DONOSTIAKO UDALAREN BARNE-INFORMAZIO SISTEMAREN FUNTZIONAMENDU ETA PROZEDURA
PROCEDIMIENTO Y FUNCIONAMIENTO DEL SISTEMA INTERNO DE INFORMACIÓN DEL AYUNTAMIENTO DE SAN SEBASTIÁN

Arau-urratzeei eta ustelkeriaren aurkako borrokari buruzko informazioa ematen duten pertsonen babesa arautzen duen otsailaren 20ko 2/2023 Legean ezarritako betebeharrak betez, Donostiako Udalaren barneko informazio-sistema sortu da. Sistema horrek aukera ematen du kontsultak eta salaketak aurkezteko edo Donostiako Udalean edo haren udal-erakundeetan gertatutako arau-hausteen, jokabide bidegabeen edo jardunbide txarren susmo arrazoituak jakinarazteko, eta erabateko konfidentzialtasuna, anonimotasuna eta babesa bermatzen ditu edozein errepresaliaren aurrean.

Cumpliendo con las obligaciones establecidas en la 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, se crea el Sistema interno de información del Ayuntamiento de San Sebastían que ofrece la posibilidad de presentar consultas y denuncias o notificar sospechas fundadas de infracciones, conductas indebidas o malas prácticas ocurridas dentro del Ayuntamiento de San Sebastián o sus entidades municipales, garantizando la absoluta confidencialidad, anonimato y protección ante cualquier posible represalia.

Alerta goiztiarreko sistema bat da, arriskuak murrizteko, etika publikoa sustatzeko eta herritarrek erakundean duten konfiantza areagotzeko.

El objetivo de esta actuación es constituir un sistema de alerta temprana para reducir riesgos, fomentar la ética pública y para aumentar la confianza de la ciudadanía en la institución.

Arlo hauetako arau-hausteak salatu ahal izango dira BARNE-INFORMAZIO SISTEMAREN BIDEZ bidez
Se podrán denunciar mediante el SISTEMA DE INFORMACIÓN INTERNA las infracciones que se identifiquen en los siguientes ámbitos

1	Kontratazio publikoa.	1	Contratación pública.
2	Finantza merkatuak, zerbitzuak eta produktuak, eta, prebentzio moduan, kapitalak zuritzea eta terrorismoa finantzatzea.	2	Servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo.
3	Produktuen segurtasuna eta haiekiko adostasuna.	3	Seguridad de los productos y conformidad.
4	Garraioaren segurtasuna.	4	Seguridad del transporte.
5	Ingurumena babestea.	5	Protección del medio ambiente.
6	Erradiazioetatik babestea eta segurtasun nuklearra.	6	Protección frente a las radiaciones y seguridad nuclear.
7	Elikagaien eta pentsuen segurtasuna, animalien osasuna eta ongizatea.	7	Seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales
8	Osasun publikoa.	8	Salud pública
9	Kontsumitzaileak babestea.	9	Protección de los consumidores
10	Pribatutasuna eta datu pertsonalak babestea, eta informazio sare eta sistemen segurtasuna.	10	Protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información
11	Iruzurra.	11	Fraude
12	Zerga-ordainketari ihes egitea edo zergak ordaintzea saihestea.	12	Evasión o elusión de impuestos

13 Lan-zuzenbidearen arau-hausteak laneko segurtasunaren eta osasunaren arloan

14 Arau-hauste penal edo administratibo larriak edo oso larriak izan daitezkeen egiteak edo ez-egiteak

13 Infracciones del Derecho laboral en materia de seguridad y salud en el trabajo

14 Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave

Honako hauek aurkeztu ahal izango dituzte salaketak Donostiako Udalaren BARNE-INFORMAZIO SISTEMAREN BIDEZ

Las personas que podrán presentar las denuncias mediante el SISTEMA DE INFORMACIÓN INTERNA del Ayuntamiento de San Sebastián son las siguientes:

