



**REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y LOPDGGD**  
**Reglamento UE 2016/679, del Parlamento Europeo y del Consejo, de 27 de Abril de 2016 (RGPD) y Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGGD)**

**REGISTRO DE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL (Art.30 RGPD)**

**TRATAMIENTO**

**A1. Nombre del Tratamiento:** *Identificación del tratamiento de datos de la organización (pej: Personal, Clientes, Proveedores, Videovigilancia, ...)*

**CLIENTES Y USUARIOS**

**B1. Identificación del Responsable y Contacto DPO:** *Identificación de entidad responsable de tratamiento y (en su caso) datos contacto DPO nombrado*

**AUTORIDAD PORTUARIA DE AVILÉS**

**dpo@puertoaviles.es**

**C1. Tipificación/Descripción de la Finalidad/es:** *Especificar finalidad/es del Tratamiento y Usos previstos*

• Uso interno, gestión comercial, relacional, operativa, administrativa, económica y contable derivada de la prestación de servicios de la Autoridad Portuaria de Avilés. La relación actualizada de servicios de la Autoridad Portuaria de Avilés está a su disposición en [www.puertoaviles.es](http://www.puertoaviles.es)

• Gestión de los servicios y de los requisitos contractuales y normativos vinculados al servicio solicitado.

• Envío de comunicaciones comerciales sobre productos o servicios similares a los prestados por parte de la Autoridad Portuaria de Avilés, legitimados conforme al artículo 21 la LSSICE.

• El contacto y envío de comunicaciones personales, encuestas, invitaciones a eventos, así como para informarle periódicamente de novedades, noticias e información corporativa y propuestas de otros proyectos y servicios de la organización\* que pudieran ser de su interés tanto por medios escritos, telefónicos como electrónicos a través de los medios de comunicación facilitados, en la medida en que nos lo hubiera consentido.

• Promoción y Difusión de la Organización: La publicación en medios de comunicación corporativos y/u otros medios de comunicación pública, de material gráfico que puede contener su imagen y/o referencia asociada a los servicios que le hemos prestado como caso de éxito, material promocional, de justificación de solvencia técnica y/o justificación en eventos, proyectos y subvenciones en los que participe la organización, en la medida en que lo hubiera consentido.

• Contacto con el interesado a través de los medios de comunicación facilitados (mail, dirección postal y/o teléfono) a fin de gestionar las consultas que nos haga llegar a través de los canales habilitados a tal efecto, gestionar avisos y coordinar actuaciones derivadas de la prestación de servicios por parte de personas relacionadas con la Autoridad Portuaria de Avilés y/o por encargados de tratamiento relacionados con el mismo para las finalidades legitimadas y/o consentidas.

• Gestión de la seguridad y salud (prevención de riesgos laborales) y evaluación de cumplimiento: Coordinación de Actividades Empresariales

• Control y registro de Visitas y Videovigilancia de las instalaciones, así como de la seguridad y el cumplimiento normativo en las mismas, preservar la seguridad de las personas y bienes e instalaciones, así como para el ejercicio de las funciones de control de los trabajadores previstas en el artículo 20.3 del Estatuto de los Trabajadores y normativa de función pública, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercibimientos o sanciones por incumplimientos de normas de seguridad.

• Atención a sus consultas y solicitudes: Gestión de Respuesta a Consultas, Reclamaciones o Incidencias, Solicitudes de Información, Recursos y/o de Actividades.

• Control de calidad sobre nuestros servicios, gestión de la calidad de procesos, instalaciones y actividades, realización de encuestas de opinión, así como la evaluación de los resultados de satisfacción/percepción y rendimiento de los grupos de interés de la organización.

• Gestión del Cumplimiento Normativo (normativa aplicable así como normativa interna de obligado cumplimiento): Investigación, monitorización y auditoría de controles establecidos para la prevención de delitos pudiendo establecerse los controles de acceso a las instalaciones, así como los controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normativa, delitos o comportamientos ilícitos.

• Fines estadísticos e históricos que nos permitan mejorar la estrategia de mejora de los servicios de la Autoridad Portuaria de Avilés.

• Consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo a través de la consulta de los sistemas de exclusión publicitaria publicados por la autoridad de control competente.

\* Inclusión en los sistemas de canal de denuncias de los datos asociados a la puesta en conocimiento (incluso de forma anónima) de la comisión en el seno de la organización o en la actuación de terceros que contratasen con ella, de actos

**D1. Base Legitimadora:** *Especificar Base de Licitud de Tratamiento (Art.6.1 RGPD). La legitimación del tratamiento de Los datos personales se realiza por ser necesario para:*

**Si** RGPD: 6.1.b) La ejecución de un contrato o relación negocial: La gestión de la solicitud de prestación del servicio de la Autoridad Portuaria de Avilés

**Si** RGPD: 6.1.c) Cumplir con una obligación jurídica: (normativa de régimen económico y de prestación de servicios de los puertos de interés general y legislación de transparencia, acceso a la información pública y buen gobierno) y la misión de interés público otorgada por la Ley de Puertos del Estado y de la Marina Mercante: Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por Real Decreto Legislativo 21/2011, de 5 de septiembre. Asimismo, la obtención de la autorización para el servicio aquí definido es necesaria para la explotación, por aquellos operadores autorizados por la Autoridad Aduanera, de los almacenes de depósito temporal (ADT) o de los otros lugares autorizados para depósito temporal (OLADT), conforme a lo establecido en el Código Aduanero Comunitario (CAU), aprobado por el Reglamento (UE) nº952/13 del Parlamento Europeo y del Consejo de 9 de octubre de 2013. Coordinación Actividades Empresariales conforme a normativa de Prevención de Riesgos Laborales (R.D. 171/2004).

**Si** RGPD: 6.1.e) Cumplir una misión de interés público: misión de interés público otorgada por la Ley de Puertos del Estado y de la Marina Mercante: Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por Real Decreto Legislativo 21/2011, de 5 de septiembre

**Si** RGPD: 6.1.f) RGPD: 6.1.f) Satisfacer un interés legítimo del Responsable: Tratamiento de datos como partes de una relación comercial y/o contrato, que sean necesarios para su mantenimiento o cumplimiento, publicación de datos con fines de transparencia y responsabilidad, marketing directo, prevención del fraude, supuestos de interés legítimo en los que el responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos del incumplidor a terceros a fin de gestionar el cumplimiento normativo y la defensa de los intereses del responsable de tratamiento, fines de videovigilancia como interés legítimo de la organización en la protección de sus activos, el interés legítimo de marketing directo habilitado por la LSSICE (envío de comunicaciones comerciales sobre productos o servicios similares a los contratados por el cliente con el que exista una relación contractual previa), así como supuestos de interés legítimo de tratamientos específicos contemplados en la LOPDGGD: Artículo 19. Tratamiento de datos de contacto y de empresarios individuales; Artículo 20. Sistemas de información crediticia; Artículo 22. Tratamientos con fines de videovigilancia; Artículo 23 Sistemas de exclusión publicitaria; Artículo 24 Sistemas de información de denuncias internas.

**Si** RGPD: 6.1.a) Cumplir las finalidades del tratamiento por consentimiento inequívoco del interesado: Su consentimiento inequívoco a través de la aceptación de las cláusulas establecidas de consentimiento habilitadas en el documento base que haya regulado la relación de contacto con la Autoridad Portuaria de Avilés:  
 La comunicación de Los datos personales en relación con las finalidades del tratamiento a los siguientes autorizados:  
 D/D': ..... - con NIF ..... - medio contacto/teléfono: .....  
 • El contacto y envío de comunicaciones personales, encuestas, invitaciones a eventos, así como para informarle periódicamente de novedades, noticias e información corporativa y propuestas de otros proyectos y servicios de la organización que pudieran ser de su interés tanto por medios escritos, telefónicos como electrónicos a través de los medios de comunicación facilitados.  
 • La publicación en medios de comunicación corporativos y/u otros medios de comunicación pública, de material gráfico y/o referencia asociada a los servicios que le hemos prestado como caso de éxito, material promocional, de justificación de solvencia técnica y/o justificación en eventos, proyectos y subvenciones en los que participe la organización.

**E1. Origen y Procedencia de los Datos:** *Especificar fuente u origen de los datos de carácter personal que conforman el tratamiento*

**Si** El propio interesado o su representante legal

**Si** Terceros con los que el responsable de tratamiento mantiene de una relación negocial o de prestación de servicios y para lo cual ha de disponer de Los datos personales personales a fin de tramitar o gestionar su acceso, incorporación al proceso/servicio objeto y/o para cumplir con nuestros compromisos organizacionales y obligaciones normativas asociados al servicio objeto de prestación y/o para la verificación del cumplimiento normativo bajo responsabilidad de la organización (pej, datos personales de beneficiarios, trabajadores y/o terceros vinculados a entidades que reciben servicios de la Autoridad Portuaria de Avilés).

**F1. Colectivo/s de Interesados :** *Identificación del colectivo/s del que se tratan datos*

Personas físicas y representantes legales y/o personas de contacto de entidades que hacen uso de los servicios comerciales de terceros dentro del APA o del propio APA.  
 Representantes legales y/o personas de contacto de Concesionarios autorizados a los que se les cobra una tasa por ocupación

**G1. Estructura de Datos Personales:** *Especificar Tipología de Datos objeto de tratamiento*

| Si | Categoría de Datos objeto de tratamiento  | Especificación   |
|----|---|--|
| No | Categorías especiales de datos personales: <i>datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física</i> | No contiene datos sensibles, salvo en los casos en los que el titular sea beneficiario de condiciones especiales y haya de facilitar registros que permitan acreditar o justificar el cumplimiento de dicha condición. Los datos que pudieran derivarse de posibles incumplimientos que pudieran incorporar datos relativos a condenas e infracciones penales estarían incorporados en el tratamiento "Infractores". Los datos potencialmente sensibles relativos a incidentes, accidentes o daños recibidos o causados por la Autoridad Portuaria estarían incorporados en el tratamiento "Incidencias y Responsabilidad Patrimonial" |
| Si | Datos identificativos: Nombre y apellidos, NIF/DNI, N° Seguridad Social / Mutualidad, Imagen/Voz, Firma, Datos huella parcial, Dirección, Teléfono particular, Dirección correo particular, Otros datos de carácter identificativo  | Datos de carácter identificativo (DNI/NIF, nombre y apellidos, dirección, teléfono)  |
| Si | Circunstancias sociales: <i>Características de alojamiento, vivienda, Situación militar, Propiedades o posesiones, Aficiones y estilo de vida, Pertencencia clubes o asociaciones, Licencias, permisos, autorizaciones, Otros datos de circunstancias sociales</i>  | Circunstancias sociales, (licencias/permisos/autorizaciones/actividades y negocios, licencias comerciales)   |
| Si | Información Comercial: <i>Actividades y Negocios, Licencias Comerciales, Suscripciones a publicaciones / medios de comunicación, Creaciones artísticas, literarias, científicas o técnicas, Otros datos de información comercial</i>  | Información comercial  |
| Si | Económicos, financieros y de seguros: <i>Ingresos, rentas, Inversiones, bienes patrimoniales, Créditos, préstamos, avales, Datos bancarios, Planes de pensiones, jubilación, Datos económicos de nómina, Datos deducciones impositivas/impuestos, Seguros, Hipotecas, Subsidios, beneficios, Historial créditos, Tarjetas crédito, Otros datos económicos, financieros y de seguros</i>   | Datos económicos y financieros (datos bancarios)   |
| Si | Transacciones de bienes y servicios: <i>Bienes y servicios suministrados por el afectado, Bienes y servicios recibidos por el afectado, Transacciones financieras, Compensaciones / Indemnizaciones, Otros datos de transacciones de bienes y servicios</i>   | Transacciones de bienes y servicios.   |

**H1. Sistema de Tratamiento:** *Especificar método de tratamiento de la información*

**Si** Mixto: Soporte papel, soporte informático/magnético.

**I1. Cesión o comunicación de datos:** *Especificar entidades destinatarias a quienes se ha comunicado o van a comunicarse los datos de carácter personal*

**Si** Organizaciones o personas directamente contratadas por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento: Entidades de mantenimiento informático, mantenimiento y soporte del registro y de la sede electrónica de la Autoridad Portuaria, Servicio de Asesoramiento en Sistema de Riesgos Penales.

**Si** Organismos u órganos de la Administración Pública con competencias en las materias objeto de las finalidades del tratamiento: Administraciones Públicas [AEAT (Ley General Tributaria), IGAE y Tribunal de Cuentas (RDL 2/2011, de 5 de septiembre, por el que se aprueba el Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante), Otros Órganos de la Administración del Estado, Tribunal de Cuentas o equivalente autonómico, Órganos Judiciales, Abogacía del Estado, Intervención de la Administración del Estado, Puertos del Estado.

**Si** Entidades Financieras: Gestión de cobro efectos y otros medios de pago

**Si** Fuerzas y Cuerpos de Seguridad: En la medida en que fuera requerido un derecho de acceso justificado en la investigación de un incumplimiento normativo. En caso de requerimiento judicial.

**Si** Representantes de los Trabajadores/Coordinación de Seguridad y Salud, Auditores externos: Conforme a Cumplir con el R.D. 171/2004 - Acreditación entrega riesgos por Coordinación de Actividades Empresariales.

|  |  |  |
|--|--|--|
| Si   | Otros:<br>• Canal de Denuncias Compliance (Las denuncias sobre vulneración de normativa y código de conducta son transmitidas a la Unidad de Cumplimiento Normativo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.<br>• Conforme a lo establecido en la LOPDGD, los órganos y organismos del Sector Público pueden comunicar los datos personales de los administrados a sujetos de derecho privado que lo soliciten(a) o bien cuando cuenten con el consentimiento de los administrados. b) o bien, cuando aparezca que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos.  |  |
| <b>J1. Transferencias internacionales de Datos (TID) (Arts.66 y 70 RLOPD): Países no UE a los que se realice o esté previsto realizar una comunicación de datos</b>  |  |  |
| Si   | Observaciones: Se pueden llevar a cabo transferencias internacionales de Los datos personales como consecuencia de la comunicación que la Autoridad Portuaria de Avilés pudiera realizar EMSA (Agencia Europea de Seguridad Marítima) en el ejercicio de sus funciones de seguridad portuaria y marítima.  |  |
| <b>K1. Plazos previstos para supresión de datos: Especificar plazo de expurgo y/o cancelación/bloqueo del dato tras finalizar la finalidad que legitimó el tratamiento</b>   |  |  |
| Si   | Datos a Conservar en Tratamientos Específicos y Referencia Legal de base   |  |
| Si   | Plazo de Conservación Exigible   |  |
| Si   | Criterio: Los datos personales serán conservados en nuestros sistemas mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento normativo por parte del interesado o de la Organización.   |  |
| Si   | Videovigilancia: Las imágenes/sonidos captados por los sistemas de video vigilancia serán cancelados en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras).  | Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art.22 LOPDGD) - 30 días. |
| Si   | Control Acceso a Edificios: Los datos incluidos en los ficheros automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios).   | 1 Mes  |
| Si   | Documentación Contable y Fiscal - A efectos Fiscales: Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria).<br>Plazo prescripción de Delitos Fiscales asociados a la comprobación de las bases o cuotas compensadas o pendientes de compensación o de deducciones aplicadas o pendientes de aplicación y a Delitos contra la Hacienda Pública y la Seguridad Social - Art. 66 bis Ley General Tributaria y Código Penal, respectivamente.  | 4 Años. Prescripción infracciones 10 años  |
| Si   | Documentación Contable y Fiscal - A efectos Fiscales: Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria)   | 4 Años   |
| Si   | Tratamientos de Solvencia: Datos referidos a deudas ciertas, vencidas y exigibles y no reclamadas (Art. 20 LOPDGD) Los datos permanecerán en el sistema mientras exista incumplimiento y como máximo un periodo de 5 años desde que este se produjo. El pago o cumplimiento de la deuda dará lugar a la supresión inmediata de esos datos, sin perjuicio de la obligación de bloqueo prevista.<br>Los datos bloqueados quedarán a disposición exclusiva del tribunal, el Ministerio Fiscal u otras Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas.<br>Los datos de ese deudor pueden ser consultados por quienes mantengan una relación contractual con este que suponga el abono de una cuantía pecuniaria o éste le hubiera solicitado la celebración de un contrato que implique financiación, pago aplazado o facturación periódica. En todo caso, será preciso informar al afectado acerca de la posible consulta del sistema.  | Mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito - 5 años   |
| Si   | Canal de Denuncias: Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.   | Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.   |
| Si   | Otros: Los datos personales serán conservados en nuestros tratamientos mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de cinco años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación).En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos.  | Mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de cinco años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación).En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos.   |
| Si   | Otros:<br>• Los datos tratados en relación con la garantía legal serán conservados durante la vigencia de la garantía legal y expirada la vigencia de la misma, durante el plazo que pudiera haber una reclamación judicial o administrativa en relación con la garantía legal.<br>• Los datos tratados para la remisión de comunicaciones comerciales serán conservados hasta que revoque el consentimiento otorgado.   |  |
| Si   | Observaciones: CRITERIOS DE SUPRESIÓN Y BLOQUEO DE LOS DATOS: conforme a lo establecido en el Artículo 32 de la LOPDGD, la Autoridad Portuaria de Avilés estará obligado a bloquear los datos cuando el afectado proceda a su supresión (ya que en videovigilancia no procede la rectificación).<br>El bloqueo de los datos consiste en la identificación y reserva de los mismos, 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 competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo. |  |
| <b>L1. Medidas de Seguridad: Identificación de Medidas técnicas y organizativas aplicables al tratamiento</b>  |  |  |
| Ver "Medidas de Seguridad" del Fichero   |  |  |
| La Autoridad Portuaria de Avilés toma todas las medidas necesarias para guardar Los datos personales personales de forma privada y segura. Sólo personas autorizadas de la Autoridad Portuaria de Avilés, personal autorizado de encargados de tratamiento o personal autorizado de nuestra organización (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a Los datos personales personales. Se exige a todo el personal de la Autoridad Portuaria de Avilés que tiene acceso a Los datos personales personales que se comprometa a respetar la Política de Privacidad y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a Los datos personales personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que los terceros que puedan tener acceso a Los datos personales personales los mantengan de forma segura. Para asegurarse de que Los datos personales personales están protegidos, la Autoridad Portuaria de Avilés dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados.<br>La Autoridad Portuaria de Avilés ha formalizado acuerdos para garantizar que tratamos Los datos personales personales correctamente y de acuerdo con la ley de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros. |  |  |
| <b>A2. Nombre del Tratamiento: Identificación del tratamiento de datos de la organización (pej: Personal, Clientes, Proveedores, Videovigilancia, ...)</b>   |  |  |
| CONCESIONES Y AUTORIZACIONES   |  |  |
| <b>B2. Identificación del Responsable y Contacto DPO: Identificación de entidad responsable de tratamiento y (en su caso) datos contacto DPO nombrado</b>  |  |  |
| AUTORIDAD PORTUARIA DE AVILÉS  |  |  |
| dpo@puertoaviles.es  |  |  |
| <b>C2. Tipificación/Descripción de la Finalidad/es: Especificar finalidad/es del Tratamiento y Usos previstos</b>  |  |  |



