio de Aguas. Cuando se precise instalar dispositivos no provistos por CADASA, deberá solicitarse autorización previa al Servicio SII.

3. Los usuarios son responsables de los equipos que les han sido asignados tanto si lo son en uso exclusivo como compartido. Su protección física y buen uso será su responsabilidad y deberán participar en su cuidado avisando de cualquier necesidad al Servicio SII.

4. Los dispositivos estarán bajo la custodia del usuario que los utilice, que deberá adoptar las medidas necesarias para evitar daños o su sustracción, así como el acceso a ellos por parte de personas no autorizadas o ajenas a la entidad.

5. El cese de actividad de cualquier usuario debe ser comunicado de forma inmediata al Servicio SII al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por la entidad estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente a su responsable cuando finalice su vinculación con dicho puesto o función.

4.2. SEGURIDAD INFORMÁTICA.

La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera vertiginosa, en particular con el uso cada vez más generalizado de la Inteligencia Artificial (IA). La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades.

Por ello:

1. Los empleados públicos tendrán acceso a los sistemas de información y a las bases de datos del Consorcio en función de la necesidad de conocer que precisen para realizar sus funciones, valorada por el Jefe/a de Servicio o la Gerencia y de acuerdo con la política de seguridad establecida.

2. El usuario debe ser consciente del volumen de amenazas actual provocadas por malware y que muchos virus y troyanos requieren de la participación de los usuarios para propagarse, ya sea con la apertura de adjuntos, clics en los enlaces de correo o webs, o usando unidades externas (USB, discos externos, CD/DVD, etc.)

3. Los usuarios deberán notificar al personal de Servicio SII, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal (sobremesa, portátiles tablets o dispositivos móviles), especialmente cuando

existan sospechas de que se haya producido algún incidente de seguridad en el mismo.

4. El usuario será responsable de toda la información extraída fuera de la organización a través de correo electrónico, entornos web o dispositivos tales como memorias USB, CD, DVD, etc. También lo será de toda aquella información en formato papel digitalizada. Es imprescindible actuar de forma responsable, especialmente en relación con la información sensible, confidencial o protegida.

5. En ningún caso se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por la entidad, especialmente aquellas relacionadas con la seguridad.

6. En general, no deben utilizarse los recursos telemáticos del Consorcio, aplicaciones, correo, Internet, etc. para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario, así como introducir contenidos carentes de utilidad para la actividad de CADASA.

7. No se debe almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento, compartidos o locales.

8. El Consorcio proporciona un acceso seguro mediante pasarela VPN (red privada virtual) a los datos del usuario en el sistema para los accesos que se realicen fuera de las instalaciones de la organización, particularmente en situación de teletrabajo.

9. Cuando se utiliza la mensajería electrónica para las funciones del trabajo no deben enviarse datos considerados confidenciales o de carácter personal.

10. El acceso a la información es personal y las credenciales de acceso, intransferibles. Se debe bloquear la sesión cuando se abandone el puesto de trabajo, bien temporalmente o bien al finalizar la jornada de trabajo, para impedir la visualización de los datos personales o evitar que ninguna persona pueda hacer un mal uso de las credenciales.

11. Las credenciales de acceso no han de estar a la vista en notas (post it) o al alcance de terceros.

4.3. IMPRESIÓN Y DIGITALIZACIÓN.

Toda la seguridad que se aplica a un sistema automatizado en el acceso a la información desaparece tras la impresión de esta en papel. El papel genera, si no se observan las medidas de seguridad adecuadas, un elevado riesgo de posibles accesos no autorizados y pérdida de privacidad y seguridad.

1. La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que solo tenga acceso a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

2. Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras de la entidad de forma que no sea recuperable la información que pudieran contener.

3. Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida.

4. El usuario será responsable de recoger los originales del escáner, una vez finalizado el proceso de digitalización.

5. No debe depositarse en papeleras o contenedores de basura y/o reciclaje cualquier soporte informático o información en soporte papel que contenga datos de carácter personal o confidencial sin haberlos previamente destruido de forma ilegible e irrecuperable, en el caso de soportes, o con el uso de trituradoras de corte adecuado, en el caso del papel.

6. Política de escritorio limpio. No debe dejarse encima de las mesas ni en estanterías y bandejas, documentos con contengan información con datos personales.

5.- USO DEL CORREO ELECTRÓNICO CORPORATIVO.

El uso del correo electrónico conlleva una serie de elevados riesgos para la seguridad y privacidad de la información porque:

- La dirección de correo electrónico puede constituir en sí misma un dato personal ya que puede identificar a la persona.
- Proporciona una vía sencilla de divulgación de información confidencial o de carácter personal.
- Es una vía de entrada de malware (cualquier programa diseñado para dañar los sistemas informáticos o sus usuarios).