- Lan-harremana duten udal-langileak, karrerako funtzionarioak izan, bitartekoak izan, lan-kontratukoak izan edo praktiketan egon.
- Udalarekin merkataritza-harremana duten kontratisten, azpikontratisten nahiz hornitzaileen gainbegiratze eta zuzendaritza pean lan egiten duen edonor.
- Amaitutako lan-harreman baten esparruan lortutako arau-hausteei buruzko informazioa publikoki jakinarazten edo ezagutarazten duten udal-langile izandakoak. Boluntarioak, bekadunak, prestakuntza-aldietako langileak, ordainsari bat jasotzen duten ala ez kontuan hartu gabe. Baita lan-harremana oraindik hasi gabe duten langileei ere, arau-hausteei buruzko informazioa hautaketa- edo kontratu-aurreko negoziazio-prozesuan lortu den kasuetan.
- Akziodunak, partaideak eta enpresa baten administrazio-, zuzendaritza- edo gainbegiratze-organoko pertsonak, baita kide ez-exekutiboak ere.

- Las personas que tengan condición de empleados/as públicos/as y trabajadores/as.
- Cualquier persona que trabaje bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores que tengan una relación mercantil con el ayuntamiento.
- Personas que hubieran tenido condición de empleados/as públicos/as y trabajadores/as y que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral ya finalizada. Voluntarios/as, becarios/as, trabajadores/as en periodos de formación con independencia de que perciban o no una remuneración. Así como a aquéllas personas cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.
- Los/as accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos.

Informazioaren edukia

Contenido de la información

1. Gertakarien deskribapena, ahal den konkretu eta zehatzena, eta, ahal dela, honako hauek ere identifikatzea: gertakarietan parte hartu duten pertsonak, eta ustezko arau-hausteak erasandako negozioak, deialdiak, tresnak nahiz espedienteak.
2. Jakinarazitako gertakariak egiaztatzeko eta gertakari horiei dagozkien jarduketak egiteko bide ematen duen dokumentazioa eta edozein froga-elementu.

1. Una descripción de los hechos de la forma más concreta y detallada posible, identificando, siempre que fuera posible, las personas que hubieran participado en los mismos; los negocios, convocatorias, instrumentos o expedientes afectados por la presunta infracción.
2. La documentación o cualquier elemento de prueba que facilite la verificación de los hechos comunicados y la realización de las actuaciones que correspondan en relación con los mismos.

3. Gertakarien berri edo salaketa bat aurkezteko ez dago informazio pertsonalik eman beharrik.

3. No es necesario aportar ninguna información de carácter personal por parte de la persona informante para poder realizar la consulta o presentar una denuncia.

Sistemaren ezaugarriak
Características del Sistema

1. Integritate-planaren eta iruzurraren aurkako neurrien arduradun teknikoari dagokio sistema kudeatzea

2. Jasotako mezuak konfidentzialtasun osoz tratatuko dira. WhistleB kanpo-zerbitzuen hornitzaileak kudeatzen du mezu anonimoak ahalbidetzen dituen informazio-sistema hori. Mezu guztiak enkriptatuta daude. Mezua bidaltzen duen pertsonaren anonimotasuna babesteko, WhistleB-k metadatu guztiak ezabatzen ditu, IP helbideak barne. Izendatutako arduradun teknikoarekin izandako elkarrizketan ere salatzailea nor den adieraziko da.

3. Jakinarazte prozesua zifratuta eta pasahitz batez babestuta dago. Mezua bidaltzen denean, identifikatzaile bat eta pasahitz pertsonal bat jasoko ditu salatzaileak. Kredentzial horiek momentuan gorde beharko dira, ezin baitira berreskuratu. Pasahitz horri esker era anonimoan elkarrizketa edo informazio osagarria eskatzeko balioko du, eta horretan guztian ez da anonimotasunik galduko.

1. La gestión del Sistema corresponderá a la persona Responsable Técnica del Plan de Integridad y de Medidas Antifraude.

2. Los mensajes recibidos se tratarán con total confidencialidad. Este sistema de información que permite mensajes anónimos está gestionado por WhistleB, un proveedor de servicios externo. Todos los mensajes están encriptados. Para salvaguardar el anonimato de la persona que envía el mensaje, WhistleB se encarga de borrar todos los metadatos, incluidas las direcciones IP. La identidad del denunciante también permanecerá a salvo durante el correspondiente diálogo que mantenga con el responsable Técnico asignado.

