Aguas Municipales de Vitoria-Gasteiz, S.A.
AMVISA
Vitoria-Gasteizko Udal Urak, A.B.

BARNEKO INFORMAZIO SISTEMA (BIS) – *SISTEMA INTERNO DE INFORMACIÓN (SII)*

Tratamenduaren arduraduna *Responsable del tratamiento*	**AMVISA SAU (IFK: A-01007376) Vitoria-Gasteizko Udalaren Udal Enpresa Publikoa ARABAn.** *AMVISA S.A.U (CIF A 01007376) Empresa Pública Municipal del Ayuntamiento de Vitoria-Gasteiz en ÁRABA.*
Tratamenduaren arduradunaren kontaktu datuak *Contacto del Responsable del tratamiento*	Calle Puerto Rico kalea, 10 Behea - Bajo 01012 Vitoria-Gasteiz, Álava 945 16 10 00 dpdamvisa@vitoria-gasteiz.org
Tratamenduaren xedeak *Finalidad del Tratamiento*	• **Tratamenduaren helburua da segurtasun sistemaren edo iruzurraren aurkako sistemaren funtzionamenduari buruzko balizko arriskuei eta ez-betetzeei buruz jasotzen den informazioa kudeatzea.** • **Enpresan ezarritako barne arauen multzoa aplikatzea, bertan antolaketa eta kudeaketa eredu eraginkor eta egoki bat ezartzeko, delituak egiteko arriskua arintzeko eta enpresa eta, hala badagokio, administrazio organoa, zuzendariek eta langileek egindako delituen erantzukizun penaletik eta zibiletik salbuesteko.** • **Interesadunen baimenarekin.** • *Tratamiento con el fin de gestionar la información que se reciba en relación con posibles riesgos e incumplimientos sobre el funcionamiento del sistema de seguridad o antifraude.* • *Aplicar el conjunto de normas de carácter interno establecidas en la empresa con la finalidad de implementar en ella un modelo de organización y gestión eficaz e idóneo que permita mitigar el riesgo de la comisión de delitos y exonerar a la empresa y, en su caso, al órgano de administración, de la responsabilidad penal y civil de los delitos cometidos por sus directivos y empleados.* • *Con el consentimiento de las personas interesadas.*
Datu pertsonalen kategoria *Categoría de datos personales*	• **Identifikazio datuak: salatzailearen eta salaketaren xede den pertsonaren edo erakundearen izen-abizenak, NANa, posta elektronikoa.** • **Lekukoen datuak adieraztea, informazioarekin eta dokumentazioarekin.** • **Gauzatutako arriskuei buruzko egitateak eta gertakariak, gauzatzetik gertu daudenak, edo AMVISArentzat erantzukizun zibil eta/edo penalak ekar litzaketen egitateak eta gertakariak.** • **Epaitegiak eta auzitegiak.** • **Ministerio Fiskala.** • *Identificativos: Nombre y apellidos, DNI, correo electrónico del denunciante y de la persona o entidad contra la que se dirige la denuncia.* • *Indicación de datos de testigos con información y documentación.* • *Hechos o sucesos relativos a riesgos materializados, cerca de materializarse, o bien sobre los que existan sospechas de haberse materializado de los que se puedan derivar responsabilidades civiles y/o penales para AMVISA.* • *Juzgados y Tribunales.* • *Ministerio Fiscal.*
Tratamenduaren legitimazioa edo oinarri juridikoa *Legitimación o base jurídica del tratamiento*	• **Zigor Kodearen 31 bis artikuluan jasotako betekizunetako bat betetzea; hain zuzen ere, 5. ataleko 4. betekizunak honako hau ezartzen du: "gerta daitezkeen arriskuen eta ez-betetzeen berri eman beharko zaio prebentzio ereduak ondo funtzionatzen duela eta bete egiten dela zaintzeko ardura duen erakundeari". Salaketa kanal bat sortzea, AMVISAn gerta litezkeen irregulartasunak eta legez kontrako egintzak jakinarazteko betebeharra ezartzeko.** • **Abenduaren 5eko 3/2018 Lege Organikoaren 24. artikulua, Datu Pertsonalak Babesteari eta eskubide digitalak bermatzeari buruzkoa (jatorrizkoa):** **"Zilegi izango da datu pertsonalak tratatzea arau hausteei buruzko informazioa ematen duten pertsonen babesa bermatzeko.** **Tratamendu horiek Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/679 Erregelamenduan (EB), lege organiko honetan eta Arau hausteei eta ustelkeriaren aurkako borrokari buruzko informazioa ematen duten pertsonen babesa arautzen duen Legean xedatutakoaren arabera arautuko dira."** • **2019/1937 (EB) Zuzentarauak ("whistleblowing" Zuzentaraua) salaketa kanal eraginkor, seguru eta konfidentzialak ezarri beharra ezartzen die estatu kideei eta sektore publiko eta pribatuari, bai eta kanal horiek erabiltzen dituzten salatzaileak babesteko neurriak hartzea ere, balizko errepresalien edo ondorio negatiboen aurrean.** • **Helburu nagusia gardentasuna bermatzea eta ustelkeriari aurre egitea da, bai esparru publikoan, bai pribatuan.**