Por ello, aparte de las medidas de seguridad establecidas por el Servicio SII, debe tenerse en cuenta lo siguiente:

1. En general, se limitarán los envíos por correo electrónico que contengan datos de carácter personal a lo mínimo imprescindible. En estos casos, si se trata de documentos a enviar fuera de la organización, deberá mencionarse lo siguiente:

   "Este mensaje va dirigido, de manera exclusiva, a su destinatario y contiene información confidencial y sujeta al secreto profesional, cuya divulgación no está permitida por Ley. En caso de haber recibido este mensaje por error, le rogamos que, de forma inmediata, nos lo comunique mediante correo electrónico remitido a nuestra atención y proceda a su eliminación, así como a la de cualquier documento adjunto al mismo.
   Asimismo, le comunicamos que la distribución, copia o utilización de este mensaje, o de cualquier documento adjunto al mismo, cualquiera que fuera su finalidad, están prohibidas por el Reglamento (UE) 2016/679 General de Protección de Datos".

2. Se debe prestar especial atención a los destinatarios de correo a fin de evitar errores en el envío de información y asegurar también que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.

3. Sólo se deben remitir correos a los interesados en el asunto, evitando en lo posible copias de cortesía por sistema o el uso de "responder a todos" cuando no es necesario por el contenido del mensaje.

4. Si consideramos que además del destinatario del correo, algunas personas simplemente han de tener constancia del envío de la comunicación, se ha de utilizar el campo CCO (copia oculta) del correo, para que su dirección no sea visible.

5. También se utilizará el campo CCO cuando exista un número elevado de destinatarios, sobre todo, en el caso de direcciones de correo de fuera de la organización.

6. En el caso de contratos o encargos, la remisión de correos electrónicos a personal externo del Consorcio sólo debe realizarse por los responsables de los contratos y encargos, sin que el resto del personal de CADASA deba relacionarse directamente con los empleados de empresas externas.

6 – USO DE LA INTELIGENCIA ARTIFICIAL.

Resulta de aplicación el artículo 6 de la Ley 2/1995, de 13 de marzo, sobre régimen jurídico de la Administración del Principado de Asturias, que dispone lo siguiente

> **Artículo 6 sexies. Inteligencia artificial y procedimiento administrativo.**
>
> 1. La Administración del Principado de Asturias dará debida publicidad y transparencia al uso de inteligencia artificial en el ejercicio de sus funciones. Serán públicos el procedimiento de calidad y uso responsable de inteligencia artificial que, en el marco de sus competencias, esta establezca, los riesgos que implica y cualesquiera otros aspectos que garanticen los derechos de los interesados.
>
> 2. Las normas que regulen los procedimientos administrativos harán, en su caso, referencia expresa a la posibilidad de uso de sistemas de inteligencia artificial en la fase que corresponda, tanto en la asistencia en la presentación de solicitudes, declaraciones responsables o comunicaciones, la comprobación o verificación de los requisitos como en la toma de decisiones.

3. Todo procedimiento que prevea el uso de inteligencia artificial como asistencia al mismo fijará el órgano responsable a efectos de impugnaciones.

Dado el impacto del uso de la IA y los riesgos que conlleva será necesaria la autorización previa del Consorcio para su utilización en los procedimientos administrativos que se tramiten, y en el caso de utilizar esta tecnología no se introducirán datos de carácter personal o de las empresas contratistas del Consorcio.

7.- MEDIDAS DE PROTECCIÓN DEL TRATAMIENTO DE DATOS PERSONALES Y DEBER DE SECRETO.

El Consorcio de Aguas de Asturias es el responsable del tratamiento de los datos conforme al RGPD, siendo el máximo responsable la personal titular de la Presidencia del Consorcio en cada momento.

La entidad va a proceder a designar un delegado de protección de datos (DPD) que se encargará de informar y asesorar al responsable, así como a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos.

El contacto del DPD es dpd@consorcioaa.com

En relación con la protección de los datos personales, los empleados del Consorcio han de conocer y observar lo siguiente:

1. El Consorcio de Aguas de Asturias garantiza el secreto profesional de quienes intervienen en el tratamiento de los datos, así como el respeto a la intimidad personal y familiar de los interesados, entendida como un derecho fundamental de los mismos.

2. Los empleados públicos tienen el deber de guardar secreto en las materias cuya difusión esté prohibida legalmente y han de mantener la debida discreción sobre aquellos asuntos que conozcan por razón de su cargo (artículo 53.12 TREBEP).