3. El proceso de notificación está cifrado y protegido por contraseña. Cuando se envíe el mensaje, la persona denunciante recibirá un identificador y una contraseña personal. Estas credenciales deberán guardarse en el momento ya que no pueden ser recuperadas por motivos de seguridad. Esta contraseña servirá para establecer un diálogo o solicitar información complementaria de forma anónima, sin pérdida de anonimato en todo ello.

Sistemaren prozedura
Procedimiento del Sistema

1. Salaketak jasotzea

Salaketa jaso eta gero, Sistemaren arduradunak salaketa jaso izanaren agiria bidaliko dio salatzaileari, salaketa jaso eta zazpi egun iragan baino lehen.

1. Recepción de las denuncias

Una vez recibida la denuncia la persona responsable del Sistema enviará un acuse de recibo de la denuncia a la persona denunciante en un plazo de siete días a partir de la recepción.

2. Salaketa izapidetzea eta aztertzea

Sistemaren arduradunak jasotako salaketak aztertuko ditu, eta, horretarako, informazioa eskatu ahal izango die bai aurkeztutako salaketaren xede diren administrazio-organoei edo erakunde instrumentalei, bai salaketaren eragina jasan dezaketen zeharkako

2. Tramitación y análisis de la denuncia

La persona responsable del Sistema procederá a estudiar las denuncias recibidas, pudiendo a tal efecto solicitar información tanto a los órganos administrativos o entes instrumentales a los que se refiera la denuncia presentada

organoei.

Sistemaren arduradunak Zuzentasun Batzordeari salaketen azterketaren inguruko emaitzak eta salaketa bera bidaliko dizkio , jakinaren gainean egon dadin, izapideak egin ditzan eta dagokion prozedura proposa dezan. Horren barruan sartzen dira diziplina-prozedurak, itzultze-prozedurak nahiz prozeduraren bat etetea, horren gainean salaketa oinarriduna egin bada, irregulartasuna dela-eta.

- ✔ Ikerketa-prozesuan parte hartzen duen inor ez da saiatuko salatzailea inola ere identifikatzen.
- ✔ Sistemaren arduradunak, beharrezkotzat jotzen duenean edo Batzordeak eskatuta, jarraipen-galdera berriak planteatu ahal izango ditu sistemaren bidez, komunikazio anonimoa bermatzeko.
- ✔ Kasuaren ikerketan ez du parte hartuko ustezko irregulartasunarekin zerikusia duen inork.
- ✔ Salaketa-mezuak konfidentzialtasunez tratatzen dituzte beti inplikatutako alderdi guztiek.
- ✔ Kanpoko edo erakundeko adituek ikerketan parte har dezakete, salatzailearen baimenarekin.

3. Erantzuteko epea

Zentzuzko epe bat ezartzen da erantzuna emateko. Epe hori ez da hiru hilabetetik gorakoa izango, salaketa jaso izanaren agiria bidali zenetik, edo, salatzaileari jaso izanaren agiririk bidali ez bazaio, salaketa egin eta zazpi eguneko epea amaitzen denetik.

4. Salaketak ez izapidetzeko arrazoiak.

Arduradun teknikoak salaketa ez du bideratuko kasu hauetan:

- ✔ Ustezko jokabidea ez da sartzen sistema honen aplikazio-eremuan.
- ✔ Mezua ez da fede onez egiten edo asmo txarrekoa da, ezta informazio faltsua edo legez kontra lortutakoa ematen dutenak ere.
- ✔ Ez dago nahikoa informazio ikerketan sakontzeko, eskatu da dokumentazioa edo froga aurkezteko, eta ez da aurkeztu.

cómo a los órganos transversales que puedan verse afectados por la misma.

La persona responsable del Sistema remitirá las conclusiones de su estudio junto con la denuncia a la Comisión de Integridad, para su conocimiento, tramitación y propuesta del procedimiento que proceda, lo que incluye los procedimientos disciplinarios, de reintegro o la suspensión de algún procedimiento sobre el que recayera alguna denuncia fundada de irregularidad.

- ✔ Nadie que forme parte del proceso de investigación, intentará identificar al denunciante bajo ningún concepto.
- ✔ El/la responsable del Sistema, cuando lo crea necesario o por solicitud de la Comisión, podrá plantear nuevas preguntas de seguimiento a través del Sistema, garantizando así una comunicación anónima.
- ✔ En la investigación del caso no participará nadie que pueda estar implicado o relacionado con la presunta irregularidad.
- ✔ Los mensajes de denuncia siempre son tratados de manera confidencial por todas las partes implicadas.
- ✔ Expertos externos o de la organización podrían participar en la investigación, con el consentimiento del denunciante.