|  |  |   |
|--|--|---|
| Si   | <b>Control Acceso a Edificios:</b> Los datos incluidos en los ficheros automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios).  | 1 Mes   |
| Si   | <b>Documentación Contable y Fiscal - A efectos Fiscales:</b> Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar, y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria).<br><b>Plazo prescripción de Delitos Fiscales</b> asociadas a la comprobación de las bases o cuotas compensadas o pendientes de compensación o de deducciones aplicadas o pendientes de aplicación y a Delitos contra la Hacienda Pública y la Seguridad Social - Art. 66 bis Ley General Tributaria y Código Penal, respectivamente.   | 4 Años. Prescripción infracciones 10 años   |
| Si   | <b>Documentación Contable y Fiscal - A efectos Fiscales:</b> Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar, y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria)   | 4 Años  |
| Si   | <b>Tratamientos de Solvencia:</b> Datos referidos a deudas ciertas, vencidas y exigibles y no reclamadas (Art. 20 LOPDGD) Los datos permanecerán en el sistema mientras exista incumplimiento y como máximo un periodo de 5 años desde que este se produjo. El pago o cumplimiento de la deuda dará lugar a la supresión inmediata de esos datos, sin perjuicio de la obligación de bloqueo prevista.<br>Los datos bloqueados quedarán a disposición exclusiva del tribunal, el Ministerio Fiscal u otras Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas.<br>Los datos de ese deudor pueden ser consultados por quienes mantengan una relación contractual con este que suponga el abono de una cuantía pecuniaria o éste le hubiera solicitado la celebración de un contrato que implique financiación, pago aplazado o facturación periódica. En todo caso, será preciso informar al afectado acerca de la posible consulta del sistema.   | Mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito - 5 años  |
| Si   | <b>Canal de Denuncias:</b> Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.  | Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.  |
| Si   | Otros: Los datos personales serán conservados en nuestros tratamientos mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de cinco años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación). En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos.   | Mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de cinco años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación). En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos. |
| Si   | Otros:<br>• Los datos tratados en relación con la garantía legal serán conservados durante la vigencia de la garantía legal y expirada la vigencia de la misma, durante el plazo que pudiera haber una reclamación judicial o administrativa en relación con la garantía legal.<br>• Los datos tratados para la remisión de comunicaciones comerciales serán conservados hasta que revoque el consentimiento otorgado.   |   |
| Si   | <b>Observaciones:</b> CRITERIOS DE SUPRESIÓN Y BLOQUEO DE LOS DATOS: conforme a lo establecido en el Artículo 32 de la LOPDGD, la Autoridad Portuaria de Avilés estará obligado a bloquear los datos cuando el afectado proceda a su supresión (ya que en videovigilancia no procede la rectificación).<br>El bloqueo de los datos consiste en la identificación y reserva de los mismos, 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 competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la manipulación de los datos durante el mismo.   |   |
| <b>L2. Medidas de Seguridad: Identificación de Medidas técnicas y organizativas aplicables al tratamiento</b>  |  |   |
| <b>Ver "Medidas de Seguridad" del Fichero</b>  |  |   |
| La Autoridad Portuaria de Avilés toma todas las medidas necesarias para guardar Los datos personales personales de forma privada y segura. Solo personas autorizadas de la Autoridad Portuaria de Avilés, personal autorizado de encargados de tratamiento o personal autorizado de nuestra organización (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a Los datos personales personales. Se exige a todo el personal de la Autoridad Portuaria de Avilés que tiene acceso a Los datos personales personales que se comprometa a respetar la Política de Privacidad y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a Los datos personales personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que los terceros que puedan tener acceso a Los datos personales personales los mantengan de forma segura. Para asegurarse de que Los datos personales personales están protegidos, la Autoridad Portuaria de Avilés dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados.<br>La Autoridad Portuaria de Avilés ha formalizado acuerdos para garantizar que tratamos Los datos personales personales correctamente y de acuerdo con la ley de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros. |  |   |
| <b>A3. Nombre del Tratamiento: Identificación del tratamiento de datos de la organización (pej: Personal, Clientes, Proveedores, Videovigilancia, ...)</b>   |  |   |
| CONTACTOS- SOLICITANTES - USUARIOS SEDE ELECTRÓNICA - REGISTRO DE ENTRADA Y SALIDA   |  |   |
| <b>B3. Identificación del Responsable y Contacto DPO: Identificación de entidad responsable de tratamiento y (en su caso) datos contacto DPO nombrado</b>  |  |   |
| AUTORIDAD PORTUARIA DE AVILÉS  |  | <a href="mailto:dpo@puertoaviles.es">dpo@puertoaviles.es</a>  |
| <b>C3. Tipificación/Descripción de la Finalidad/es: Especificar finalidad/es del Tratamiento y Usos previstos</b>  |  |   |
| Si   | Atención a sus consultas y solicitudes: Gestión de Respuesta a Solicitudes de Tramitación Electrónica, Información, Recursos y/o de Actividades, Gestión de los servicios o procedimientos que se deriven de la solicitud o instancia, la Respuesta a Consultas, Reclamaciones o Incidencias que pudiera formularnos, Gestión del Registro de Entrada y Salida de Documentación, así como, en caso de que haya consentido, para las finalidades descritas en los consentimientos adicionales.<br>• Registro electrónico de recepción y remisión de solicitudes, escritos, documentación y comunicaciones relativas a los trámites y procedimientos competencia de la Autoridad Portuaria. Asignación de número de registro.<br>• Conexión al Portal de Emisión de facturas para registrar sus facturas, las cuales se emitirán en formato E-factura, previa solicitud de alta en el Dpto. Económico-Financiero.<br>• Conexión al Portal de Recepción de facturas, donde se depositarán regularmente las facturas emitidas por la Autoridad Portuaria. Previamente se debe firmar un contrato de adhesión.<br>• Atención a Consultas sobre estructura y funcionamiento de esta plataforma puede consultarse en el Plan de medidas de impulso de la Reutilización de información de la Autoridad Portuaria de Avilés<br>• Contacto con el interesado a través de los medios de comunicación facilitados (mail, dirección postal y/o teléfono) a fin de gestionar las consultas que nos haga llegar a través de los canales habilitados a tal efecto, gestionar avisos y coordinar actuaciones derivadas de los servicios que nos solicite por parte de personas relacionadas con la Autoridad Portuaria de Avilés y/o por encargados de tratamiento relacionados con la misma para las finalidades legitimadas y/o consentidas.<br>• Gestión y Respuesta a las solicitudes que nos remita a través del Formulario de Atención al Cliente.<br>• Gestión de inscripción en jornadas y eventos de la Autoridad Portuaria de Avilés<br>• Gestión de la suscripción al boletín de noticias de la Autoridad Portuaria de Avilés<br>El contacto y envío de comunicaciones personales, invitaciones a eventos, así como para informarle periódicamente de novedades, noticias e información corporativa y propuestas de proyectos y servicios de la organización que |   |
| <b>D3. Base Legitimadora: Especificar Base de Licitud de Tratamiento (Art.6.1 RGPD). La legitimación del tratamiento de Los datos personales se realiza por ser necesario para:</b>  |  |   |
| Si   | RGPD: 6.1.b) La ejecución de un contrato o relación comercial: La base legal para el tratamiento de Los datos personales es el cumplimiento de la solicitud que nos formula. Los datos solicitados son necesarios para la correcta prestación del mismo.   |   |
| Si   | RGPD: 6.1.c) Cumplir con una obligación jurídica: Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas  |   |
| Si   | RGPD: 6.1.e) Cumplir una misión de interés público: misión de interés público otorgada por la Ley de Puertos del Estado y de la Marina Mercante: Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por Real Decreto Legislativo 21/2011, de 5 de septiembre  |   |
| Si   | RGPD: 6.1.f) Satisfacer un interés legítimo del Responsable: Supuestos de interés legítimo en los que el responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos del incumplidor a terceros a fin de gestionar el cumplimiento normativo y la defensa de los intereses del responsable de tratamiento, publicación de datos con fines de transparencia y responsabilidad, fines de videovigilancia como interés legítimo de la organización en la protección de sus activos, así como supuestos de interés legítimo de tratamientos específicos contemplados en la LOPDGD: Artículo 19. Tratamiento de datos de contacto y de empresarios individuales; Artículo 22. Tratamientos con fines de videovigilancia; Artículo 23 Sistemas de exclusión publicitaria; Artículo 24 Sistemas de Información de denuncias internas).  |   |
| Si   | RGPD: 6.1.a) Cumplir las finalidades del tratamiento por consentimiento inequívoco del interesado: Su consentimiento inequívoco a través de la aceptación de las cláusulas establecidas de consentimiento habilitadas en el documento base que haya regulado la relación de contacto con la Autoridad Portuaria de Avilés:<br>El contacto y envío de comunicaciones personales, invitaciones a eventos, así como para informarle periódicamente de novedades, noticias e información corporativa y propuestas de proyectos y servicios de la organización* que pudieran ser de su interés tanto por medios escritos, telefónicos como electrónicos a través de los medios de comunicación facilitados.   |   |
| <b>E3. Origen y Procedencia de los Datos: Especificar fuente u origen de los datos de carácter personal que conforman el tratamiento</b>   |  |   |
| Si   | El propio interesado o su representante legal  |   |
| Si   | Entidad privada: Terceros con los que el responsable de tratamiento mantiene de una relación comercial o de prestación de servicios y para lo cual ha de disponer de Los datos personales personales a fin de tramitar o gestionar su acceso, incorporación al proceso/servicio objeto y/o para cumplir con nuestros compromisos organizacionales y obligaciones normativas asociados al servicio objeto de prestación y/o para la verificación del cumplimiento normativo bajo responsabilidad de la organización (pej), datos personales de trabajadores y/o terceros vinculados a entidades concesionarias o autorizadas).  |   |
| <b>F3. Colectivo/s de Interesados: Identificación del colectivo/s del que se tratan datos</b>  |  |   |
| Personas físicas y representantes legales y/o personas de contacto que formulan consultas y solicitudes a la Autoridad Portuaria de Avilés a través de canales de contacto (formularios web, sede electrónica y registro de entrada y salida)  |  |   |
| <b>G3. Estructura de Datos Personales: Especificar Tipología de Datos objeto de tratamiento</b>  |  |   |
| Si   | Categoría de Datos objeto de tratamiento   | Especificación  |
| No   | Categorías especiales de datos personales: datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física   | No contiene datos sensibles, salvo en los casos en los que el titular sea beneficiario de condiciones especiales y haya de facilitar registros que permitan acreditar o justificar el cumplimiento de dicha condición. Los datos que pudieran derivarse de posibles incumplimientos que pudieran incorporar datos relativos a condenas e infracciones penales estarían incorporados en el tratamiento "Infractores". Los datos potencialmente sensibles relativos a incidentes, accidentes o daños recibidos o causados por la Autoridad Portuaria estarían incorporados en el tratamiento "Incidencias y Responsabilidad Patrimonial"  |

|  |   |   |
|--|---|---|
| SI   | Datos identificativos: Nombre y apellidos, NIF/DNI, N° Seguridad Social / Mutualidad, Imagen/Voz, Firma, Datos huella parcial, Dirección, Teléfono particular, Dirección correo particular, Otros datos de carácter identificativo  | Datos identificativos y de contacto, así como relacionados con la Solicitud de Tramitación Electrónica, Solicitud de Información, Recursos y/o de Actividades, Consultas, Reclamaciones o Incidencias, Solicitudes de Información, Recursos y/o de Actividades que nos formula contenidos en la instancia/solicitud/formulario, la que pudiera adjuntar a dichos trámites, así como los datos personales de terceros que nos pudiera facilitar  |
| SI   | Otro tipo de datos: En la medida en que como consecuencia de la solicitud formulada se tramitasen servicios o actuaciones por parte de la APA, los datos personales formarían parte del tratamiento que en función del asunto correspondiera.   |   |
| <b>H3. Sistema de Tratamiento: Especificar método de tratamiento de la información</b>   |   |   |
| SI   | Mixto: Soporte papel, soporte informático/magnético.  |   |
| <b>I3. Cesión o comunicación de datos: Especificar entidades destinatarias a quienes se ha comunicado o van a comunicarse los datos de carácter personal</b>   |   |   |
| SI   | Organizaciones o personas directamente contratadas por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento: Colaboradores, Entidades contratadas para la ejecución de procedimientos/servicios objeto de solicitud o consulta.  |   |
| SI   | Fuerzas y Cuerpos de Seguridad: En la medida en que fuera requerido un derecho de acceso justificado en la investigación de un incumplimiento normativo. En caso de requerimiento judicial.   |   |
| SI   | Otros:<br>• Canal de Denuncias Compliance (Las denuncias sobre vulneración de normativa y código de conducta son transmitidas a la Unidad de Cumplimiento Normativo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.<br>• Conforme a lo establecido en la LOPDGD, los órganos y organismos del Sector Público pueden comunicar los datos personales de los administrados a sujetos de derecho privado que lo soliciten: a) o bien cuando cuenten con el consentimiento de los administrados. b) o bien, cuando aprecien que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos.  |   |
| SI   | Observaciones: En la medida en que como consecuencia de la solicitud formulada se tramitasen servicios o actuaciones por parte de la APA, los datos personales formarían parte del tratamiento que en función del asunto correspondiera.  |   |
| <b>J3. Transferencias internacionales de Datos (TID) (Arts.66 y 70 RLOPD): Países no UE a los que se realice o esté previsto realizar una comunicación de datos</b>  |   |   |
| SI   | Observaciones: En la medida en que como consecuencia de la solicitud formulada se tramitasen servicios o actuaciones por parte de la APA, los datos personales formarían parte del tratamiento que en función del asunto correspondiera.  |   |
| <b>K3. Plazos previstos para supresión de datos: Especificar plazo de expurgo y/o cancelación/bloqueo del dato tras finalizar la finalidad que legitimó el tratamiento</b>   |   |   |
| SI   | Datos a Conservar en Tratamientos Específicos y Referencia Legal de base  | Plazo de Conservación Exigible  |
| SI   | Criterio: Los datos personales serán conservados en nuestros sistemas mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento normativo por parte del interesado o de la Organización.  |   |
| SI   | Videovigilancia: Las imágenes/sonidos captados por los sistemas de video vigilancia serán cancelados en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras).  | Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art. 22 LOPDGD). |
| SI   | Control Acceso a Edificios: Los datos incluidos en los ficheros automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios).  | 1 Mes   |
| SI   | Canal de Denuncias: Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.  | Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.  |
| SI   | Otros: Los datos personales serán conservados en nuestros tratamientos mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de cinco años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación). En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos.  |   |
| SI   | Otros:<br>• Los datos tratados para la remisión de comunicaciones comerciales serán conservados hasta que revoque el consentimiento otorgado.   |   |
| SI   | Observaciones: CRITERIOS DE SUPRESIÓN Y BLOQUEO DE LOS DATOS: conforme a lo establecido en el Artículo 32 de la LOPDGD, la Autoridad Portuaria de Avilés estará obligado a bloquear los datos cuando el afectado proceda a su supresión (ya que en videovigilancia no procede la rectificación).<br>El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.   |   |
| <b>L3. Medidas de Seguridad: Identificación de Medidas técnicas y organizativas aplicables al tratamiento</b>  |   |   |
| <b>Ver "Medidas de Seguridad" del Fichero</b>  |   |   |
| La Autoridad Portuaria de Avilés toma todas las medidas necesarias para guardar Los datos personales personales de forma privada y segura. Solo personas autorizadas de la Autoridad Portuaria de Avilés, personal autorizado de encargados de tratamiento o personal autorizado de nuestra organización (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a Los datos personales personales. Se exige a todo el personal de la Autoridad Portuaria de Avilés que tiene acceso a Los datos personales personales que se comprometa a respetar la Política de Privacidad y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a Los datos personales personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que los terceros que puedan tener acceso a Los datos personales personales los mantengan de forma segura. Para asegurarse de que Los datos personales personales están protegidos, la Autoridad Portuaria de Avilés dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados.<br>La Autoridad Portuaria de Avilés ha formalizado acuerdos para garantizar que tratamos Los datos personales personales correctamente y de acuerdo con la ley de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros. |   |   |
| <b>A4. Nombre del Tratamiento: Identificación del tratamiento de datos de la organización (pej: Personal, Clientes, Proveedores, Videovigilancia, ...)</b>   |   |   |
| <b>INCIDENCIAS Y RESPONSABILIDAD PATRIMONIAL</b>   |   |   |
| <b>B4. Identificación del Responsable y Contacto DPO: Identificación de entidad responsable de tratamiento y (en su caso) datos contacto DPO nombrado</b>  |   |   |
| AUTORIDAD PORTUARIA DE AVILÉS  |   | dpo@puertoaviles.es   |
| <b>C4. Tipificación/Descripción de la Finalidad/es: Especificar finalidad/es del Tratamiento y Usos previstos</b>  |   |   |
| SI   | <ul style="list-style-type: none"> <li>• Tramitación de expedientes de incidencia o responsabilidad patrimonial: Uso interno, tramitación de expediente incidencia o responsabilidad patrimonial, resolución de incoación de expediente, así como en su caso, la gestión administrativa, económica y contable derivada del cobro de indemnizaciones por daños causados por terceros a la APA o bien abono de daños causados por la APA a terceros</li> <li>• Gestión de la notificación del expediente de incidencia o responsabilidad patrimonial: Contacto con el interesado a través de los medios de comunicación facilitados (mail, dirección postal y/o teléfono)</li> <li>• Gestión del cobro de indemnizaciones por daños causados por terceros a la APA o bien abono de daños causados por la APA a terceros</li> <li>• Gestión de Visitas y Videovigilancia de las instalaciones, así como de la seguridad y el cumplimiento normativo en las mismas, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercebimientos o sanciones por incumplimientos de normas de seguridad.</li> <li>• Atención a sus consultas y solicitudes: Gestión de Respuesta a Consultas, Reclamaciones o Incidencias, Solicitudes de Información, Recursos y/o de Actividades.</li> <li>• Gestión del Cumplimiento Normativo (normativa aplicable así como normativa interna de obligado cumplimiento): Investigación, monitorización y auditoría de controles establecidos para la prevención de delitos pudiendo establecerse los controles de acceso a las instalaciones, así como los controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normativa, delitos o comportamientos ilícitos.</li> <li>• Fines estadísticos e históricos que nos permitan mejorar la estrategia de mejora de los servicios de la Autoridad Portuaria de Avilés.</li> </ul> |   |
| <b>D4. Base Legitimadora: Especificar Base de Licitud de Tratamiento (Art.6.1 RGPD). La legitimación del tratamiento de Los datos personales se realiza por ser necesario para:</b>  |   |   |
| SI   | RGPD: 6.1.c) Cumplir con una obligación jurídica: normativa de régimen económico y de prestación de servicios de los puertos de interés general, Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por Real Decreto Legislativo 2/2011 y Reglamento de Servicios de Policía y Régimen del Puerto.   |   |
| SI   | RGPD: 6.1.e) Cumplir una misión de interés público: misión de interés público otorgada por la Ley de Puertos del Estado y de la Marina Mercante: Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por Real Decreto Legislativo 2/2011, de 5 de septiembre  |   |
| SI   | RGPD: 6.1.f) Satisfacer un interés legítimo del Responsable: Publicación de datos con fines de transparencia y responsabilidad; interés público general o interés de un tercero, interés legítimo de la entidad en la protección de sus activos, Prevención del Fraude y supuestos de interés legítimo en los que el responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos del incumplidor a terceros a fin de gestionar el cumplimiento normativo y la defensa de los intereses del responsable de tratamiento   |   |
| SI   | RGPD: 6.1.a) Cumplir las finalidades del tratamiento por consentimiento inequívoco del interesado: Su consentimiento inequívoco a través de la aceptación de las cláusulas establecidas de consentimiento habilitadas en el documento base que haya regulado la relación de contacto con la Autoridad Portuaria de Avilés:<br>La comunicación de Los datos personales en relación con la incidencia a los siguientes autorizados:<br>D/D': ..... con NIF ..... medio contacto/teléfono: .....<br>D/D': ..... con NIF ..... medio contacto/teléfono: .....   |   |
| <b>E4. Origen y Procedencia de los Datos: Especificar fuente u origen de los datos de carácter personal que conforman el tratamiento</b>   |   |   |
| SI   | El propio interesado o su representante legal   |   |