3. Todos los interesados en los procedimientos tienen derecho a acceder, rectificar, suprimir, limitar u oponerse al tratamiento de sus datos.

4. Se debe facilitar a los interesados toda la información sobre el tratamiento y derechos sobre sus datos de carácter personal, de una forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

5. Con carácter general, no se cederán datos a terceros, salvo obligación legal. Las cesiones para finalidades concretas han de estar reflejadas en el registro de actividades de tratamiento.

6. Cada uno de los empleados es responsable de la confidencialidad de la información que produce y de prevenir la salida de información no autorizada del sistema. El usuario que genera la información es responsable de asegurar su custodia.

7. Se debe informar al DPD sin dilación indebida sobre cualquier evento que pueda afectar a la seguridad y privacidad de los datos de carácter personal.

8. Sólo se ha de almacenar aquella información que sea estrictamente necesaria y será imprescindible borrar la que ya no es de utilidad. Se ha de revisar, y en su caso, eliminar la información que se guarda en el correo electrónico, en documentos propios y en las carpetas propias y compartidas, etc. Esta norma obedece tanto a un uso eficiente de los recursos como de cumplimiento normativo a fin de limitar el plazo de conservación de los datos de carácter personal y borrar los ficheros temporales que hayan perdido su finalidad.

9. Los empleados serán responsables de asegurar el borrado de aquellos soportes de uso propio que hayan utilizado para almacenamiento temporal y muy especialmente si la información que contenían era confidencial.

10. En las resoluciones administrativas que deban notificarse o comunicarse, se identificará a los interesados con el nombre y apellidos. Sólo cuando sea imprescindible incluir el documento nacional de identidad, se consignarán los dígitos en las posiciones cuarta a séptima del documento, sustituyendo el resto por asteriscos (ej.: ***4567**), conforme a la orientación conjunta de las autoridades de protección de datos de marzo de 2019.

11. Las fotografías y videos que se tomen que incluyan datos de carácter personal han de realizarse exclusivamente para fines relacionados con el cumplimiento de una obligación legal o en el ejercicio de poderes públicos competencia del Consorcio, y realizarse desde un terminal o dispositivo corporativo.

8.- REGISTRO DE ACTIVIDADES DE TRATAMIENTO.

El Consorcio ha de llevar un registro de las actividades de tratamiento realizadas bajo su responsabilidad.

Dicho registro debe contener toda la información indicada a continuación:

1. el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
2. los fines del tratamiento;
3. una descripción de las categorías de interesados y de las categorías de datos personales
4. categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales
5. en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, la documentación de garantías adecuadas;
6. cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
7. cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad

El Consorcio ha realizado el registro de las actividades de tratamiento que realiza, aprobado por la resolución número 2020/614 de 25/11/2020 de la Presidencia (expediente CAA/2019/491), y publicadas en el portal de transparencia del Consorcio de Aguas, en el documento: “Registro de actividades de tratamiento (RT)”

https://consorcioaa.com/wp-content/uploads/2020/12/RESOLUCION-2020_614-Y-DOCUMEN.pdf

Son las siguientes:

1. RAT-01-001 Gestión de personal.
2. RAT-01-002 Seguridad de las instalaciones
3. RAT-01-003 Selección del personal.
4. RAT-01-004 Prevención de riesgos laborales.
5. RAT-01-005 Seguridad de la información.
6. RAT-01-006 Protección de datos personales (Brechas y ejercicio de derechos ARSOLP)
7. RAT-01-007 Agenda de contactos.
8. RAT-01-008 Contratación.
9. RAT-01-009 Gestión presupuestaria contabilidad y tesorería.
10. RAT-01-010 Archivo.
11. RAT-01-011 Servicios de atención al ciudadano.
12. RAT-01-012 Actividades de promoción y divulgación.
13. RAT-01-013 Órganos de gobierno y administración.
14. RAT-01-014 Registro.
15. RAT-01-015 Servicio de saneamiento y abastecimiento.

Cada Servicio deberá elaborar y tramitar, en colaboración con el Delegado de Protección de Datos (DPD) del Consorcio, la publicación del registro de actividades de los nuevos tratamientos que efectúe, así como verificar el cumplimiento de la normativa sobre protección de datos antes del inicio del tratamiento.

Así mismo, ha de realizar las actualizaciones y modificaciones de los RAT correspondientes a sus funciones, en el momento en que sea preciso.

9.- ENLACES DE INTERÉS

- Seguridad de la información Principado de Asturias.

  https://miprincipado.asturias.es/ast/seguridad-informacion

- Agencia Española de Protección de Datos.

  https://aepd.es - https://www.aepd.es/guias-y-herramientas/guias