3. Plazo de respuesta

Se establece un plazo razonable para dar respuesta, que no será superior a tres meses a partir del acuse de recibo o, si no se remitió un acuse de recibo al denunciante, a tres meses a partir del vencimiento del plazo de siete días después de hacerse la denuncia.

4. Causas de denegación a trámite de la denuncia.

El responsable técnico no dará curso a la denuncia recibida cuando :

- ✓ La supuesta conducta no entra dentro del ámbito de aplicación de este Sistema.
- ✓ El mensaje no se hace de buena fe o resulta malintencionado, proporcionando información falsa u obtenida de manera ilícita.
- ✓ No haya suficiente información como para profundizar en la investigación, se hubiera requerido aportación de documentación o prueba y no se haya presentado.

Kasu horietan guztietan, aurkeztutako salaketa artxibatuko da, artxibatzeko arrazoiak adierazita.

En todos estos casos se procederá al archivo de la denuncia presentada, haciendo constar los motivos del archivo.

5. Salaketen erregistroa eta ezabaketa

Arduradun teknikoak jasotako informazio guztien eta egindako barne-ikerketen erregistroa egingo du, betiere legean aurreikusitako konfidentzialtasun-baldintzak bermatuz.

Salaketa-mezuetan eta ikerketaren dokumentazio osoan jasotako datu pertsonalak ezabatu egingo dira ikerketa amaitzen denean, salbu eta datu pertsonalak gorde behar badira aplikatu beharreko beste lege batzuek hala adierazten dutelako. Ikerketa amaitu eta 30 egunera, datuak behin betiko ezabatuko dira. Ikerketaren dokumentazioak eta salatzaileak artxibatzen dituen mezuek konfidentzialak eta anonimoak izan beharko dute, DBEOk ezartzen duenaren arabera. Ez dute informazio pertsonalik jaso behar, kasuan inplikatutako gizabanakoak zuzenean edo zeharka identifikatzeko balio duenik.

5. Registro y borrado de las denuncias

La persona Responsable técnica llevará un registro de todas las las informaciones recibidas y de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad previstos en la ley .

Los datos personales incluidos en los mensajes de denuncia y en toda la documentación de la investigación se eliminarán cuando la investigación concluya, salvo en el caso de que los datos personales deban conservarse porque otras leyes aplicables así lo indiquen. Se procederá a la eliminación permanente de los datos 30 días después de que la investigación haya concluido. La documentación de la investigación y los mensajes del denunciante que se archiven deberán ser confidenciales y anónimos, según establece el RGPD. No deberan incluir ninguna información personal que sirva para identificar directa o indirectamente a los individuos involucrados en el caso.

6. Datu pertsonalen tratamenduaren arduraduna.

Alde batetik, Donostiako Udala, eta zehazki,Lehendakaritza Zuzendaritza, arduratuko da salaketa-zerbitzuan prozesatutako datu pertsonalez.

Bestalde, WhistleB Whistleblowing Centre Ab (World Trade Centre, Klarabergsviadukten 70, SE-107 24 Estocolmo, Suedia) arduratzen da salaketak aplikatzeaz, baita enkriptatutako datuak prozesatzeaz ere, hala nola salaketa-mezuak. WhistleB eta haren azpihornitzaileek ezin dituzte mezuak desenkriptatu edo irakurri. WhistleB eta haren azpihornitzaileak ezin dira irakurri.

6. Responsable de Tratamiento de los datos personales.

Por un lado, el Ayuntamiento de San Sebastían y en concreto, la Dirección de Presidencia, será el responsable de los datos personales procesados dentro del servicio de denuncias.

Por otro lado, WhistleB Whistleblowing Centre Ab (World Trade Centre, Klarabergsviadukten 70, SE-107 24 Estocolmo, Suecia) es responsable de la aplicación de denuncias, incluido el procesamiento de los datos encriptados, como los mensajes de denuncias. Tanto WhistleB como sus subproveedores no pueden desencriptar ni leer los mensajes. Como tal, tanto WhistleB como sus subproveedores no tienen acceso al contenido legible.