|   |  |
|---|--|
| SI  | Entidad privada:<br><ul style="list-style-type: none"> <li>En el caso de Incidencias: por los propios cedentes, por identificación a requerimiento de los agentes, o bien tras requerimiento a la Jefatura Provincial de Tráfico, como consecuencia de su acceso a la zona de servicio del puerto y que por sus acciones u omisiones puedan ser causar daños a la APA. En caso de empresas, por medio de los consignatarios o de los registros disponibles en la Autoridad Portuaria de Avilés (Registro de Clientes). En caso de buques, bien por el consignatario o bien por oficio a la Capitanía Marítima Avilés.</li> <li>En el caso de Responsabilidad Patrimonial: a instancia del propio afectado, o bien a través de compañías aseguradoras como consecuencia de que la APA haya podido ocasionar cualquier daño que no esté obligado a soportar.</li> </ul>  |
| <b>F4. Colectivo/s de Interesados :</b> <i>Identificación del colectivo/s del que se tratan datos</i>   |  |
| Personas físicas y representantes legales y/o personas de contacto que constan en expedientes de incidencias y responsabilidad patrimonial en los que esté implicada la APA       |  |
| <b>G4. Estructura de Datos Personales:</b> <i>Especificar Tipología de Datos objeto de tratamiento</i>  |  |
| SI  | Categoría de Datos objeto de tratamiento   |
| SI  | <p><b>Categorías especiales de datos personales:</b> <i>datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física</i></p> <p>Puede contener datos sensibles relativos a incidentes, accidentes o daños recibidos o causados por el titular o por terceros</p>  |
| SI  | <p><b>Datos identificativos:</b> <i>Nombre y apellidos, NIF/DNI, Nº Seguridad Social / Mutualidad, Imagen/Voz, Firma, Datos huella parcial, Dirección, Teléfono particular, Dirección correo particular, Otros datos de carácter identificativo</i></p> <p>Datos de carácter identificativo (DNI/NIF, nombre y apellidos, dirección postal), hechos denunciados, así como en su caso, datos del vehículo, matrícula y propietario.</p>   |
| SI  | <p><b>Económicos, financieros y de seguros:</b> <i>Ingresos, rentas, Inversiones, bienes patrimoniales, Créditos, préstamos, avales, Datos bancarios, Planes de pensiones, jubilación, Datos económicos de nómina, Datos deducciones impositivas/impuestos, Seguros, Hipotecas, Subsidios, beneficios, Historial créditos, Tarjetas crédito, Otros datos económicos, financieros y de seguros</i></p> <p>Datos económicos y financieros (datos bancarios cuenta abono)</p>   |
| <b>H4. Sistema de Tratamiento:</b> <i>Especificar método de tratamiento de la información</i>   |  |
| SI  | Mixto: Soporte papel, soporte informático/magnético.   |
| <b>I4. Cesión o comunicación de datos:</b> <i>Especificar entidades destinatarias a quienes se ha comunicado o van a comunicarse los datos de carácter personal</i>               |  |
| SI  | Organizaciones o personas directamente contratadas por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento: Internamente en la APA, intervienen los departamentos de Secretaría General, Económico Financiero (cobros o abonos), Infraestructuras (presupuestos) y Policía Portuaria (atestados), así como Entidades de mantenimiento informático, mantenimiento y soporte del registro y de la sede electrónica de la Autoridad Portuaria, Servicio de Asesoramiento en Sistema de Riesgos Penales.   |
| SI  | Organismos u órganos de la Administración Pública con competencias en las materias objeto de las finalidades del tratamiento: el Servicio Regional de Recaudación (deudas en apremio), la Jefatura Provincial de Tráfico y Capitanía Marítima, así como en su caso juzgados y tribunales y a cuantas Instituciones y Organismos proceda de acuerdo con la legislación vigente, así como a entidades públicas en el ámbito de sus competencias, por obligación legal  |
| SI  | Entidades Financieras: Entidad bancaria donde se ha establecido la cuenta corriente de cobro de indemnizaciones o bien abono de daños  |
| SI  | Fuerzas y Cuerpos de Seguridad: En la medida en que fuera requerido un derecho de acceso justificado en la investigación de un incumplimiento normativo. En caso de requerimiento judicial.  |
| SI  | <p>Utrós:</p> <ul style="list-style-type: none"> <li>Canal de Denuncias Compliance (Las denuncias sobre vulneración de normativa y código de conducta son transmitidas a la Unidad de Cumplimiento Normativo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.</li> <li>Conforme a lo establecido en la LOPDGD, los órganos y organismos del Sector Público pueden comunicar los datos personales de los administrados a sujetos de derecho privado que lo soliciten:a) o bien cuando cuenten con el consentimiento de los administrados. b) o bien, cuando aprecien que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos.</li> <li>Asimismo pueden estar implicadas, además de los propios interesados, las compañías aseguradoras (propias de la APA o bien de los interesados, o a aquellas personas físicas o jurídicas autorizadas a las que nos haya consentido de forma inequívoca</li> </ul>   |
| <b>J4. Transferencias internacionales de Datos (TID) (Arts.66 y 70 RLOPD):</b> <i>Países no UE a los que se realice o esté previsto realizar una comunicación de datos</i>        |  |
| <b>K4. Plazos previstos para supresión de datos:</b> <i>Especificar plazo de expurgo y/o cancelación/bloqueo del dato tras finalizar la finalidad que legitimó el tratamiento</i> |  |
| SI  | Datos a Conservar en Tratamientos Específicos y Referencia Legal de base   |
| SI  | Plazo de Conservación Exigible   |
| SI  | <p><b>Criterio:</b> Los datos personales serán conservados en nuestros sistemas mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento normativo por parte del interesado o de la Organización.</p>   |
| SI  | <p><b>Videovigilancia:</b> <i>Las imágenes/sonidos captados por los sistemas de video vigilancia serán cancelados en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras).</i></p> <p>Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art.22 LOPDGD) : 30 días.</p>   |
| SI  | <p><b>Control Acceso a Edificios:</b> <i>Los datos incluidos en los ficheros automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios).</i></p> <p>1 Mes</p>   |
| SI  | <p><b>Documentación Contable y Fiscal - A efectos Fiscales:</b> <i>Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria).</i></p> <p>Plazo prescripción de Delitos Fiscales asociados a la comprobación de las bases o cuotas compensadas o pendientes de compensación o de deducciones aplicadas o pendientes de aplicación y a Delitos contra la Hacienda Pública y la Seguridad Social - Art. 66 bis Ley General Tributaria y Código Penal, respectivamente.</p> <p>4 Años. Prescripción infracciones 10 años</p>  |
| SI  | <p><b>Documentación Contable y Fiscal - A efectos Fiscales:</b> <i>Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria)</i></p> <p>4 Años</p>  |
| SI  | <p><b>Tratamientos de Solvencia:</b> <i>Datos referidos a deudas ciertas, vencidas y exigibles y no reclamadas (Art. 20 LOPDGD)</i></p> <p>Los datos permanecerán en el sistema mientras exista incumplimiento y como máximo un periodo de 5 años desde que este se produjo. El pago o cumplimiento de la deuda dará lugar a la supresión inmediata de esos datos, sin perjuicio de la obligación de bloqueo prevista.</p> <p>Los datos bloqueados quedarán a disposición exclusiva del tribunal, el Ministerio Fiscal u otras Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas.</p> <p>Los datos de ese deudor pueden ser consultados por quienes mantengan una relación contractual con este que suponga el abono de una cuantía pecuniaria o éste le hubiera solicitado la celebración de un contrato que implique financiación, pago aplazado o facturación periódica. En todo caso, será preciso informar al afectado acerca de la posible consulta del sistema.</p> <p>Mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito - 5 años</p>  |
| SI  | <p><b>Canal de Denuncias:</b> <i>Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.</i></p> <p>Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.</p>  |
| SI  | <p>Otros: Los datos personales serán conservados en nuestros tratamientos mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de cinco años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación). En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos.</p> <p>Mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de cinco años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación). En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos.</p> |

|  |   |
|--|---|
| SI   | Otros:<br>• Los datos tratados en relación con la garantía legal serán conservados durante la vigencia de la garantía legal y expirada la vigencia de la misma, durante el plazo que pudiera haber una reclamación judicial o administrativa en relación con la garantía legal.   |
| SI   | Observaciones: CRITERIOS DE SUPRESIÓN Y BLOQUEO DE LOS DATOS: conforme a lo establecido en el Artículo 32 de la LOPDGD, la Autoridad Portuaria de Avilés estará obligado a bloquear los datos cuando el afectado proceda a su supresión (ya que en videovigilancia no procede la rectificación).<br>El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.   |
| <b>L4. Medidas de Seguridad: Identificación de Medidas técnicas y organizativas aplicables al tratamiento</b>  |   |
| Ver "Medidas de Seguridad" del Fichero   |   |
| La Autoridad Portuaria de Avilés toma todas las medidas necesarias para guardar Los datos personales de forma privada y segura. Solo personas autorizadas de la Autoridad Portuaria de Avilés, personal autorizado de encargados de tratamiento o personal autorizado de nuestra organización (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a Los datos personales personales. Se exige a todo el personal de la Autoridad Portuaria de Avilés que tiene acceso a Los datos personales personales que se comprometa a respetar la Política de Privacidad y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a Los datos personales personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que los terceros que puedan tener acceso a Los datos personales personales los mantengan de forma segura. Para asegurarse de que Los datos personales personales están protegidos, la Autoridad Portuaria de Avilés dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados. La Autoridad Portuaria de Avilés ha formalizado acuerdos para garantizar que tratamos Los datos personales personales correctamente y de acuerdo con la ley de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros. |   |
| <b>A5. Nombre del Tratamiento: Identificación del tratamiento de datos de la organización (pej: Personal, Clientes, Proveedores, Videovigilancia, ...)</b>   |   |
| INFRACCIONES   |   |
| <b>B5. Identificación del Responsable y Contacto DPO: Identificación de entidad responsable de tratamiento y (en su caso) datos contacto DPO nombrado</b>  |   |
| AUTORIDAD PORTUARIA DE AVILÉS <span style="float: right;">dpo@puertoaviles.es</span>   |   |
| <b>C5. Tipificación/Descripción de la Finalidad/es: Especificar finalidad/es del Tratamiento y Usos previstos</b>  |   |
| SI   | • Tramitación de Expedientes sancionadores: uso interno, tramitación de boletín de denuncia, expediente sancionador, resolución de imposición de sanción, así como en su caso, la gestión administrativa, económica y contable derivada del abono de la sanción.<br>• Gestión de la notificación del expediente sancionador: Contacto con el interesado a través de los medios de comunicación facilitados (mail, dirección postal y/o teléfono)<br>• Gestión del cobro de las multas en vía ejecutiva, cuando no son abonadas en el periodo voluntario<br>• Gestión de Visitas y Videovigilancia de las Instalaciones, así como de la seguridad y el cumplimiento normativo en las mismas, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercebimientos o sanciones por incumplimientos de normas de seguridad.<br>• Atención a sus consultas y solicitudes: Gestión de Respuesta a Consultas, Reclamaciones o Incidencias, Solicitudes de Información, Recursos y/o de Actividades.<br>• Gestión del Cumplimiento Normativo (normativa aplicable así como normativa interna de obligado cumplimiento): Investigación, monitorización y auditoría de controles establecidos para la prevención de delitos pudiendo establecerse los controles de acceso a las instalaciones, así como los controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normativa, delitos o comportamientos ilícitos.<br><i>Financ. Administrac. o Juzgados que por no permitir mostrar la actividad de mujeres de las unidades de la Autoridad Portuaria de Avilés.</i> |
| <b>D5. Base Legitimadora: Especificar Base de Licitud de Tratamiento (Art.6.1 RGPD). La legitimación del tratamiento de Los datos personales se realiza por ser necesario para:</b>  |   |
| SI   | RGPD: 6.1.c) Cumplir con una obligación jurídica: (normativa de régimen económico y de prestación de servicios de los puertos de interés general y legislación de transparencia, acceso a la información pública y buen gobierno) y la misión de interés público otorgada por la Ley de Puertos del Estado y de la Marina Mercante: Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por Real Decreto Legislativo 2/2011 y Reglamento de Servicios de Policía y Régimen del Puerto.  |
| SI   | RGPD: 6.1.e) Cumplir una misión de interés público: misión de interés público otorgada por la Ley de Puertos del Estado y de la Marina Mercante: Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por Real Decreto Legislativo 2/2011, de 5 de septiembre  |
| SI   | RGPD: 6.1.f) Satisfacer un Interés legítimo del Responsable: Publicación de datos con fines de transparencia y responsabilidad; interés público general o interés de un tercero, interés legítimo de la entidad en la protección de sus activos, Prevención del Fraude y supuestos de interés legítimo en los que el responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos del incumplidor a terceros a fin de gestionar el cumplimiento normativo y la defensa de los intereses del responsable de tratamiento   |
| <b>E5. Origen y Procedencia de los Datos: Especificar fuente u origen de los datos de carácter personal que conforman el tratamiento</b>   |   |
| SI   | El propio interesado o su representante legal   |
| SI   | Otras personas físicas distintas del interesado :<br>• Propios cedentes por identificación a requerimiento de los agentes o bien por oficio a la Jefatura Provincial de Tráfico, como consecuencia de su acceso a la zona de servicio del puerto y que por sus acciones u omisiones puedan ser denunciados por agentes de la Policía Portuaria o por otros responsables de la Autoridad Portuaria de Avilés.  |
| SI   | Otros:<br>• En caso de empresas, por medio de los consignatarios o de los registros disponibles en la Autoridad Portuaria de Avilés (Registro de Clientes). En caso de buques, bien por el consignatario o bien por oficio a la Capitanía Marítima Avilés.  |
| <b>F5. Colectivo/s de Interesados : Identificación del colectivo/s del que se tratan datos</b>   |   |
| Personas físicas y representantes legales y/o personas de contacto que constan en expedientes sancionadores tramitados en la APA   |   |
| <b>G5. Estructura de Datos Personales: Especificar Tipología de Datos objeto de tratamiento</b>  |   |
| SI   | Categoría de Datos objeto de tratamiento  |
| SI   | • Categorías especiales de datos personales: <i>datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física</i><br>Puede contener datos sensibles relativos a incidentes, accidentes o daños causados por el infractor a terceros, así como en aquellos casos en los que el infractor sea beneficiario de condiciones especiales y haya de facilitar registros que permitan acreditar o justificar el cumplimiento de dicha condición.  |
| SI   | Datos identificativos: Nombre y apellidos, NIF/DNI, N° Seguridad Social / Mutualidad, Imagen/Voz, Firma, Datos huella parcial, Dirección, Teléfono particular, Dirección correo particular, Otros datos de carácter identificativo<br>Datos de carácter identificativo (DNI/NIF, nombre y apellidos, dirección postal), hechos denunciados, así como en su caso, datos del vehículo, matrícula y propietario.   |
| SI   | Económicos, financieros y de seguros: Ingresos, rentas, Inversiones, bienes patrimoniales, Créditos, préstamos, avals, Datos bancarios, Planes de pensiones, jubilación, Datos económicos de nómina, Datos deducciones impositivas/impuestos, Seguros, Hipotecas, Subsidios, beneficios, Historial créditos, Tarjetas crédito, Otros datos económicos, financieras y de seguros<br>Datos económicos y financieros (datos bancarios cuenta abono)  |
| <b>H5. Sistema de Tratamiento: Especificar método de tratamiento de la información</b>   |   |
| SI   | Mixto: Soporte papel, soporte informático/magnético.  |
| <b>I5. Cesión o comunicación de datos: Especificar entidades destinatarias a quienes se ha comunicado o van a comunicarse los datos de carácter personal</b>   |   |
| SI   | Financiero y Policía Portuaria (explotación), así como Entidades de mantenimiento informático, mantenimiento y soporte del registro y de la sede electrónica de la Autoridad Portuaria, Servicio de Asesoramiento en Sistema de Riesgos Penales.  |
| SI   | Organismos u órganos de la Administración Pública con competencias en las materias objeto de las finalidades del tratamiento: : el Servicio Regional de Recaudación (deudas en apremio), la Jefatura Provincial de Tráfico y Capitanía Marítima. Entidad bancaria donde se ha establecido la cuenta corriente de abono de las sanciones.  |
| SI   | Entidades Financieras: Entidad bancaria donde se ha establecido la cuenta corriente de abono de las sanciones   |
| SI   | Fuerzas y Cuerpos de Seguridad: En la medida en que fuera requerido un derecho de acceso justificado en la investigación de un incumplimiento normativo. En caso de requerimiento judicial.   |
| SI   | Otros:<br>• Canal de Denuncias Compliance (Las denuncias sobre vulneración de normativa y código de conducta son transmitidas a la Unidad de Cumplimiento Normativo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.<br>• Conforme a lo establecido en la LOPDGD, los órganos y organismos del Sector Público pueden comunicar los datos personales de los administrados a sujetos de derecho privado que lo soliciten:a) o bien cuando cuenten con el consentimiento de los administrados. b) o bien, cuando aprecien que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos.   |
| Observaciones:   |   |
| <b>J5. Transferencias internacionales de Datos (TID) (Arts.66 y 70 RLOPD): Países no UE a los que se realice o esté previsto realizar una comunicación de datos</b>  |   |
| <b>K5. Plazos previstos para supresión de datos: Especificar plazo de expurgo y/o cancelación/bloqueo del dato tras finalizar la finalidad que legitimó el tratamiento</b>   |   |
| SI   | Datos a Conservar en Tratamientos Específicos y Referencia Legal de base <span style="float: right;">Plazo de Conservación Exigible</span>  |
| SI   | Criterio: Los datos personales serán conservados en nuestros sistemas mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento normativo por parte del interesado o de la Organización.  |

|    |   |  |
|----|---|--|
| Si | <b>Videovigilancia:</b> Las imágenes/sonidos captados por los sistemas de video vigilancia serán cancelados en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras).  | Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art.22 LOPDGD) - 30 días. |
| Si | <b>Control Acceso a Edificios:</b> Los datos incluidos en los ficheros automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios).   | 1 Mes  |
| Si | <b>Documentación Contable y Fiscal - A efectos Fiscales:</b> Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria).<br>Plazo prescripción de Delitos Fiscales asociados a la comprobación de las bases o cuotas compensadas o pendientes de compensación o de deducciones aplicadas o pendientes de aplicación y a Delitos contra la Hacienda Pública y la Seguridad Social - Art. 66 bis Ley General Tributaria y Código Penal, respectivamente.  | 4 Años. Prescripción infracciones 10 años  |
| Si | <b>Documentación Contable y Fiscal - A efectos Fiscales:</b> Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria)   | 4 Años   |
| Si | <b>Tratamientos de Solvencia:</b> Datos referidos a deudas ciertas, vencidas y exigibles y no reclamadas (Art. 20 LOPDGD)<br>Los datos permanecerán en el sistema mientras exista incumplimiento y como máximo un periodo de 5 años desde que este se produjo. El pago o cumplimiento de la deuda dará lugar a la supresión inmediata de esos datos, sin perjuicio de la obligación de bloqueo prevista.<br>Los datos bloqueados quedarán a disposición exclusiva del tribunal, el Ministerio Fiscal u otras Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas.<br>Los datos de ese deudor pueden ser consultados por quienes mantengan una relación contractual con este que suponga el abono de una cuantía pecuniaria o éste le hubiera solicitado la celebración de un contrato que implique financiación, pago aplazado o facturación periódica. En todo caso, será preciso informar al afectado acerca de la posible consulta del sistema.   | Mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito - 5 años   |
| Si | <b>Canal de Denuncias:</b> Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.   | Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.   |
| Si | Otros: Los datos personales serán conservados en nuestros tratamientos mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de cinco años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación). En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos.  | Mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de cinco años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación). En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos.  |
| Si | Otros:<br>• Los datos tratados en relación con la garantía legal serán conservados durante la vigencia de la garantía legal y expirada la vigencia de la misma, durante el plazo que pudiera haber una reclamación judicial o administrativa en relación con la garantía legal.   |  |
| Si | <b>Observaciones:</b> CRITERIOS DE SUPRESIÓN Y BLOQUEO DE LOS DATOS: conforme a lo establecido en el Artículo 32 de la LOPDGD, la Autoridad Portuaria de Avilés estará obligado a bloquear los datos cuando el afectado proceda a su supresión (ya que en videovigilancia no procede la rectificación).<br>El bloqueo de los datos consiste en la identificación y reserva de los mismos, 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 competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo. |  |

**L5. Medidas de Seguridad:** Identificación de Medidas técnicas y organizativas aplicables al tratamiento

Ver "Medidas de Seguridad" del Fichero

La Autoridad Portuaria de Avilés toma todas las medidas necesarias para guardar Los datos personales personales de forma privada y segura. Sólo personas autorizadas de la Autoridad Portuaria de Avilés, personal autorizado de encargados de tratamiento o personal autorizado de nuestra organización (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a Los datos personales personales. Se exige a todo el personal de la Autoridad Portuaria de Avilés que tiene acceso a Los datos personales personales que se comprometa a respetar la Política de Privacidad y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a Los datos personales personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que los terceros que puedan tener acceso a Los datos personales personales los mantengan de forma segura. Para asegurarse de que Los datos personales personales están protegidos, la Autoridad Portuaria de Avilés dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados.