	• **2/2023 Legea, otsailaren 20koa, arau hausteei eta ustelkeriaren aurkako borrokari buruzko informazioa ematen duten pertsonak babesteari buruzkoa.**
	• *Cumplimiento de uno de los requisitos previstos en el artículo 31 bis del Código Penal el 4º requisito apartado 5 que establece "impondrán la obligación de informar de los posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención".* • *Creación de un canal de denuncias para imponer la obligación de comunicar posibles irregularidades o actos ilícitos que se produzcan en AMVISA.* • *Art. 24 LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (original):* *"Serán lícitos los tratamientos de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas.* *Dichos tratamientos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en esta ley orgánica y en la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción."* • *La Directiva (UE) 2019/1937 (Directiva "whistleblowing") impone a los Estados Miembros (EM) y al Sector Público y Privado el establecimiento de canales de denuncia efectivos, seguros y confidenciales, así como la adopción de medidas que protejan a las personas denunciantes que utilicen estos canales frente a posibles represalias o consecuencias negativas.* *Su objetivo principal es garantizar la transparencia y combatir la corrupción tanto en el ámbito público como en el privado.* • *Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.*
Hartzaileak *Destinatarios*	• **Enplegatu publikoak edo besteren konturako langileak;** • **autonomoak;** • **akziodunak, partaideak eta enpresa baten administrazio, zuzendaritza edo ikuskapen organoko kideak, kide ez-exekutiboak barne;** • **kontratisten, azpikontratisten eta hornitzaileen ikuskaritzapean edo zuzendaritzapean lan egiten duen edozein pertsona;** • **amaitutako lan harreman edo estatutu harreman baten esparruan arau hausteei buruz eskuratutako informazioa jendaurrean jakinarazten edo agerian jartzen duten informatzaileak, boluntarioak, bekadunak, prestakuntza aldian dauden langileak eta lan harremana oraindik hasi gabe dutenak (arau hausteei buruzko informazioa hautaketa edo kontratu aurreko negoziazio prozesuan zehar lortu bada).**
	• *Empleados/as públicos o los/las trabajadores por cuenta ajena;* • *autónomos/as;* • *accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos;* • *cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores* • *informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación, y aquellos cuya relación laboral todavía no haya comenzado (casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual).*
Gordetzeko epea *Plazo de conservación*	**Informazioaren/komunikazioaren kudeaketaren iraupena: gehienez 3 hilabete (+ 3 hilabete, kasu konplexua bada – DBLren 9. artikulua)**
	Duración de la gestión de la información/comunicación: máximo 3 meses (+ 3 meses si complejo - art 9 LPD-)
Pertsonen eskubideak *Derechos de las personas*	**Datuak babesteko delegatuearen bitartez, pertsona interesatuak datuak ikusi ditzake, aldatzeko eskatu, edo, hala behar bada, datuak ezeztatzeko eskatu, horien kontra agertu edo tratamendua mugatzeko eskatu.**
	Las personas tienen derecho a retirar el consentimiento y pueden acceder a sus datos, solicitar su rectificación o, en su caso, supresión, oposición o limitación de tratamiento, a través de la persona designada como Delegada de Protección de Datos.