La Autoridad Portuaria de Avilés ha formalizado acuerdos para garantizar que tratamos Los datos personales personales correctamente y de acuerdo con la ley de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros.

**A6. Nombre del Tratamiento:** Identificación del tratamiento de datos de la organización (pej: Personal, Clientes, Proveedores, Videovigilancia, ...)

PROVEEDORES/COLABORADORES Y ADJUDICATARIOS

**B6. Identificación del Responsable y Contacto DPO:** Identificación de entidad responsable de tratamiento y (en su caso) datos contacto DPO nombrado

AUTORIDAD PORTUARIA DE AVILÉS

dpo@puertoaviles.es

**C6. Tipificación/Descripción de la Finalidad/es:** Especificar finalidad/es del Tratamiento y Usos previstos



|   |   |
|---|---|
| Si  | <ul style="list-style-type: none"> <li>• Uso interno, Gestión comercial y relacional, Realización de operaciones y Gestión administrativa, económica y contable derivada de la relación con el proveedor/colaborador/licitador/adjudicatario</li> <li>• Comunicaciones y Consultas sobre oferta comercial y/o evolución del servicio solicitado: Confirmación/actualización del estado del pedido o servicio, gestión logística, ... Requerimiento de evidencias de los acuerdos alcanzados en la licitación, adjudicación y/o contrato.</li> <li>• Gestión de la Contratación y prestación de servicios por parte del proveedor/colaborador, así como del cumplimiento de requisitos contractuales y normativos vinculados a la organización u operación solicitada y/o de los servicios vinculados a la licitación así como del cumplimiento del PCAP, en su caso.</li> <li>• Gestión de la Selección, Homologación y Contratación de Proveedores/Colaboradores y verificación de cumplimiento normativo.</li> <li>• Gestión de la Seguridad y salud (prevención de riesgos laborales y coordinación de actividades empresariales), así como la evaluación de su cumplimiento</li> <li>• Gestión de Respuesta a Consultas, Reclamaciones o Incidencias, Solicitudes de Información, Recursos y/o de Actividades que pudiera formular el interesado y/o un tercero relacionado con la organización en relación con los trabajos y/o servicios prestados por el proveedor/colaborador a la organización.</li> <li>• Control horario y/o presencial o de asistencia y monitorización a través de registro de accesos, videovigilancia y confirmación del desempeño funcional tanto en las instalaciones de la organización como en instalaciones de terceros en los que el interesado lleve a cabo funciones de prestación de servicios a la organización (vigilancia y control para verificar el cumplimiento por parte del proveedor/colaborador de las obligaciones contractuales).</li> <li>• Promoción y Difusión de la Organización: Difusión de nuestras mejores prácticas y/o la publicación y/o comunicación de Los datos personales profesionales, currículum y/o material gráfico (vídeos, grabaciones y fotos asociadas a las actividades desarrolladas por la organización que pueden incorporar su imagen y la de personal a su cargo) en medios de comunicación corporativos (por ejemplo y no limitativo, web, redes sociales, boletines informativos, memoria de actividad, reportajes, presencia en medios de comunicación) y/u otros medios de comunicación pública (publicaciones sectoriales y/o reportajes en prensa escrita, TV, ...), como difusión de los resultados de la actividad, promoción y difusión, gestión de campañas, actividades y eventos y/o como acreditación de solvencia técnica ante solicitudes de evidencias de justificación en procesos de licitación, ofertas técnicas, proyectos y subvenciones en los que participe la APA, en los casos en los que el interesado lo consienta de forma inequívoca.</li> <li>• Gestión de la Calidad de procesos y actividades, así como la evaluación de los resultados de satisfacción/percepción y rendimiento de los grupos de interés de la organización. Realización de encuestas.</li> </ul>  |
| Si  | <ul style="list-style-type: none"> <li>• Gestión del Cumplimiento Normativo (normativa aplicable así como normativa interna de obligado cumplimiento): Investigación, monitorización y auditoría de controles establecidos para la prevención de delitos pudiendo establecerse los controles de acceso a las instalaciones, sistemas de información e impresión de documentación para todos los datos de carácter personal bajo responsabilidad de la organización y por lo tanto para todos los sistemas de información de dicha entidad, así como los controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normas laborales, delitos o comportamientos ilícitos.</li> <li>• Gestión del Contacto con el interesado a través de los medios de comunicación corporativos facilitados por la organización (mail y/o teléfono) a fin de gestionar avisos y coordinar actuaciones por parte de personas relacionadas con la organización, así como facilitando dichos medios a terceros que soliciten el contacto con el interesado. En los casos en los que el interesado lo consienta de forma inequívoca, se podrá llevar a cabo la utilización y facilitación de los medios de contacto privados (mail y teléfonos particulares) a personas relacionadas con la organización y a terceros que lo soliciten.</li> <li>• Fines estadísticos, históricos: estadísticas e indicadores de desempeño, seguridad y salud... así como histórico de relación profesional que nos permitan mejorar la estrategia de mejora de los servicios de la Autoridad Portuaria de Avilés</li> <li>• Gestión de Visitas y Videovigilancia de las Instalaciones, así como la seguridad y el cumplimiento normativo en las mismas, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercibimientos o sanciones por incumplimientos de normas de seguridad.</li> <li>• La gestión y auditoría de sistemas de gestión y/o gestión de seguridad laboral y cumplimiento normativo de procesos e instalaciones de la organización, así como la reserva del derecho de realizar auditorías periódicas en sus instalaciones como parte de los acuerdos alcanzados en la relación comercial.</li> <li>• Control de calidad sobre nuestros servicios, gestión de la calidad de procesos, instalaciones y actividades, realización de encuestas de opinión, así como la evaluación de los resultados de satisfacción/percepción y rendimiento de los grupos de interés de la organización</li> <li>• Evidenciar el Cumplimiento Normativo de la Organización ante un tercero que lo requiera: Comunicación a terceros de aquellos datos relativos al interesado que sean requeridos por estos a fin de cumplir con la coordinación de actividades empresariales, evidenciar cumplimiento normativo de la organización y de la normativa interna del tercero y/o para la gestión del acceso a instalaciones. En los casos en los que el interesado lo consienta de forma inequívoca, se podrá llevar a cabo la comunicación de aquella información/documentación requerida por el tercero que no estén explícitamente recogidas en las obligaciones normativas o legales establecidas, sino en la normativa interna del tercero.</li> <li>• La publicación en la web de la Autoridad Portuaria de Avilés o en la Plataforma de Contratación del Estado de alguno o varios de Los datos personales de contacto (denominación, teléfono, e-mail designado a efectos de notificaciones).</li> <li>• El contacto y envío de comunicaciones personales, encuestas, invitaciones a eventos, así como para informarle periódicamente de novedades, noticias e información corporativa de proyectos y servicios de la organización que pudieran ser de su interés tanto por medios escritos, telefónicos como electrónicos a través de los medios de comunicación facilitados, en la medida en que el interesado lo consienta de forma inequívoca.</li> <li>• La referencia asociada a los servicios prestados como acreditación de solvencia técnica ante solicitudes de evidencias de justificación en proyectos y subvenciones en los que participe la APA</li> </ul> |
| <b>D6. Base Legitimadora: Especificar Base de Licitud de Tratamiento (Art.6.1 RGPD). La legitimación del tratamiento de Los datos personales se realiza por ser necesario para:</b>   |   |
| Si  | RGPD: 6.1.b) La ejecución de un contrato o relación negocial: Cumplimiento de la adjudicación, contrato comercial y/o contrato licitado conforme al PCAP y de acuerdo a lo dispuesto en la 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.   |
| Si  | RGPD: 6.1.c) Cumplir con una obligación jurídica: (normativa de régimen económico y de prestación de servicios de los puertos de interés general y legislación de transparencia, acceso a la información pública y buen gobierno) y la misión de interés público otorgada por la Ley de Puertos del Estado y de la Marina Mercante: Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por Real Decreto Legislativo 212011, de 5 de septiembre. Asimismo, la obtención de la autorización para el servicio aquí definido es necesaria para la explotación, por aquellos operadores autorizados por la Autoridad Aduanera, de los almacenes de depósito temporal (ADT) o de los otros lugares autorizados para depósito temporal (OLADT), conforme a lo establecido en el Código Aduanero Comunitario (CAU), aprobado por el Reglamento (UE) nº952/13 del Parlamento Europeo y del Consejo de 9 de octubre de 2013. Coordinación Actividades Empresariales conforme a normativa de Prevención de Riesgos Laborales (R.D. 171/2004).   |
| Si  | RGPD: 6.1.e) Cumplir una misión de interés público: misión de interés público otorgada por la Ley de Puertos del Estado y de la Marina Mercante: Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por Real Decreto Legislativo 212011, de 5 de septiembre  |
| Si  | RGPD: 6.1.f) Satisfacer un interés legítimo del Responsable: Publicación de datos con fines de transparencia y responsabilidad; interés público general o interés de un tercero, interés legítimo de la entidad en la protección de sus activos, Prevención del Fraude y supuestos de interés legítimo en los que el responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos del interesado para cumplir con la defensa de los intereses del responsable de tratamiento   |
| Si  | <p>RGPD: 6.1.a) Cumplir las finalidades del tratamiento por consentimiento inequívoco del interesado: Su consentimiento inequívoco a través de la aceptación de las cláusulas establecidas de consentimiento habilitadas en el documento base que haya regulado la relación de contacto con la Autoridad Portuaria de Avilés:</p> <p>El contacto y envío de comunicaciones personales, encuestas, invitaciones a eventos, así como para informarle periódicamente de novedades, noticias e información corporativa de proyectos y servicios de la organización que pudieran ser de su interés tanto por medios escritos, telefónicos como electrónicos a través de los medios de comunicación facilitados.</p> <p>Evidenciar el Cumplimiento Normativo de la Organización ante un tercero que lo requiera: Comunicación a terceros de aquellos datos relativos al interesado que sean requeridos por estos a fin de cumplir con la normativa interna del tercero y/o para la gestión del acceso a instalaciones. La negativa a facilitar dicha información provocará la limitación a la participación del interesado en aquellos proyectos en los que la misma sea condición necesaria para su ejecución. La referencia asociada a los servicios prestados como acreditación de solvencia técnica ante solicitudes de evidencias de justificación en proyectos y subvenciones en los que participe la APA</p> <p>Difusión de nuestras mejores prácticas y/o la publicación y/o comunicación de Los datos personales profesionales, currículum y/o material gráfico (vídeos, grabaciones y fotos asociadas a las actividades desarrolladas por la organización que pueden incorporar su imagen y la de personal a su cargo) en medios de comunicación corporativos (por ejemplo y no limitativo, web, redes sociales, boletines informativos, memoria de actividad, reportajes, presencia en medios de comunicación) y/u otros medios de comunicación pública (publicaciones sectoriales y/o reportajes en prensa escrita, TV, ...), como difusión de los resultados de la actividad, promoción y difusión, gestión de campañas, actividades y eventos y/o como acreditación de solvencia técnica ante solicitudes de evidencias de justificación en procesos de licitación, ofertas técnicas, proyectos y subvenciones en los que participe la APA.</p> <p>Utilización y facilitación de los medios de contacto privados (mail y teléfonos particulares) a personas relacionadas con la Autoridad Portuaria de Avilés y a terceros que lo soliciten</p> <p>La transferencia internacional de Los datos personales en la medida en que sea estrictamente necesario para cumplir con la gestión de un proyecto en un país fuera de la UE o por la ubicación de los sistemas de tratamiento de aplicaciones de gestión del tratamiento. La no aceptación de esta cláusula impedirá la ejecución del proyecto en dicho país.</p>  |
|   | Otros:  |
| <b>E6. Origen y Procedencia de los Datos: Especificar fuente u origen de los datos de carácter personal que conforman el tratamiento</b>  |   |
| Si  | El propio interesado o su representante legal   |
| Si  | Entidad privada: A través de la entidad oferente/licitante/adjudicatario/proveedora/contratista que facilita datos personales de personas de la organización a fin de confirmar requisitos de solvencia técnica y adscripción de medios, gestionar su acceso, incorporación al proyecto/servicio objeto, la gestión administrativa, operacional y/o verificación del cumplimiento normativo bajo responsabilidad de la organización (pej), datos personales de los representantes legales de la entidad y/o de las personas involucradas en el proyecto (currículum vitae) y/o referencias personales de trabajos previos a fin de acreditar solvencia técnica y adscripción de medios y, en su caso, datos personales relativos a trabajadores que vayan a efectuar los trabajos contratados por razón del contrato en el caso de subrogación y por coordinación de actividades empresariales coordinación de actividades empresariales asociados a la prevención de riesgos laborales).   |
| <b>F6. Colectivo/s de Interesados : Identificación del colectivo/s del que se tratan datos</b>  |   |
| Personas físicas y representantes legales y/o personas de contacto de entidades solicitantes de colaboración, contratación y/o licitación, así como personas involucradas en procesos de licitación (mesas de contratación) |   |
| <b>G6. Estructura de Datos Personales: Especificar Tipología de Datos objeto de tratamiento</b>   |   |
| Si  | Categoría de Datos objeto de tratamiento  |
| No  | <p>Categorías especiales de datos personales: <i>datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física</i></p> <p>No contiene datos sensibles, salvo en los casos en los que el titular sea beneficiario de condiciones especiales y haya de facilitar registros que permitan acreditar o justificar el cumplimiento de dicha condición. Los datos que pudieran derivarse de posibles incumplimientos que pudieran incorporar datos relativos a condenas e infracciones penales estarían incorporados en el tratamiento "Infractores". Los datos potencialmente sensibles relativos a incidentes, accidentes o daños recibidos o causados por la Autoridad Portuaria estarían incorporados en el tratamiento "Incidencias y Responsabilidad Patrimonial"</p>  |

|  |   |   |
|--|---|---|
| SI   | Datos identificativos: Nombre y apellidos, NIF/DNI, N° Seguridad Social / Mutualidad, Imagen/Voz, Firma, Datos huella parcial, Dirección, Teléfono particular, Dirección correo particular, Otros datos de carácter identificativo  | Datos de personas de contacto para la gestión administrativa y operacional asociada a la ejecución del contrato/proyecto y de trabajadores que vayan a efectuar los trabajos contratados en términos de coordinación de actividades empresariales asociados a la prevención de riesgos laborales; En el caso de trabajadores que vayan a efectuar los trabajos contratados en términos de coordinación de actividades empresariales asociados a la prevención de riesgos laborales;   |
| SI   | Circunstancias sociales: Características de alojamiento, vivienda, Situación militar, Propiedades o posesiones, Aficiones y estilo de vida, Pertenencia clubes o asociaciones, Licencias, permisos, autorizaciones, Otros datos de circunstancias sociales  | Licencias u homologaciones, en el caso de trabajadores que vayan a efectuar los trabajos contratados en términos de coordinación de actividades empresariales asociados a la prevención de riesgos laborales;   |
| SI   | Información Comercial: Actividades y Negocios, Licencias Comerciales, Suscripciones a publicaciones / medios de comunicación, Creaciones artísticas, literarias, científicas o técnicas, Otros datos de información comercial   | Datos mercantiles, Datos de información comercial y homologación;   |
| SI   | Económicos, financieros y de seguros: Ingresos, rentas, Inversiones, bienes patrimoniales, Créditos, préstamos, avales, Datos bancarios, Planes de pensiones, jubilación, Datos económicos de nómina, Datos deducciones impositivas/impuestos, Seguros, Hipotecas, Subsidios, beneficios, Historial créditos, Tarjetas crédito, Otros datos económicos, financieros y de seguros  | Datos económico, financieros y/o de condiciones de cobro; Transacciones financieras;  |
| SI   | Transacciones de bienes y servicios: Bienes y servicios suministrados por el afectado, Bienes y servicios recibidos por el afectado, Transacciones financieras, Compensaciones / Indemnizaciones, Otros datos de transacciones de bienes y servicios  | Bienes y servicios suministrados por el afectado  |
| SI   | Otro tipo de datos: Otro tipo de datos: Nombre, apellidos y NIF de representante legal, datos de contacto de personas de la organización involucradas o relacionadas con el proyecto objeto del contrato/pedido.  |   |
| <b>H6. Sistema de Tratamiento: Especificar método de tratamiento de la información</b>   |   |   |
| SI   | Mixto: Soporte papel, soporte informático/magnético.  |   |
| <b>I6. Cesión o comunicación de datos: Especificar entidades destinatarias a quienes se ha comunicado o van a comunicarse los datos de carácter personal</b>               |   |   |
| SI   | Organizaciones o personas directamente contratadas por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento: Entidades de mantenimiento informático, mantenimiento y soporte del registro y de la sede electrónica de la Autoridad Portuaria, Servicio de Asesoramiento en Sistema de Riesgos Penales.   |   |
| SI   | Organismos u órganos de la Administración Pública con competencias en las materias objeto de las finalidades del tratamiento: Administraciones Públicas (AEAT (Ley General Tributaria), IGAE y Tribunal de Cuentas (Ley de Contratos del Sector Público), Otros Organos de la Administración del Estado, Tribunal de Cuentas o equivalente autonómico, Organos Judiciales, Abogacía del Estado, Intervención de la Administración del Estado, Puertos del Estado.   |   |
| SI   | Entidades Financieras: Gestión de cobro efectos y otros medios de pago  |   |
| SI   | Fuerzas y Cuerpos de Seguridad: En la medida en que fuera requerido un derecho de acceso justificado en la investigación de un incumplimiento normativo. En caso de requerimiento judicial.   |   |
| SI   | Representantes de los Trabajadores/Coordinación de Seguridad y Salud, Auditores externos: Conforme a Cumplir con el R.D. 171/2004 - Acreditación entrega riesgos por Coordinación de Actividades Empresariales.   |   |
| SI   | Otros:<br>• Canal de Denuncias Compliance (Las denuncias sobre vulneración de normativa y código de conducta son transmitidas a la Unidad de Cumplimiento Normativo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.<br>• Conforme a lo establecido en la LOPDGD, los órganos y organismos del Sector Público pueden comunicar los datos personales de los administrados a sujetos de derecho privado que lo soliciten: a) bien cuando cuenten con el consentimiento de los administrados. b) o bien, cuando aparezca que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos.  |   |
| <b>J6. Transferencias internacionales de Datos (TID) (Arts.66 y 70 RLOPD): Países no UE a los que se realice o esté previsto realizar una comunicación de datos</b>        |   |   |
| SI   | Observaciones: Se pueden llevar a cabo transferencias internacionales de Los datos personales como consecuencia de la comunicación que la Autoridad Portuaria de Avilés pudiera realizar EMSA (Agencia Europea de Seguridad Marítima) en el ejercicio de sus funciones de seguridad portuaria y marítima.   |   |
| <b>K6. Plazos previstos para supresión de datos: Especificar plazo de expurgo y/o cancelación/bloqueo del dato tras finalizar la finalidad que legitimó el tratamiento</b> |   |   |
| SI   | Datos a Conservar en Tratamientos Específicos y Referencia Legal de base  | Plazo de Conservación Exigible  |
| SI   | Criterio: Los datos personales serán conservados en nuestros sistemas mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento normativo por parte del interesado o de la Organización.  |   |
| SI   | Videovigilancia: Las imágenes/sonidos captados por los sistemas de video vigilancia serán cancelados en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras).   | Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art.22 LOPDGD) - |
| SI   | Control Acceso a Edificios: Los datos incluidos en los ficheros automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios).  | 1 Mes   |
| SI   | Documentación Contable y Fiscal - A efectos Fiscales: Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria).<br>Plazo prescripción de Delitos Fiscales asociadas a la comprobación de las bases o cuotas compensadas o pendientes de compensación o de deducciones aplicadas o pendientes de aplicación y a Delitos contra la Hacienda Pública y la Seguridad Social - Art. 66 bis Ley General Tributaria y Código Penal, respectivamente.   | 4 Años. Prescripción infracciones 10 años   |
| SI   | Documentación Contable y Fiscal - A efectos Mercantiles: Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria)   | 4 Años  |
| SI   | Tratamientos de Solvencia: Datos referidos a deudas ciertas, vencidas y exigibles y no reclamadas (Art. 20 LOPDGD). Los datos permanecerán en el sistema mientras exista incumplimiento y como máximo un periodo de 5 años desde que este se produjo. El pago o cumplimiento de la deuda dará lugar a la supresión inmediata de esos datos, sin perjuicio de la obligación de bloqueo prevista.<br>Los datos bloqueados quedarán a disposición exclusiva del tribunal, el Ministerio Fiscal u otras Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas.<br>Los datos de ese deudor pueden ser consultados por quienes mantengan una relación contractual con este que suponga el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que implique financiación, pago aplazado o facturación periódica. En todo caso, será preciso informar al afectado acerca de la posible consulta del sistema.  | Mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito - 5 años  |
| SI   | • Documentación pública relativa a las ofertas presentadas en el procedimiento de contratación de la licitación, conforme al pliego de condiciones administrativas particulares, presentada la oferta por el licitador, este vendrá obligado a mantener la misma durante 4 meses desde su recepción. Adjudicado el contrato y expirado el plazo para la presentación de recursos sin que estos hayan sido interpuestos, la documentación acreditativa de cumplimiento de requisitos previos quedará a disposición de los licitadores. Si éstos no retiran su documentación en los tres meses siguientes a la fecha en que se les notifique la adjudicación, la Autoridad Portuaria de Avilés no estará obligada a seguir custodiándola, pudiendo devolverla a los licitadores, a costa de éstos. Si ésta devolución no es posible podrá acordarse su destrucción levantando el correspondiente acta donde se hará constar la relación de todos y cada uno de los documentos que son objeto de destrucción, incorporándose la misma en el expediente.<br>• Documentación pública relativa al procedimiento de adjudicación, conforme a los plazos de prescripción penal (en base al acogimiento del principio de prudencia) se proponen plazos de hasta 20 años. | 4 meses siguientes a la notificación de adjudicación en relación con las ofertas recibidas y 20 años en relación con el procedimiento de adjudicación   |

|  |  |   |
|--|--|---|
| Si   | <b>Canal de Denuncias:</b> Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.  | Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.  |
| Si   | Otros: Los datos personales serán conservados en nuestros tratamientos mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de cinco años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación). En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos.   | Mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización (reforma del Código Civil establece un plazo de cinco años para poder llevar a cabo una acción por responsabilidad civil, plazo que computa desde la fecha en que pueda exigirse el cumplimiento de la obligación). En cualquier caso, al término de la relación los Datos del interesado serán debidamente bloqueados, según lo previsto en la normativa vigente de protección de datos. |
| Si   | Otros:<br><ul style="list-style-type: none"> <li>Los datos tratados en relación con la garantía legal serán conservados durante la vigencia de la garantía legal y expirada la vigencia de la misma, durante el plazo que pudiera haber una reclamación judicial o administrativa en relación con la garantía legal.</li> <li>Los datos tratados para la remisión de comunicaciones comerciales serán conservados hasta que revoque el consentimiento otorgado.</li> <li>Documentación pública relativa a las ofertas presentadas en el procedimiento de contratación expediente de licitación, conforme al pliego de cláusulas jurídicas, presentada la oferta por el licitador, este vendrá obligado a mantener la misma durante 4 meses desde su recepción. Adjudicado el contrato y expirado el plazo para la presentación de recursos sin que estos hayan sido interpuestos, la documentación acreditativa de cumplimiento de requisitos previos quedará a disposición de los licitadores. Si éstos no retiran su documentación en los tres meses siguientes a la fecha en que se les notifique la adjudicación, la Autoridad Portuaria de Avilés no estará obligada a seguir custodiándola, pudiendo devolverla a los licitadores, a costa de éstos. Si ésta devolución no es posible podrá acordarse su destrucción levantando el correspondiente acta donde se hará constar la relación de todos y cada uno de los documentos que son objeto de destrucción, incorporándose la misma en el expediente.</li> <li>Documentación pública relativa al expediente de adjudicación/contratación, conforme a los plazos de prescripción penal (en base al acogimiento del principio de prudencia) proponen plazos de hasta 20 años.</li> </ul>  |   |
| Si   | <b>Observaciones:</b> CRITERIOS DE SUPRESIÓN Y BLOQUEO DE LOS DATOS: conforme a lo establecido en el Artículo 32 de la LOPDGD, la Autoridad Portuaria de Avilés estará obligado a bloquear los datos cuando el afectado proceda a su supresión (ya que en videovigilancia no procede la rectificación).<br>El bloque de los datos consiste en la identificación y reserva de los mismos, 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 competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.   |   |
| <b>L6. Medidas de Seguridad: Identificación de Medidas técnicas y organizativas aplicables al tratamiento</b>  |  |   |
| <u>Ver "Medidas de Seguridad" del Fichero</u>  |  |   |
| La Autoridad Portuaria de Avilés toma todas las medidas necesarias para guardar Los datos personales personales de forma privada y segura. Sólo personas autorizadas de la Autoridad Portuaria de Avilés, personal autorizado de encargados de tratamiento o personal autorizado de nuestra organización (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a Los datos personales personales. Se exige a todo el personal de la Autoridad Portuaria de Avilés que tiene acceso a Los datos personales personales que se comprometa a respetar la Política de Privacidad y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a Los datos personales personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que los terceros que puedan tener acceso a Los datos personales personales los mantengan de forma segura. Para asegurarse de que Los datos personales personales están protegidos, la Autoridad Portuaria de Avilés dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados.<br>La Autoridad Portuaria de Avilés ha formalizado acuerdos para garantizar que tratamos Los datos personales personales correctamente y de acuerdo con la ley de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros. |  |   |
| <b>A7. Nombre del Tratamiento: Identificación del tratamiento de datos de la organización (pej: Personal, Clientes, Proveedores, Videovigilancia, ...)</b>   |  |   |
| <b>CANDIDATOS</b>  |  |   |
| <b>B7. Identificación del Responsable y Contacto DPO: Identificación de entidad responsable de tratamiento y (en su caso) datos contacto DPO nombrado</b>  |  |   |
| AUTORIDAD PORTUARIA DE AVILÉS  |  | dpo@puertoaviles.es   |
| <b>C7. Tipificación/Descripción de la Finalidad/es: Especificar finalidad/es del Tratamiento y Usos previstos</b>  |  |   |
| Si   | <ul style="list-style-type: none"> <li>Uso interno para el proceso selectivo para el que se ha convocado, para su incorporación a la Bolsa de Trabajo y para la oferta y gestión de las posibles ofertas de empleo o colaboración que pudieran generarse.</li> <li>Gestión de evaluación de competencias de candidatos y personas en selección y/o promoción interna a puestos de trabajo</li> <li>Gestión del Contacto con el interesado a través de los medios de comunicación facilitados (mail y/o teléfono) a fin de gestionar avisos y coordinar actuaciones para la gestión del proceso de selección por parte de personas relacionadas con AUTORIDAD PORTUARIA DE AVILÉS y/o terceros a los que contratan los procesos de selección de candidatos a vacantes o puestos de trabajo.</li> <li>Gestión del Cumplimiento Normativo (normativa aplicable así como normativa interna de obligado cumplimiento): Investigación, monitorización y auditoría de controles establecidos para la prevención de delitos pudiendo establecerse los controles de acceso a las instalaciones, sistemas de información e impresión de documentación para todos los datos de carácter personal bajo responsabilidad de la organización y por lo tanto para todos los sistemas de información de dicha entidad, así como los controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normas laborales, delitos o comportamientos ilícitos.</li> <li>Gestión de Visitas y Videovigilancia de las Instalaciones, así como la seguridad y el cumplimiento normativo en las mismas, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercebimientos o sanciones por incumplimientos de normas de seguridad.</li> </ul> |   |
| <b>D7. Base Legitimadora: Especificar Base de Licitud de Tratamiento (Art.6.1 RGPD). La legitimación del tratamiento de Los datos personales se realiza por ser necesario para:</b>  |  |   |
| Si   | RGPD: 6.1.b) La ejecución de un contrato o relación negocial: El cumplimiento de la solicitud de incorporación al proceso de selección por convocatoria pública de empleo y/o autocandidatura a la bolsa de empleo por parte del interesado a través de la remisión de su cv por medio de los canales de contacto de la organización y/o a través del SEPE   |   |
| Si   | RGPD: 6.1.f) Satisfacer un interés legítimo del Responsable: fines de videovigilancia como interés legítimo de la organización en la protección de sus activos, prevención del fraude y supuestos de interés legítimo en los que el responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos ante incumplimientos a terceros a fin de gestionar el cumplimiento normativo y la defensa de los intereses del responsable de tratamiento.   |   |
| <b>E7. Origen y Procedencia de los Datos: Especificar fuente u origen de los datos de carácter personal que conforman el tratamiento</b>   |  |   |
| Si   | El propio interesado o su representante legal  |   |
| Si   | Entidad privada: A través de terceros a los que se contrate los procesos de selección de candidatos a vacantes o puestos de trabajo de AUTORIDAD PORTUARIA DE AVILÉS   |   |
| <b>F7. Colectivo/s de Interesados : Identificación del colectivo/s del que se tratan datos</b>   |  |   |
| Candidatos que solicitan su incorporación al proceso de selección por convocatoria pública de empleo y/o autocandidatura a la bolsa de empleo por parte del interesado a través de la remisión de su cv por medio de los canales de contacto de la organización y/o a través del SEPE  |  |   |
| <b>G7. Estructura de Datos Personales: Especificar Tipología de Datos objeto de tratamiento</b>  |  |   |
| Si   | Categoría de Datos objeto de tratamiento   | Especificación  |
| Si   | <b>Categorías especiales de datos personales:</b> <i>datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física</i>   | Contiene datos relativos a condenas e infracciones penales por el requerimiento del certificado de penales, así como, en el los casos en los que el titular disponga de condiciones especiales (pej: discapacidad) y haya de facilitar documentación que incorpore dicha información a fin de que pueda ser acreditado o justificado el cumplimiento de dicha condición. En la medida en que el candidato informe sobre una condición de discapacidad, se podrán requerir los certificados que así lo acreditan. (Certificado de minusvalía, declaración de no haber sido separado del servicio por sanción alguna, etc)  |
| Si   | <b>Datos identificativos:</b> <i>Nombre y apellidos, NIF/DNI, N° Seguridad Social / Mutualidad, Imagen/Voz, Firma, Datos huella parcial, Dirección, Teléfono particular, Dirección correo particular, Otros datos de carácter identificativo</i>   | Cv de los candidatos. Instancia; junto con la instancia los candidatos deben presentar Cv y copia de documentación acreditativa (DNI, Datos identificativos y de contacto; fecha y lugar de nacimiento, edad, sexo).  |
| Si   | <b>Datos académicos y profesionales:</b> <i>Formación y titulaciones, Experiencia profesional, Historial de estudiante, Cargo/puesto/función y organización en la que ha desempeñado dicha función, Pertenencia a colegios o a asociaciones profesionales, Otros datos académicos y profesionales</i>  | Copia de titulaciones oficiales; Datos académicos y profesionales relativos a formación, titulaciones y experiencia profesional.  |
| Si   | <b>Circunstancias personales:</b> <i>Datos de estado civil, Datos de familia, Fecha de nacimiento, Lugar de nacimiento, Edad, Sexo, Nacionalidad, Lengua materna, Características físicas o antropométricas (no biométricos unívocos), Otros datos de circunstancias personales</i>  | Datos personales asociados al estado civil, datos de familia, nacionalidad.   |
| Si   | <b>Circunstancias sociales:</b> <i>Características de alojamiento, vivienda, Situación militar, Propiedades o posesiones, Aficiones y estilo de vida, Pertenencia clubes o asociaciones, Licencias, permisos, autorizaciones, Otros datos de circunstancias sociales</i>   | Carnet de conducir. Permiso de trabajo, Ocio y aficiones.   |
| Si   | <b>Detalles de empleo:</b> <i>Profesión, Puesto de trabajo, Datos no económicos de nómina, Historial del trabajador, Otros datos de detalle de empleo</i>  | Vida laboral, copia de contratos, Datos de Estado laboral; Otros datos (Aspiraciones profesionales).  |

|   |  |
|---|--|
| <b>H7. Sistema de Tratamiento: Especificar método de tratamiento de la información</b>  |  |
| Si  | Mixto: Soporte papel, soporte informático/magnético.   |
| <b>I7. Cesión o comunicación de datos: Especificar entidades destinatarias a quienes se ha comunicado o van a comunicarse los datos de carácter personal</b>  |  |
| Si  | Organizaciones o personas directamente contratadas por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento: terceros a los que se contrate los procesos de selección de candidatos a vacantes o puestos de trabajo de AUTORIDAD PORTUARIA DE AVILÉS (personal de Registro, Secretaría General, RRHH, miembros del tribunal y, cuando se contrata con un externo la realización de servicios (pej): entrevistas y psicotécnico, pruebas dentro del proceso (ej), pruebas de informática o de inglés),...) )   |
| Si  | Fuerzas y Cuerpos de Seguridad: En la medida en que fuera requerido un derecho de acceso justificado en la investigación de un incumplimiento normativo. En caso de requerimiento judicial.  |
| Si  | Otros:<br><ul style="list-style-type: none"> <li>Canal de Denuncias Compliance (Las denuncias sobre vulneración de normativa y código de conducta son transmitidas a la Unidad de Cumplimiento Normativo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.</li> <li>Conforme a lo establecido en la LOPDGDD, los órganos y organismos del Sector Público pueden comunicar los datos personales de los administrados a sujetos de derecho privado que lo soliciten:a) o bien cuando cuenten con el consentimiento de los administrados. b) o bien, cuando aprecien que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos.</li> </ul>   |
| <b>J7. Transferencias internacionales de Datos (TID) (Arts.66 y 70 RLOPD): Países no UE a los que se realice o esté previsto realizar una comunicación de datos</b>   |  |
| Si  | Observaciones: No se realizan transferencias internacionales de datos  |
| <b>K7. Plazos previstos para supresión de datos: Especificar plazo de expurgo y/o cancelación/bloqueo del dato tras finalizar la finalidad que legitimó el tratamiento</b>  |  |
| Si  | Datos a Conservar en Tratamientos Específicos y Referencia Legal de base   |
| Si  | Plazo de Conservación Exigible   |
| Si  | Criterio: Los datos personales serán conservados en nuestros sistemas mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento normativo por parte del interesado o de la Organización.   |
| Si  | Videovigilancia: Las imágenes/sonidos captados por los sistemas de video vigilancia serán cancelados en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras).  |
| Si  | Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art.22 LOPDGDD) - 30 días.  |
| Si  | Control Acceso a Edificios: Los datos incluidos en los ficheros automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios).   |
| Si  | 1 Mes  |
| Si  | Canal de Denuncias: Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGDD.  |
| Si  | Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGDD.  |
| Si  | Otros:   |
| Si  | Los datos personales serán conservados durante 5 años (excepto en los casos en los que el candidato sea seleccionado en cuyo caso, pasarán a formar parte del tratamiento de datos de RRHH de la organización contratante), así como los plazos legalmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento contractual por parte del interesado o de la Organización.   |
| Si  | Observaciones: CRITERIOS DE SUPRESIÓN Y BLOQUEO DE LOS DATOS: conforme a lo establecido en el Artículo 32 de la LOPDGDD, la Autoridad Portuaria de Avilés estará obligado a bloquear los datos cuando el afectado proceda a su supresión (ya que en videovigilancia no procede la rectificación). El bloqueo de los datos consiste en la identificación y reserva de los mismos, 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 competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo. |
| <b>L7. Medidas de Seguridad: Identificación de Medidas técnicas y organizativas aplicables al tratamiento</b>   |  |
| Ver "Medidas de Seguridad" del Fichero  |  |
| La Autoridad Portuaria de Avilés toma todas las medidas necesarias para guardar Los datos personales personales de forma privada y segura. Sólo personas autorizadas de la Autoridad Portuaria de Avilés, personal autorizado de encargados de tratamiento o personal autorizado de nuestra organización (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a Los datos personales personales. Se exige a todo el personal de la Autoridad Portuaria de Avilés que tiene acceso a Los datos personales personales que se comprometa a respetar la Política de Privacidad y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a Los datos personales personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que los terceros que puedan tener acceso a Los datos personales personales los mantengan de forma segura. Para asegurarse de que Los datos personales personales están protegidos, la Autoridad Portuaria de Avilés dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados. La Autoridad Portuaria de Avilés ha formalizado acuerdos para garantizar que tratamos Los datos personales personales correctamente y de acuerdo con la ley de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros. |  |
| <b>A8. Nombre del Tratamiento: Identificación del tratamiento de datos de la organización (pej: Personal, Clientes, Proveedores, Videovigilancia, ...)</b>  |  |
| RECURSOS HUMANOS (RRHH)   |  |
| <b>B8. Identificación del Responsable y Contacto DPO: Identificación de entidad responsable de tratamiento y (en su caso) datos contacto DPO nombrado</b>   |  |
| AUTORIDAD PORTUARIA DE AVILÉS   |  |
| dpo@puertoaviles.es   |  |
| <b>C8. Tipificación/Descripción de la Finalidad/es: Especificar finalidad/es del Tratamiento y Usos previstos</b>   |  |

|  |   |
|--|---|
| Si   | <ul style="list-style-type: none"> <li>• Uso interno, Gestión de recursos humanos y Gestión administrativa, laboral, económica, contable y de prevención de riesgos laborales, derivada de la relación con el cedente (relación profesional/laboral y/o de gestión de prácticas)</li> <li>• Gestión de la contratación, acogida, formación, remuneración y cumplimiento normativo en materia laboral, seguros sociales, seguridad laboral, seguridad de la información, gestión de permisos y vacaciones, gestión de dietas y autorización de la comisión de servicio, reserva de crédito en caso de jubilaciones parciales... y demás normativa aplicable a la gestión de recursos humanos con relación laboral/prácticas/trabajo temporal/beca y/o los generados como consecuencia del desempeño de funciones en la organización (aplicables a ex empleados, empleados actuales y candidatos a futuro empleo).</li> <li>• Alta del trabajador en la Seguridad Social, la comunicación del contrato al SEPE (y consiguientes procesos de comunicaciones de variaciones de datos y extinciones que deben ser obligatoriamente comunicadas a estos organismos)</li> <li>• Descuento de cuota sindical al trabajador e ingreso en la cuenta del sindicato.</li> <li>• Gestión de evaluación de competencias y/o promoción interna a puestos de trabajo.</li> <li>• Gestión de la Seguridad y salud (prevención de riesgos laborales y vigilancia de la salud), así como la evaluación de su cumplimiento. Gestión revisiones médicas con SPA. Bajas médicas, partes IT, permisos, licencias, etc,</li> <li>• La Gestión y contratación de seguros (salud, vida, asistencia, ...) y/o planes de pensiones en beneficio de sus empleados, bien de modo voluntario, bien en virtud de lo pactado en un Convenio Colectivo. Así mismo, se puede llevar a cabo la intermediación o tramitación de gestiones asociadas a pólizas de seguros (tramitación de la designación de beneficiarios respecto a la póliza de accidentes, remisión a aseguradora de información asociada a siniestros para solicitud de indemnización, ...) y pensiones (descuento en nómina de las aportaciones a planes de pensiones y comunicación al promotor del plan, intermediación en el proceso de rescate del plan de pensiones, intermediación en la gestión de incidencias en el cobro de pensiones ...), en la medida en que lo hubiera consentido inequívocamente.</li> <li>• Gestión de becas de ayuda al estudio: tramitación de solicitudes y documentación acreditativa (matrículas de hijos a cargo)</li> <li>• Gestión viajes, ferias, congresos, etc con agencia externa (reserva de vuelos, hoteles). Gestión de visados y pasaportes, en su caso. Gestión de reservas con agencias de alquiler de vehículos</li> <li>• Gestión de Formación externa: comunicación de Los datos personales para la tramitación de su inscripción en acciones formativas, gestión de FUNDAE (en su caso), control de asistencia, gestión de justificación y emisión de certificados asociados.</li> <li>• Firma de Compromiso de confidencialidad y de Código de Conducta de Cumplimiento Normativo, así como la verificación de su cumplimiento.</li> <li>• Gestión Organizativa: Elaboración y difusión de organigrama, Pie de firma correos electrónicos de empresa, Currículum Profesional</li> <li>• Gestión de Órganos Sociales: Gestión administrativa asociada a la generación de la documentación societaria: Escrituras (socios, apoderados, representante legal, ...), Gestión de Convocatoria, Comunicación, Organización y Funcionamiento de Órganos Sociales, Tramitación de los asuntos a debatir en reuniones de órganos sociales, adopción de acuerdos, así como gestión fiscal y bancaria asociada a la retribución, creación y funcionamiento del órgano de administración y de sus miembros, gestión de actos y contratación formal con clientes, proveedores, trabajadores, entidades financieras y organismos públicos que requieran de firma autorizada en nombre de la organización,</li> <li>• Gestión de Respuesta a Consultas, Reclamaciones e Incidencias, Solicitudes de Información, Recursos y/o de Actividades que pudiera formular el interesado y/o un tercero relacionado con la organización</li> <li>• Control de fichajes y absentismo: control horario y/o presencial o de asistencia y monitorización a través de registro de accesos por huella, videovigilancia y/o geolocalización para la coordinación operativa de trabajos y confirmación del desempeño funcional y laboral tanto en las instalaciones de la organización como en instalaciones de terceros en los que el interesado lleve a cabo funciones laborales o formativas durante su jornada laboral, conforme a lo establecido en el Estatuto de los Trabajadores (ET: vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales). En caso de ausencia del trabajador por motivos médicos, propios o de familiares, gestión de solicitud de justificante médico asociado.</li> <li>• Comité de Préstamos al personal por adquisición de vivienda y por necesidades urgentes: Tramitación de la solicitud correspondiente con la documentación acreditativa (pej: contrato de compraventa o presupuestos para reforma de vivienda, ...) para el estudio y, en su caso, concesión por parte de Comité de Préstamos, formado por trabajadores de la Autoridad Portuaria.</li> <li>• Difusión de nuestras mejores prácticas y/o la publicación y/o comunicación de Los datos personales profesionales, currículum y/o material gráfico (videos, grabaciones y fotos asociadas a las actividades desarrolladas por la organización que pueden incorporar su imagen) en medios de comunicación corporativos (por ejemplo y no limitativo, web, redes sociales, boletines informativos, memoria de actividad, reportajes, presencia en medios de comunicación) y/u otros medios de comunicación pública (publicaciones sectoriales y/o reportajes en prensa escrita, TV, ...), como difusión de los resultados de la actividad, promoción y difusión, gestión de campañas, actividades y eventos y/o como acreditación de solvencia técnica ante solicitudes de evidencias de justificación en procesos de licitación, ofertas técnicas, proyectos y subvenciones en los que participe la Autoridad Portuaria de Avilés, en la medida en que así lo haya consentido.</li> </ul> |
| Si   | <ul style="list-style-type: none"> <li>• Gestión de la Calidad de procesos y actividades, así como la evaluación de los resultados de satisfacción/percepción y rendimiento de los grupos de interés de la organización. Realización de encuestas (satisfacción, clima laboral y/o psicosociales)</li> <li>• Gestión de solvencia técnica en presentación ofertas y/o solicitud, gestión y justificación de campañas, actividades, eventos, concursos, proyectos y subvenciones en los que participe la organización, para lo cual podrá facilitarse el currículum profesional y/o documentación/información relativa al interesado relacionada con la relación profesional/laboral y/o gestión de prácticas como evidencia o justificación de cumplimiento. En los casos en los que el interesado lo consienta de forma inequívoca, se podrá llevar a cabo la utilización y facilitación del currículum particular del interesado a personas relacionadas con la organización y a terceros que lo soliciten.</li> <li>• Gestión del Cumplimiento Normativo (normativa aplicable así como normativa interna de obligado cumplimiento): Investigación, monitorización y auditoría de controles establecidos para la prevención de delitos pudiendo establecerse los controles de acceso a las instalaciones, sistemas de información e impresión de documentación para todos los datos de carácter personal bajo responsabilidad de la organización y por lo tanto para todos los sistemas de información de dicha entidad, así como los controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normas laborales, delitos o comportamientos ilícitos.</li> <li>• Gestión del Contacto con el interesado a través de los medios de comunicación corporativos facilitados por la organización (mail y/o teléfono corporativo) a fin de gestionar avisos y coordinar actuaciones por parte de personas relacionadas con la organización, así como facilitando dichos medios a terceros que soliciten el contacto con el interesado. En los casos en los que el interesado lo consienta de forma inequívoca, se podrá llevar a cabo la utilización y facilitación de los medios de contacto privados (mail y teléfonos particulares) a personas relacionadas con la organización y a terceros que lo soliciten.</li> <li>• Fines estadísticos, históricos o científicos: estadísticas e indicadores de desempeño laboral, siniestralidad laboral, absentismo, clima laboral... así como histórico de gestión laboral de la organización</li> <li>• Gestión de Visitas y Videovigilancia de las Instalaciones, así como la seguridad y el cumplimiento normativo en las mismas, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercebimientos o sanciones por incumplimientos de normas de seguridad.</li> <li>• La gestión de la representación de los trabajadores, facilitando la información requerida por sindicatos o representantes de trabajadores para la gestión de la representación sindical objeto de la relación laboral (8.3 ET)</li> <li>• El Envío de Boletines de Noticias, Memorias de Actividad e Información asociada a la Actividad de la Organización.</li> <li>• La gestión y auditoría de los sistemas de gestión, sistemas de cumplimiento normativo y sistemas de seguridad laboral de procesos e instalaciones de la organización</li> <li>• Evidenciar el Cumplimiento Normativo de la Organización ante un tercero que lo requiera: Comunicación a terceros de aquellos datos relativos al interesado que sean requeridos por estos a fin de cumplir con la coordinación de actividades empresariales, evidenciar cumplimiento normativo de la organización y de la normativa interna del tercero y/o para la gestión del acceso a instalaciones. En los casos en los que el interesado lo consienta de forma inequívoca, se podrá llevar a cabo la comunicación de aquella información/documentación requerida por el tercero que no estén explícitamente recogidas en las obligaciones normativas o legales establecidas, sino en la normativa interna del tercero. La negativa a facilitar dicha información provocará la limitación a la participación del interesado en aquellos proyectos en los que la misma sea condición necesaria para su ejecución.</li> </ul>  |
| <b>D8. Base Legitimadora: Especificar Base de Licitud de Tratamiento (Art.6.1 RGD). La legitimación del tratamiento de Los datos personales se realiza por ser necesario para:</b> |   |
| Si   | RGPD: 6.1.b) La ejecución de un contrato o relación negocial: Tratamiento de datos como partes del contrato asociado a la relación con el cedente (relación profesional/laboral y/o de gestión de prácticas), que sean necesarios para su mantenimiento o cumplimiento  |
| Si   | RGPD: 6.1.c) Cumplir con una obligación jurídica: Normativa administrativa, mercantil, tributaria, fiscal, contable y financiera a la que está sujeta el responsable de tratamiento.  |
| Si   | RGPD: 6.1.f) Satisfacer un interés legítimo del Responsable: supuestos de interés legítimo en los que el responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos del incumplidor a terceros a fin de gestionar el cumplimiento normativo y la defensa de los intereses del responsable de tratamiento; Facultad de control legitimada por el art. 20.3 del Estatuto de Trabajadores, que expresamente faculta al empresario a adoptar medidas de vigilancia y control para verificar el cumplimiento por los trabajadores de sus obligaciones laborales, el cumplimiento normativo, la prevención del fraude o la investigación de accidentes o incidentes laborales para lo cual podrá utilizar las imágenes de las cámaras de videovigilancia instaladas, así como los datos de los dispositivos que pudiera instalar de geolocalización en dispositivos electrónicos facilitados por la organización y/o vehículos para las que resulte relevante conocer donde se encuentra la persona y/o el vehículo para la gestión de un proyecto; Prevención del Fraude. Tratamientos con fines de videovigilancia como interés legítimo de la empresa en la protección de sus   |
| Si   | <p>RGPD: 6.1.a) Cumplir las obligaciones de tratamiento por consentimiento inequívoco del interesado. El consentimiento del interesado que nos haya facilitado de forma inequívoca a través de medios normados y/o en el caso que haya marcado las casillas habilitadas a tal efecto en la presente cláusula de protección de datos:</p> <ul style="list-style-type: none"> <li>* Difusión de nuestras mejores prácticas y/o la publicación y/o comunicación de Los datos personales profesionales, currículum y/o material gráfico (videos, grabaciones y fotos asociadas a las actividades desarrolladas por la organización que pueden incorporar su imagen) en medios de comunicación corporativos (por ejemplo y no limitativo, web, redes sociales, boletines informativos, memoria de actividad, reportajes, presencia en medios de comunicación) y/u otros medios de comunicación pública (publicaciones sectoriales y/o reportajes en prensa escrita, TV, ...), como difusión de los resultados de la actividad, promoción y difusión, gestión de campañas, actividades y eventos y/o como acreditación de solvencia técnica ante solicitudes de evidencias de justificación en procesos de licitación, ofertas técnicas, proyectos y subvenciones en los que participe la Autoridad Portuaria de Avilés</li> <li>* Evidenciar el Cumplimiento Normativo de la Organización ante un tercero que lo requiera: Comunicación a terceros de aquellos datos relativos al interesado que sean requeridos por estos a fin de cumplir con la normativa interna del tercero y/o para la gestión del acceso a instalaciones. La negativa a facilitar dicha información provocará la limitación a la participación del interesado en aquellos proyectos en los que la misma sea condición necesaria para su ejecución.</li> <li>* Utilización y facilitación de los medios de contacto privados (mail y teléfonos particulares) a personas relacionadas con la organización y a terceros que lo soliciten</li> <li>* La intermediación o tramitación de gestiones asociadas a pólizas de seguros (tramitación de la designación de beneficiarios respecto a la póliza de accidentes, remisión a aseguradora de información asociada a siniestros para solicitud de indemnización, ...) y pensiones (descuento en nómina de las aportaciones a planes de pensiones y comunicación al promotor del plan, intermediación en el proceso de rescate del plan de pensiones, intermediación en la gestión de incidencias en el cobro de pensiones ...)</li> <li>* La transferencia internacional de Los datos personales en la medida en que sea estrictamente necesario para cumplir con su incorporación a un proyecto en un país fuera de la UE. La no aceptación de esta cláusula impedirá su incorporación al proyecto en dicho país.</li> </ul>  |
| <b>E8. Origen y Procedencia de los Datos: Especificar fuente u origen de los datos de carácter personal que conforman el tratamiento</b>   |   |
| Si   | El propio interesado o su representante legal   |
| Si   | Entidad privada: A través de terceros a los que se contrate los procesos de selección de candidatas a vacantes o puestos de trabajo de AUTORIDAD PORTUARIA DE AVILÉS  |
| <b>F8. Colectivo/s de Interesados : Identificación del colectivo/s del que se tratan datos</b>   |   |
| Personal laboral y/o de gestión de prácticas   |   |
| <b>G8. Estructura de Datos Personales: Especificar Tipología de Datos objeto de tratamiento</b>  |   |
| Si   | Categoría de Datos objeto de tratamiento  |
| Si   | <p><b>Categorías especiales de datos personales:</b> <i>datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física</i></p> <p>Puede contener datos especialmente protegidos relativos a Situación de Discapacidad Reconocida tanto del interesado como de familiares a su cargo (Mod. 145), Datos de afiliación sindical, Datos Situación de Baja - Mantenimiento Enfermedad/Accidente/Maternidad, así como datos relativos a condenas e infracciones (en caso de embargos) y por el requerimiento del certificado de penales.</p> <p>Contiene los siguientes datos relativos a: Datos Situación de aptitud, Datos de Situación de Baja - Mantenimiento Enfermedad/Accidente/Maternidad y Situación de Discapacidad Reconocida tanto del interesado como de familiares a su cargo (Mod. 145);</p> <p>En la medida en que el candidato informe sobre una condición de discapacidad o solicite indemnización por accidente, se podrán requerir los certificados que así lo acrediten. En caso de ausencia del trabajador por motivos médicos, propios o de familiares, gestión de solicitud de justificante médico asociado.</p>   |
| Si   | <p><b>Datos identificativos:</b> Nombre y apellidos, NIF/DNI, Nº Seguridad Social / Mutualidad, Imagen/Voz, Firma, Datos huella parcial, Dirección, Teléfono particular, Dirección correo particular, Otros datos de carácter identificativo</p> <p>DNI, Datos identificativos y de contacto; fecha y lugar de nacimiento, edad, sexo Imagen y control de Acceso a Instalaciones</p>  |
| Si   | <p><b>Datos académicos y profesionales:</b> Formación y titulaciones, Experiencia profesional, Historial de estudiante, Cargo/puesto/función y organización en la que ha desempeñado dicha función, Pertenencia a colegios o a asociaciones profesionales, Otros datos académicos y profesionales</p> <p>Datos académicos y profesionales relativos a formación, titulaciones y experiencia profesional;</p>  |

|  |  |  |
|--|--|--|
| Si   | Circunstancias personales: Datos de estado civil, Datos de familia, Fecha de nacimiento, Lugar de nacimiento, Edad, Sexo, Nacionalidad, Lengua materna, Características físicas o antropométricas (no biométricos unívocos), Otros datos de circunstancias personales  | Datos personales asociados al estado civil, datos de familia, nacionalidad.  |
| Si   | Circunstancias sociales: Características de alojamiento, vivienda, Situación militar, Propiedades o posesiones, Aficiones y estilo de vida, Pertenece a clubes o asociaciones, Licencias, permisos, autorizaciones, Otros datos de circunstancias sociales   | Carnet de conducir. Permiso de trabajo, Ocio y aficiones.  |
| Si   | Detalles de empleo: Profesión, Puesto de trabajo, Datos no económicos de nómina, Historial del trabajador, Otros datos de detalle de empleo  | Vida laboral, copia de contratos, Datos de Estado laboral; Otros datos (Aspiraciones profesionales).   |
| Si   | Económicos, financieros y de seguros: Ingresos, rentas, Inversiones, bienes patrimoniales, Créditos, préstamos, avales, Datos bancarios, Planes de pensiones, jubilación, Datos económicos de nómina, Datos deducciones impositivas/impuestos, Seguros, Hipotecas, Subsidios, beneficios, Historial créditos, Tarjetas crédito, Otros datos económicos, financieros y de seguros   | Datos bancarios y de nómina, bonificaciones, seguros pensiones y pagos   |
| Si   | Otro tipo de datos: Datos de tráfico conexiones a internet, correos electrónicos y llamadas enviadas o recibidas de telefonía fija y móvil a medios de comunicación corporativos facilitados por la organización.  |  |
| <b>H8. Sistema de Tratamiento: Especificar método de tratamiento de la información</b>   |  |  |
| Si   | Mixto: Soporte papel, soporte informático/magnético.   |  |
| <b>I8. Cesión o comunicación de datos: Especificar entidades destinatarias a quienes se ha comunicado o van a comunicarse los datos de carácter personal</b>               |  |  |
| Si   | Organizaciones o personas directamente contratadas por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento: terceros a los que se contrate los procesos de selección de candidatos a vacantes o puestos de trabajo de Autoridad Portuaria de Avilés (personal de Registro, Secretaría General, RRHH, miembros del tribunal y, cuando se contrata con un externo la realización de servicios (pej): entrevistas y psicotécnico, pruebas dentro del proceso (ej, pruebas de informática o de inglés,...), Empresas de Mantenimiento Informático, Empresas relacionadas con la gestión de viajes y reservas, alquiler de vehículos, gestión de visados y pasaportes, Asesoría Jurídica, Entidades de Gestión de Cobro y Seguro de Crédito, Auditores de Gestión y/o de Cumplimiento Normativo.  |  |
| Si   | Organismos u órganos de la Administración Pública con competencias en las materias objeto de las finalidades del tratamiento: Instituto Nacional de Seguridad Social; Ministerio de Trabajo; Autoridad sanitaria en el marco de la Ley General de Sanidad, a la inspección de trabajo, a la autoridad laboral, así como la cesión de datos requeridos por jueces y tribunales, o las necesarias en caso de urgencia médica, o en estudios epidemiológicos  |  |
| Si   | Entidades Financieras: Domiciliación nóminas.  |  |
| Si   | Entidades Aseguradoras: Seguros de salud, accidente y planes de pensiones en beneficio de sus empleados, bien de modo voluntario, bien en virtud de lo pactado en un Convenio Colectivo. La empresa se limita a facilitar, previa información a los trabajadores, los datos de éstos a la aseguradora o gestora, para que a su vez ésta inicie su relación con el asegurado o participe del plan y recabe los datos que resulten necesarios, así como poniendo a disposición del trabajador la ficha o solicitud de adhesión al seguro de vida colectivo que éste deberá cumplimentar con cuantos datos resulten necesarios, por ejemplo en relación con los beneficiarios.  |  |
| Si   | Fuerzas y Cuerpos de Seguridad:<br>• En la medida en que fuera requerido un derecho de acceso justificado en la investigación de un incumplimiento normativo. En caso de requerimiento judicial.<br>• Juzgados en caso de embargos por pensiones (y otras entidades que puedan llevar a cabo embargos, por ejemplo Hacienda, estatal o autonómica, en el supuesto de multas)   |  |
| Si   | representantes de los trabajadores: Coordinación de seguridad y salud, Auditores externos, Comité de empresa y secciones sindicales. A los representantes de trabajadores para la gestión de la representación sindical objeto de la relación laboral (8.3 del ET), el empresario está obligado a entregar a los representantes de los trabajadores una copia básica de todos los contratos que se celebren por escrito salvo aquellos de carácter especial correspondientes a personal de alta dirección. Así mismo, deberá entregarse copia de TC2 como control sindical de la actuación de la empresa y la garantía del cumplimiento de los deberes empresariales en supuestos de subcontratación. El comité de empresa de la Autoridad Portuaria maneja datos personales de la plantilla de la entidad: censo electoral (en el que aparecen DNI, edad, etc) y otros datos relativos a la clasificación profesional de los trabajadores. Se informa de la formación que reciben los trabajadores (cursos bonificados) y se les facilita un listado de los alumnos que participan en dichos cursos que incluyen datos personales de los mismos). Firman también las copias básicas de los contratos de trabajo. Los miembros del comité de empresa y éste en su conjunto, así como, en su caso, los expertos que les asistan, deberán observar el deber de sigilo con respecto a aquella información que, en legítimo y objetivo interés de la empresa o del centro de trabajo, les haya sido expresamente comunicada con carácter reservado. (art. 65.2 Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores): "La documentación entregada se declara expresamente de carácter reservado, de acuerdo con el apartado 2 del artículo 65 del Estatuto de los Trabajadores, en virtud del cual, los miembros del comité de empresa, y éste en su conjunto, observarán sigilo profesional en todo lo referente a los párrafos 1.º, 2.º, 3.º, 4.º y 5.º del apartado 1 del artículo 64, aún después de dejar de pertenecer al comité de empresa y en especial en todas aquellas materias sobre las que la dirección señale expresamente el carácter reservado. En todo caso, ningún tipo de documento entregado por la organización al comité podrá ser utilizado fuera del estricto ámbito de aquélla y para distintos fines de los que motivaron su entrega. Adicionalmente, en el ámbito de la normativa vigente de Protección de Datos de Carácter Personal, el trabajador se compromete, durante su relación con la organización e incluso después de haber finalizado esta relación, a mantener absoluta confidencialidad y discreción sobre la información obtenida en el ejercicio de su trabajo en lo que se refiere a Datos de Carácter Personal de trabajadores, clientes, empresas, etc."  |  |
| Si   | Otros:<br>• Comité de Préstamos al personal por adquisición de vivienda y por necesidades urgentes: Estudio y concesión por parte de comité de préstamos, formado por trabajadores de la Autoridad Portuaria, de la solicitud correspondiente con la documentación acreditativa en su caso (pej): contrato de compraventa o presupuestos para reforma de viviendas, ...).<br>• Puertos del Estado: Solicitudes de autorización de una jubilación parcial, Listados de datos de trabajadores con edad próxima a la jubilación, Listados de personal que trabajan en un determinado servicio, como puede ser flota o policía portuario.<br>• Igaes: Como consecuencia de la auditoría de la actividad de la Autoridad Portuaria se facilita: Trabajadores que han sido alta y baja durante el ejercicio (nombre y apellidos y fecha del alta o de la baja), Listado de trabajadores, categoría profesional, fecha de antigüedad), tipo de contrato, Contratos concretos de personas en el periodo de referencia, Recibos de nómina de trabajadores<br>• Centros de estudios en el caso de las becas.<br>• Entidad que realiza la formación (para la elaboración de presupuesto, gestión de la acción formativa, informe final y el diploma acreditativo o el informe, en su caso, respecto a la no superación del curso por un trabajador y/o la tramitación de la bonificación de Fundae.<br>• Servicios de Prevención de Riesgos Laborales: el tratamiento por parte de los servicios de prevención de riesgos laborales del historial médico, consecuencia de los reconocimientos médicos realizados a los trabajadores, deberá limitarse a las previsiones del artículo 22.4 de la LPRL. En este sentido, se prohíbe el acceso a la información médica obtenida al amparo de lo dispuesto en la LPRL por parte del empresario o de cualquier tercero, incluidas las personas u órganos con responsabilidades en materia de prevención, distintos del "personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores", con la única excepción de las conclusiones derivadas de dicho seguimiento en cuanto a la aptitud de los trabajadores para el desempeño del puesto de trabajo.<br>• Colaboradores, Eventos, Proyectos y Subvenciones en los que participe la organización para la justificación técnica o económica de las mismas, Medios de Comunicación para la Promoción de las Actividades de la Organización,<br>• Terceros que soliciten Los datos personales para la coordinación de actuaciones en relación con su puesto o con el proyecto o servicio en el que participa, el acceso a las instalaciones y/o a fin de acreditar la solvencia técnica en la presentación de ofertas, el cumplimiento de las obligaciones normativas de la organización o la aptitud para el desempeño de su función,<br>• Empresas de Trabajo Temporal, así como Organizaciones y Tutores de las mismas con las que se han establecido convenios de colaboración para prácticas formativas.<br>• Canal de Denuncias Compliance (Las denuncias sobre vulneración de normativa y código de conducta son transmitidas a la Unidad de Cumplimiento Normativo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.<br>• Conforme a lo establecido en la LOPDGD, los órganos y organismos del Sector Público pueden comunicar los datos personales de los administrados a sujetos de derecho privado que lo soliciten(a) o bien cuando cuenten con el consentimiento de los administrados. b) o bien, cuando aparezca que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos. |  |
| <b>J8. Transferencias internacionales de Datos (TID) (Arts.66 y 70 RLOPD): Países no UE a los que se realice o esté previsto realizar una comunicación de datos</b>        |  |  |
| Si   | Observaciones: No se realizan transferencias internacionales de datos  |  |
| <b>K8. Plazos previstos para supresión de datos: Especificar plazo de expurgo y/o cancelación/bloqueo del dato tras finalizar la finalidad que legitimó el tratamiento</b> |  |  |
| Si   | Datos a Conservar en Tratamientos Específicos y Referencia Legal de base   | Plazo de Conservación Exigible   |
| Si   | <b>Criterio:</b> Los datos personales serán conservados en nuestros sistemas mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento normativo por parte del interesado o de la Organización.  |  |
| Si   | <b>Videovigilancia:</b> Las imágenes/sonidos captados por los sistemas de video vigilancia serán cancelados en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras).   | Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art.22 LOPDGD) - 30 días. |
| Si   | <b>Control Acceso a Edificios:</b> Los datos incluidos en los ficheros automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios).  | 1 Mes  |
| Si   | <b>Documentación de carácter laboral o relacionada con seguridad social:</b> Documentación o los registros o soportes informáticos en que se hayan transmitido los correspondientes datos que acrediten el cumplimiento de las obligaciones en materia de afiliación, altas, bajas o variaciones que, en su caso, se produjeran en relación con dichas materias, así como los documentos de cotización y los recibos justificativos del pago de salarios y del pago delegado de prestaciones (Art. 21 del RD Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social).<br>Añadir toda la documentación contractual: El RD 1424/2002, de 27 de diciembre, por el que se regula la comunicación del contenido de los contratos y de sus copias básicas, nada establece al respecto, por lo que analógicamente se aplica el presente.  | 4 Años   |
| Si   | <b>Documentación Contable y Fiscal - A efectos Fiscales:</b> Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria).<br>Plazo prescripción de Delitos Fiscales asociados a la comprobación de las bases o cuotas compensadas o pendientes de compensación o de deducciones aplicadas o pendientes de aplicación y a Delitos contra la Hacienda Pública y la Seguridad Social - Art. 66 bis Ley General Tributaria y Código Penal, respectivamente.   | 4 Años. Prescripción infracciones 10 años  |
| Si   | <b>Documentación Contable y Fiscal - A efectos Fiscales:</b> Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria)  | 4 Años   |
| Si   | <b>Datos de tráfico relativos a conexiones a internet, correos electrónicos y llamadas enviadas o recibidas de telefonía fija y móvil:</b> Identificación de usuario, dirección IP (origen/destino), número de teléfono, IMSI e IMEI (origen/destino), fecha y hora de la comunicación (inicio/fin), identificación del tipo de servicio o comunicación utilizado (voz, datos, SMS o MMS, ...), .. (Art. 5 Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones).  | 1 Año  |

|   |  |   |
|---|--|---|
| SI  | <p><b>Canal de Denuncias:</b> Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.</p>   | <p>Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.</p> |
| SI  | <p><b>Documentación de Prevención de Riesgos Laborales</b> - Documentación sobre información y formación a los trabajadores. Expedientes de accidentes laborales o enfermedades profesionales (RD Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social) - 5 años</p>   | <p>5 Años</p>   |
| SI  | <p><b>Observaciones:</b> CRITERIOS DE SUPRESIÓN Y BLOQUEO DE LOS DATOS: conforme a lo establecido en el Artículo 32 de la LOPDGD, la Autoridad Portuaria de Avilés estará obligado a bloquear los datos cuando el afectado proceda a su rectificación o supresión.<br/>El bloqueo de los datos consiste en la identificación y reserva de los mismos, 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 competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.</p>  |   |
| <p><b>L8. Medidas de Seguridad: Identificación de Medidas técnicas y organizativas aplicables al tratamiento</b></p>  |  |   |
| <p style="text-align: center;"><u>Ver "Medidas de Seguridad" del Fichero</u></p> <p>La Autoridad Portuaria de Avilés toma todas las medidas necesarias para guardar Los datos personales personales de forma privada y segura. Solo personas autorizadas de la Autoridad Portuaria de Avilés, personal autorizado de encargados de tratamiento o personal autorizado de nuestra organización (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a Los datos personales personales. Se exige a todo el personal de la Autoridad Portuaria de Avilés que tiene acceso a Los datos personales personales que se comprometa a respetar la Política de Privacidad y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a Los datos personales personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que los terceros que puedan tener acceso a Los datos personales personales los mantengan de forma segura. Para asegurarse de que Los datos personales personales están protegidos, la Autoridad Portuaria de Avilés dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados. La Autoridad Portuaria de Avilés ha formalizado acuerdos para garantizar que tratamos Los datos personales personales correctamente y de acuerdo con la ley de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros.</p> |  |   |
| <p><b>A9. Nombre del Tratamiento: Identificación del tratamiento de datos de la organización (pej: Personal, Clientes, Proveedores, Videovigilancia, ...)</b></p>   |  |   |
| <p style="text-align: center;"><b>MIEMBROS DE ÓRGANOS DE ADMINISTRACIÓN</b></p>   |  |   |
| <p><b>B9. Identificación del Responsable y Contacto DPO: Identificación de entidad responsable de tratamiento y (en su caso) datos contacto DPO nombrado</b></p>  |  |   |
| <p><b>C1. Tipificación/Descripción de la Finalidad/es: Especificar finalidad/es del Tratamiento</b>   <span style="float: right;"><a href="mailto:dpo@puertoaviles.es">dpo@puertoaviles.es</a></span></p>   |  |   |
| <p><b>C9. Tipificación/Descripción de la Finalidad/es: Especificar finalidad/es del Tratamiento y Usos previstos</b></p>  |  |   |
| SI  | <ul style="list-style-type: none"> <li>• Gestión de Convocatoria, Comunicación, Organización y Funcionamiento del Consejo de Administración.</li> <li>• Tramitación de los asuntos a debatir en los Consejos, adopción de acuerdos, así como gestión fiscal y bancaria asociada a la retribución de las dietas de asistencia, creación y funcionamiento del órgano de administración y de sus miembros.</li> <li>• Para la gestión de actos y contratación formal con clientes, proveedores, trabajadores, entidades financieras y organismos públicos que requieran de firma autorizada en nombre de la organización.</li> <li>• Gestión administrativa asociada a la generación de la documentación societaria. Transmisión de documentos del orden del día mediante aplicación de Gobierno Corporativo</li> <li>• Gestión de Visitas y Videovigilancia de las Instalaciones, así como de la seguridad y el cumplimiento normativo en las mismas, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercibimientos o sanciones por incumplimientos de normas de seguridad.</li> <li>• Atención a consultas y solicitudes: Gestión de Respuesta a Consultas, Reclamaciones o Incidencias, Solicitudes de Información, Recursos y/o de Actividades.</li> <li>• Gestión del Cumplimiento Normativo (normativa aplicable así como normativa interna de obligado cumplimiento): Investigación, monitorización y auditoría de controles establecidos para la prevención de delitos pudiendo establecerse los controles de acceso a las instalaciones, así como los controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de incidentes que pudieran producirse, así como incumplimientos de normativa, delitos o comportamientos ilícitos.</li> <li>• El contacto y envío de comunicaciones personales, encuestas, invitaciones a eventos, así como para informarle periódicamente de novedades, noticias e información corporativa, proyectos y servicios de la organización* que pudieran ser de su interés tanto por medios escritos, telefónicos como electrónicos a través de los medios de comunicación facilitados, si así nos lo ha consentido inequívocamente.</li> <li>• La publicación en medios de comunicación corporativos y/u otros medios de comunicación pública, de material gráfico que puede contener su imagen y/o referencia asociada a su condición con miembro del Consejo de Administración en material promocional, de justificación de solvencia técnica y/o justificación en eventos, proyectos y subvenciones en los que participe la organización, si así nos lo ha consentido inequívocamente.</li> </ul>  |   |
| SI  | <ul style="list-style-type: none"> <li>• Gestión de la Calidad de procesos y actividades, así como la evaluación de los resultados de satisfacción/percepción y rendimiento de los grupos de interés de la organización. Realización de encuestas (satisfacción, clima laboral y/o psicosociales)</li> <li>• Gestión de solvencia técnica en presentación ofertas y/o solicitud, gestión y justificación de campañas, actividades, eventos, concursos, proyectos y subvenciones en los que participe la organización, para lo cual podrá facilitarse el currículum profesional y/o documentación/información relativa al interesado relacionada con la relación profesional/laboral y/o gestión de prácticas como evidencia o justificación de cumplimiento. En los casos en los que el interesado lo consenta de forma inequívoca, se podrá llevar a cabo la utilización y facilitación del currículum particular del interesado a personas relacionadas con la organización y a terceros que lo soliciten.</li> <li>• Gestión del Cumplimiento Normativo (normativa aplicable así como normativa interna de obligado cumplimiento): Investigación, monitorización y auditoría de controles establecidos para la prevención de delitos pudiendo establecerse los controles de acceso a las instalaciones, sistemas de información e impresión de documentación para todos los datos de carácter personal bajo responsabilidad de la organización y por lo tanto para todos los sistemas de información de dicha entidad, así como los controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normas laborales, delitos o comportamientos ilícitos.</li> <li>• Gestión del Contacto con el interesado a través de los medios de comunicación corporativos facilitados por la organización (mail y/o teléfono corporativo) a fin de gestionar avisos y coordinar actuaciones por parte de personas relacionadas con la organización, así como facilitando dichos medios a terceros que solicitasen el contacto con el interesado. En los casos en los que el interesado lo consenta de forma inequívoca, se podrá llevar a cabo la utilización y facilitación de los medios de contacto privados (mail y teléfonos particulares) a personas relacionadas con la organización y a terceros que lo solicitasen.</li> <li>• Fines estadísticos, históricos o científicos: estadísticas e indicadores de desempeño laboral, siniestralidad laboral, absentismo, clima laboral..., así como histórico de gestión laboral de la organización</li> <li>• Gestión de Visitas y Videovigilancia de las Instalaciones, así como la seguridad y el cumplimiento normativo en las mismas, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercibimientos o sanciones por incumplimientos de normas de seguridad.</li> <li>• La gestión de la representación de los trabajadores, facilitando la información requerida por sindicatos o representantes de trabajadores para la gestión de la representación sindical objeto de la relación laboral (8.3 ET)</li> <li>• El Envío de Boletines de Noticias, Memorias de Actividad e Información asociada a la Actividad de la Organización.</li> <li>• La gestión y auditoría de los sistemas de gestión, sistemas de cumplimiento normativo y sistemas de seguridad laboral de procesos e instalaciones de la organización</li> <li>• Evidenciar el Cumplimiento Normativo de la Organización ante un tercero que lo requiera: Comunicación a terceros de aquellos datos relativos al interesado que sean requeridos por estos a fin de cumplir con la coordinación de actividades empresariales, evidenciar cumplimiento normativo de la organización y de la normativa interna del tercero y/o para la gestión del acceso a instalaciones. En los casos en los que el interesado lo consenta de forma inequívoca, se podrá llevar a cabo la comunicación de aquella información/documentación requerida por el tercero que no estén explícitamente recogidas en las obligaciones normativas o legales establecidas, sino en la normativa interna del tercero. La negativa a facilitar dicha información provocará la limitación a la participación del interesado en aquellos proyectos en los que la misma sea condición necesaria para su ejecución.</li> <li>• La Gestión de la solicitud de comunicación del recibo de nómina en la dirección de correo electrónico facilitada por el interesado</li> <li>• La Gestión de ropa laboral y EPI's (adquisición y facilitación de tallas para su puesta a disposición por parte de las organizaciones contratadas para su provisión)</li> </ul> |   |
| <p><b>D9. Base Legitimadora: Especificar Base de Licitud de Tratamiento (Art.6.1 RGPD). La legitimación del tratamiento de Los datos personales se realiza por ser necesario para:</b></p>  |  |   |
| SI  | <p>RGPD: 6.1.b) La ejecución de un contrato o relación negocial: Acuerdo societario</p>  |   |
| SI  | <p>RGPD: 6.1.c) Cumplir con una obligación jurídica: Normativa de régimen económico y de prestación de servicios de los puertos de interés general y legislación de transparencia, acceso a la información pública y buen gobierno) y la misión de interés público otorgada por la Ley de Puertos del Estado y de la Marina Mercante: Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por Real Decreto Legislativo 212011 y Reglamento de Servicios de Policía y Régimen del Puerto</p>  |   |
| SI  | <p>RGPD: 6.1.f) Satisfacer un interés legítimo del Responsable: publicación de datos con fines de transparencia y responsabilidad; interés público general o interés de un tercero, interés legítimo de la entidad en la protección de sus activos, Prevención del Fraude y supuestos de interés legítimo en los que el responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos del inculpidor a terceros a fin de gestionar el cumplimiento normativo y la defensa de los intereses del responsable de tratamiento.</p>   |   |

|  |  |  |
|--|--|--|
| SI   | <p>RGPD: 6.1.a) Cumplir las finalidades del tratamiento por consentimiento inequívoco del interesado: El consentimiento del interesado que nos haya facilitado de forma inequívoca a través de medios formales y/o en el caso que haya marcado las casillas habilitadas a tal efecto en la presente cláusula de protección de datos:</p> <p>* La comunicación de Los datos personales en relación con la incidencia a los siguientes autorizados:<br/> D/D*: ..... - con NIF ..... - medio contacto/teléfono: .....<br/> D/D*: ..... - con NIF ..... - medio contacto/teléfono: .....</p> <p>* El contacto y envío de comunicaciones personales, encuestas, invitaciones a eventos, así como para informarle periódicamente de novedades, noticias e información corporativa, proyectos y servicios de la organización* que pudieran ser de su interés tanto por medios escritos, telefónicos como electrónicos a través de los medios de comunicación facilitados.</p> <p>* La publicación en medios de comunicación corporativos y/u otros medios de comunicación pública, de material gráfico que puede contener su imagen y/o referencia asociada a su condición con miembro del Consejo de Administración en material promocional, de justificación de solvencia técnica y/o justificación en eventos, proyectos y subvenciones en los que participe la organización.</p> |  |
| <b>E9. Origen y Procedencia de los Datos: Especificar fuente u origen de los datos de carácter personal que conforman el tratamiento</b>                                   |  |  |
| SI   | El propio interesado o su representante legal  |  |
| <b>F9. Colectivo/s de Interesados : Identificación del colectivo/s del que se tratan datos</b>   |  |  |
| Miembros de Órganos de Administración de la APA  |  |  |
| <b>G9. Estructura de Datos Personales: Especificar Tipología de Datos objeto de tratamiento</b>  |  |  |
| SI   | Categoría de Datos objeto de tratamiento   | Especificación   |
| No   | <p><b>Categorías especiales de datos personales:</b> <i>datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física</i></p>  | <p>No contiene datos sensibles, salvo en los casos en los que el titular sea beneficiario de condiciones especiales y haya de facilitar registros que permitan acreditar o justificar el cumplimiento de dicha condición. Los datos que pudieran derivarse de posibles incumplimientos que pudieran incorporar datos relativos a condenas e infracciones penales estarían incorporados en el tratamiento "Infractores". Los datos potencialmente sensibles relativos a incidentes, accidentes o daños recibidos o causados por la Autoridad Portuaria estarían incorporados en el tratamiento "Incidencias y Responsabilidad Patrimonial"</p>  |
| SI   | <p><b>Datos identificativos:</b> <i>Nombre y apellidos, NIF/DNI, N° Seguridad Social / Mutualidad, Imagen/Voz, Firma, Datos huella parcial, Dirección, Teléfono particular, Dirección correo particular, Otros datos de carácter identificativo</i></p>  | Datos de carácter identificativo (DNI/NIF, nombre y apellidos, dirección, firma) y participación societaria.   |
| SI   | <p><b>Económicos, financieros y de seguros:</b> <i>Ingresos, rentas, Inversiones, bienes patrimoniales, Créditos, préstamos, avales, Datos bancarios, Planes de pensiones, jubilación, Datos económicos de nómina, Datos deducciones impositivas/impuestos, Seguros, Hipotecas, Subsidios, beneficios, Historial créditos, Tarjetas crédito, Otros datos económicos, financieros y de seguros</i></p>  | Datos económicos y financieros (datos bancarios)   |
| <b>H9. Sistema de Tratamiento: Especificar método de tratamiento de la información</b>   |  |  |
| SI   | Mixto: Soporte papel, soporte informático/magnético.   |  |
| <b>I9. Cesión o comunicación de datos: Especificar entidades destinatarias a quienes se ha comunicado o van a comunicarse los datos de carácter personal</b>               |  |  |
| SI   | Organizaciones o personas directamente contratadas por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento: Internamente en la APA, intervienen los departamentos de Secretario General, Recursos Humanos, y Económico-Financiero, así como Entidades de mantenimiento informático, mantenimiento y soporte del registro y de la sede electrónica de la Autoridad Portuaria, Servicio de Asesoramiento en Sistema de Riesgos Penales.  |  |
| SI   | Organismos u órganos de la Administración Pública con competencias en las materias objeto de las finalidades del tratamiento: Administraciones Públicas [AEAT (Ley General Tributaria), IGAE Y Tribunal de Cuentas (Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante), Otros Órganos de la Administración del Estado, Tribunal de Cuentas o equivalente autonómico, Órganos Judiciales, Abogacía del Estado, Intervención de la Administración del Estado, Puertos del Estado, así como en su caso juzgados y tribunales y a cuantas Instituciones y Organismos proceda de acuerdo con la legislación vigente, así como a entidades públicas en el ámbito de sus competencias, por obligación legal.  |  |
| SI   | Entidades Financieras: Entidad bancaria donde se ha establecido la cuenta corriente de gestión de dietas y retribuciones.  |  |
| SI   | Entidades Aseguradoras: Seguros de salud, accidente y planes de pensiones en beneficio de sus empleados, bien de modo voluntario, bien en virtud de lo pactado en un Convenio Colectivo. La empresa se limita a facilitar, previa información a los trabajadores, los datos de éstos a la aseguradora o gestora, para que a su vez ésta inicie su relación con el asegurado o participe del plan y recabe los datos que resulten necesarios, así como poniendo a disposición del trabajador la ficha o solicitud de adhesión al seguro de vida colectivo que éste deberá cumplimentar con cuantos datos resulten necesarios, por ejemplo en relación con los beneficiarios.  |  |
| SI   | Fuerzas y Cuerpos de Seguridad: En la medida en que fuera requerido un derecho de acceso justificado en la investigación de un incumplimiento normativo. En caso de requerimiento judicial.  |  |
| SI   | <p>Otros:</p> <ul style="list-style-type: none"> <li>• Puertos del Estado: información sobre el número de asistencias y retribución del consejero de Puertos del Estado.</li> <li>• Canal de Denuncias Compliance (Las denuncias sobre vulneración de normativa y código de conducta son transmitidas a la Unidad de Cumplimiento Normativo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.</li> <li>• Conforme a lo establecido en la LOPDGDD, los órganos y organismos del Sector Público pueden comunicar los datos personales de los administrados a sujetos de derecho privado que lo soliciten: a) o bien cuando cuenten con el consentimiento de los administrados.b) o bien, cuando aprecien que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos.</li> </ul>                |  |
| <b>J9. Transferencias internacionales de Datos (TID) (Arts.66 y 70 RLOPD): Países no UE a los que se realice o esté previsto realizar una comunicación de datos</b>        |  |  |
| SI   | Observaciones: No se realizan transferencias internacionales de datos  |  |
| <b>K9. Plazos previstos para supresión de datos: Especificar plazo de expurgo y/o cancelación/bloqueo del dato tras finalizar la finalidad que legitimó el tratamiento</b> |  |  |
| SI   | Datos a Conservar en Tratamientos Específicos y Referencia Legal de base   | Plazo de Conservación Exigible   |
| SI   | Criterio: Los datos personales serán conservados en nuestros sistemas mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento normativo por parte del interesado o de la Organización.   |  |
| SI   | <p><b>Videovigilancia:</b> <i>Las imágenes/sonidos captados por los sistemas de video vigilancia serán cancelados en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras).</i></p>   | <p>Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art.22 LOPDGDD).</p> |
| SI   | <p><b>Control Acceso a Edificios:</b> <i>Los datos incluidos en los ficheros automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios).</i></p>  | 1 Mes  |
| SI   | <p><b>Documentación Contable y Fiscal - A efectos Fiscales:</b> <i>Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria).</i></p> <p><i>Plazo prescripción de Delitos Fiscales asociados a la comprobación de las bases o cuotas compensadas o pendientes de compensación o de deducciones aplicadas o pendientes de aplicación y a Delitos contra la Hacienda Pública y la Seguridad Social - Art. 66 bis Ley General Tributaria y Código Penal, respectivamente.</i></p>  | 4 Años. Prescripción infracciones 10 años  |



|  |   |  |
|--|---|--|
| Si   | Documentación Contable y Fiscal - A efectos Fiscales: Los libros de contabilidad y otros libros registros obligatorios según la normativa tributaria que proceda (IRPF, IVA, IS, etc), así como los soportes documentales que justifiquen las anotaciones registradas en los libros (incluidos los programas y archivos informáticos y cualquier otro justificante que tengan trascendencia fiscal), deben conservarse, al menos, durante el periodo en que la Administración tiene derecho a comprobar e investigar y, en consecuencia, a liquidar deuda tributaria (Arts. 66 a70 Ley General Tributaria)  | 4 Años   |
| Si   | Datos de tráfico relativos a conexiones a internet, correos electrónicos y llamadas enviadas o recibidas de telefonía fija y móvil: Identificación de usuario, dirección IP (origen/destino), número de teléfono, IMSI e IMEI (origen/destino), fecha y hora de la comunicación (inicio/fin), identificación del tipo de servicio o comunicación utilizado (voz, datos, SMS o MMS, ...), .. (Art. 5 Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones).  | 1 Año  |
| Si   | Canal de Denuncias: Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD.  | Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGD. |
| Si   | Otros: Los datos personales serán conservados en nuestros sistemas de información mientras se mantenga vigente la relación de colaboración durante los plazos de conservación establecidos por la normativa vigente, así como los plazos legales o contractualmente previstos para el ejercicio o prescripción de cualquier acción por parte del interesado o de la Organización.   |  |
| Si   | Observaciones: CRITERIOS DE SUPRESIÓN Y BLOQUEO DE LOS DATOS: conforme a lo establecido en el Artículo 32 de la LOPDGD, la Autoridad Portuaria de Avilés estará obligado a bloquear los datos cuando el afectado proceda a su rectificación o supresión.<br>El bloqueo de los datos consiste en la identificación y reserva de los mismos, 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 competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.  |  |
| <b>L9. Medidas de Seguridad: Identificación de Medidas técnicas y organizativas aplicables al tratamiento</b>  |   |  |
| <u>Ver "Medidas de Seguridad" del Fichero</u>  |   |  |
| La Autoridad Portuaria de Avilés toma todas las medidas necesarias para guardar Los datos personales personales de forma privada y segura. Solo personas autorizadas de la Autoridad Portuaria de Avilés, personal autorizado de encargados de tratamiento o personal autorizado de nuestra organización (que tienen la obligación legal y contractual de guardar toda la información de forma segura) tienen acceso a Los datos personales personales. Se exige a todo el personal de la Autoridad Portuaria de Avilés que tiene acceso a Los datos personales personales que se comprometa a respetar la Política de Privacidad y la normativa de protección de datos y a todos los empleados de Terceros que tienen acceso a Los datos personales personales que firmen los compromisos de confidencialidad en los términos establecidos en la legislación vigente. Además, se asegura contractualmente que los terceros que puedan tener acceso a Los datos personales personales los mantengan de forma segura. Para asegurarse de que Los datos personales personales están protegidos, la Autoridad Portuaria de Avilés dispone de un entorno de seguridad IT y adopta las medidas necesarias para evitar accesos no autorizados.<br>La Autoridad Portuaria de Avilés ha formalizado acuerdos para garantizar que tratamos Los datos personales personales correctamente y de acuerdo con la ley de protección de datos. Estos acuerdos reflejan las respectivas funciones y responsabilidades en relación con usted, y contemplan qué entidad se encuentra en la mejor posición para cumplir con sus necesidades. Estos acuerdos no afectan a sus derechos en virtud de la ley de protección de datos. Para obtener más información sobre estos acuerdos, no dude en ponerse en contacto con nosotros. |   |  |
| <b>A10. Nombre del Tratamiento: Identificación del tratamiento de datos de la organización (pe): Personal, Clientes, Proveedores, Videovigilancia, ...)</b>  |   |  |
| <b>VIDEOVIGILANCIA Y REGISTRO DE ACCESOS</b>   |   |  |
| <b>B10. Identificación del Responsable y Contacto DPO: Identificación de entidad responsable de tratamiento y (en su caso) datos contacto DPO nombrado</b>   |   |  |
| AUTORIDAD PORTUARIA DE AVILÉS  |   | dpo@puertoaviles.es  |
| <b>C10. Tipificación/Descripción de la Finalidad/es: Especificar finalidad/es del Tratamiento y Usos previstos</b>   |   |  |
| Si   | <ul style="list-style-type: none"> <li>Registro de Accesos y Videovigilancia de las Instalaciones, así como de la seguridad y el cumplimiento normativo en las mismas, la investigación de posibles incidentes o accidentes, gestión de seguros asociados y gestión de apercibimientos o sanciones por incumplimientos de normas de seguridad, a través del sistema de videovigilancia.</li> <li>Verificar el cumplimiento por parte de trabajadores de sus obligaciones y deberes laborales conforme al artículo 20.3 del Estatuto de los Trabajadores que faculta al empresario a adoptar medidas de vigilancia y control al efecto (controles relativos al uso de las imágenes captadas por los sistemas de videovigilancia para la investigación de los accidentes y/o incidentes que pudieran producirse, así como incumplimientos de normas laborales, delitos o comportamientos ilícitos).</li> <li>Gestión de la seguridad y salud (prevención de riesgos laborales y vigilancia de la seguridad) y evaluación de cumplimiento</li> <li>Control horario y/o presencial o de asistencia y monitorización del desempeño funcional</li> </ul>  |  |
| <b>D10. Base Legitimadora: Especificar Base de Licitud de Tratamiento (Art.6.1 RGPD). La legitimación del tratamiento de Los datos personales se realiza por ser necesario para:</b>   |   |  |
| Si   | <p>RGPD: 6.1.f) Satisfacer un interés legítimo del Responsable:</p> <ul style="list-style-type: none"> <li>Seguridad y supuestos de interés legítimo en los que el responsable pudiera ser parte perjudicada y fuera necesario el tratamiento y la comunicación de los datos del incumplidor a terceros a fin de gestionar el cumplimiento normativo y la defensa de los intereses del responsable de tratamiento.</li> <li>Art. 20.3 y 4 Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (ET): El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.</li> <li>Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo (LA LEY. 218/2016), al argumentar que esta facultad de control viene legitimada por el art. 20.3 del ET, que expresamente faculta al empresario a adoptar medidas de vigilancia y control para verificar el cumplimiento por los trabajadores de sus obligaciones laborales. Esta facultad general de control prevista en la ley, legitima el control empresarial del cumplimiento por parte de los trabajadores de sus tareas profesionales y el consentimiento de los trabajadores a tales efectos viene implícito en la celebración del contrato de trabajo. La legitimación de esta finalidad se cumple con la existencia de varios distintivos desplegados por la organización en las instalaciones que anuncian la presencia de instalación de cámaras y captación de imágenes y con una información explícita, a poder ser por escrito, consistente en que se les va a grabar, con el único objetivo de controlar el cumplimiento de las obligaciones laborales y que se les podrá sancionar con arreglo a las imágenes grabadas en caso de incumplimiento constatado. En el mismo sentido, STS 77/2017 de 31 de enero 2017.</li> </ul> |  |
|  | Otros:  |  |
| <b>E10. Origen y Procedencia de los Datos: Especificar fuente u origen de los datos de carácter personal que conforman el tratamiento</b>  |   |  |
| Si   | El propio interesado o su representante legal   |  |
| <b>F9. Colectivo/s de Interesados : Identificación del colectivo/s del que se tratan datos</b>   |   |  |
| Personas que acceden a las instalaciones bajo responsabilidad de la Autoridad Portuaria de Avilés  |   |  |
| <b>G10. Estructura de Datos Personales: Especificar Tipología de Datos objeto de tratamiento</b>   |   |  |
| Si   | Categoría de Datos objeto de tratamiento  | Especificación   |
| No   | Categorías especiales de datos personales: <i>datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física</i>   |  |
| Si   | Datos identificativos: <i>Nombre y apellidos, NIF/DNI, Nº Seguridad Social / Mutualidad, Imagen/Voz, Firma, Datos huella parcial, Dirección, Teléfono particular, Dirección correo particular, Otros datos de carácter identificativo</i>   | Imagen   |
| <b>H10. Sistema de Tratamiento: Especificar método de tratamiento de la información</b>  |   |  |
| Si   | Mixto: Soporte papel, soporte informático/magnético.  |  |
| <b>I10. Cesión o comunicación de datos: Especificar entidades destinatarias a quienes se ha comunicado o van a comunicarse los datos de carácter personal</b>  |   |  |
| Si   | Organizaciones o personas directamente contratadas por el Responsable de Tratamiento para la prestación de servicios vinculados con las finalidades de tratamiento: mantenimiento sistema videovigilancia y empresas de seguridad   |  |
| Si   | Entidades Aseguradoras. En caso de siniestro, incidente o accidente se facilita a entidades aseguradoras para la investigación del suceso a fin de determinar alcance y cobertura de la prima de seguro contratada por el responsable de tratamiento.   |  |
| Si   | Fuerzas y Cuerpos de Seguridad: En la medida en que fuera requerido un derecho de acceso justificado en la investigación de un incumplimiento normativo. En caso de requerimiento judicial.   |  |
| Si   | Otros: El dueño del establecimiento, por interés legítimo en la protección de los activos bajo su propiedad   |  |
|  | Otros:  |  |
| Si   | <ul style="list-style-type: none"> <li>Canal de Denuncias Compliance (Las denuncias sobre vulneración de normativa y código de conducta son transmitidas a la Unidad de Cumplimiento Normativo): El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.</li> <li>Conforme a lo establecido en la LOPDGD, los órganos y organismos del Sector Público pueden comunicar los datos personales de los administrados a sujetos de derecho privado que lo soliciten: a) bien cuando cuenten con el consentimiento de los administrados. b) o bien, cuando aprecien que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos.</li> </ul>  |  |
| <b>J10. Transferencias internacionales de Datos (TID) (Arts.66 y 70 RLOPD): Países no UE a los que se realice o esté previsto realizar una comunicación de datos</b>   |   |  |

|   |  |   |
|---|--|---|
| Si  | Observaciones: No se realizan transferencias internacionales de datos  |   |
| <b>K10. Plazos previstos para supresión de datos: Especificar plazo de expurgo y/o cancelación/bloqueo del dato tras finalizar la finalidad que legitimó el tratamiento</b>   |  |   |
| Si  | Datos a Conservar en Tratamientos Específicos y Referencia Legal de base   | Plazo de Conservación Exigible  |
| Si  | Criterio: Los datos personales serán conservados en nuestros sistemas mientras se mantenga vigente la relación de licitud de tratamiento, en base a los plazos de conservación establecidos por la normativa vigente, así como los plazos legal o contractualmente previstos para el ejercicio o prescripción de cualquier acción de responsabilidad por incumplimiento normativo por parte del interesado o de la Organización.   |   |
| Si  | Videovigilancia: Las imágenes/sonidos captados por los sistemas de video vigilancia serán cancelados en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras).  | Las imágenes/sonidos captados por los sistemas de videovigilancia serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones (en cuyo caso, las imágenes serán puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación), o estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto (Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y Art.22 LOPDGDD) : 30 días. |
| Si  | Control Acceso a Edificios: Los datos incluidos en los ficheros automatizados creados para controlar el acceso a edificios (Instrucción 1/1996, de 1 de Marzo, de la AEPD, sobre Ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios).   | 1 Mes   |
| Si  | Canal de Denuncias: Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGDD.  | Los datos de quien formule la comunicación de una denuncia y de los empleados y terceros se conservan en el sistema de denuncias para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados así como posteriormente como evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica, conforme a lo establecido en el artículo 24 de la LOPDGDD.   |
| Si  | Observaciones: CRITERIOS DE SUPRESIÓN Y BLOQUEO DE LOS DATOS: conforme a lo establecido en el Artículo 32 de la LOPDGDD, la Autoridad Portuaria de Avilés estará obligado a bloquear los datos cuando el afectado proceda a su supresión (ya que en videovigilancia no procede la rectificación). El bloqueo de los datos consiste en la identificación y reserva de los mismos, 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 competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo. |   |
| <b>L10. Medidas de Seguridad: Identificación de Medidas técnicas y organizativas aplicables al tratamiento</b>  |  |   |
| <u>Ver "Medidas de Seguridad" del Fichero</u>   |  |   |
| <p>AUTORIDAD PORTUARIA DE AVILÉS toma todas las medidas necesarias para guardar Los datos personales personales de forma privada y segura.</p> <p>UBICACIÓN DE LAS CÁMARAS: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores.</p> <p>UBICACIÓN DE MONITORES: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros no autorizados.</p> <p>CONSERVACIÓN DE IMÁGENES: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.</p> <p>DEBER DE INFORMACIÓN: Se informa acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso.</p> <p>CONTROL LABORAL: En la medida en que las cámaras pueden ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informa a los trabajadores y a sus representantes acerca de las presentes medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras, conforme a lo indicado en la cláusula de notificación de inclusión y en la presente política de privacidad.</p> <p>DERECHO DE ACCESO A LAS IMÁGENES: Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso. No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado</p> |  |   |