PLIEGO DE PRESCRIPCIONES TÉCNICAS

PROCEDIMIENTO ABIERTO PARA LA ADJUDICACIÓN DEL CONTRATO DE SUMINISTRO, CONFIGURACIÓN Y OPERACIÓN DE UN SISTEMA INTEGRAL PARA LA IDENTIFICACIÓN, DETECCIÓN, PROTECCIÓN Y RESPUESTA FRENTE A POSIBLES BRECHAS EN EL USO DE APLICACIONES Y SERVICIOS EN LA NUBE PARA LAS EMPRESAS DEL GRUPO VEOLIA

(Referencia: 2026_C12_0003)

8 de julio de 2026

1. OBJETO DEL ACUERDO MARCO

La presente licitación tiene por objeto el suministro, operación, mantenimiento y respuesta a incidentes nivel 1 y nivel 2 del sistema integral para la identificación, detección, protección y respuesta frente a posibles brechas en el uso de aplicaciones y servicios en la nube, con la tecnología Netskope (en adelante la Solución).

En la actualidad, la gran mayoría del tráfico que circula a través de nuestros sistemas es tráfico cifrado lo que permite a los ciberdelincuentes ocultar malware o exfiltrar datos sin ser detectados por firewalls tradicionales que no tienen capacidad de descifrado a escala. Además, el usuario final interactúa cada vez más con la inteligencia artificial, sin control de lo que subimos. Es por ello que las organizaciones necesitamos soluciones de primer nivel que nos ayuden a descifrar este tráfico, poder detectar fugas de información a fuentes de terceros como las inteligencias artificiales y securizar la navegación que sale de los equipos de usuario, como descarga de malware.

Hasta ahora disfrutábamos de los módulos de Gateway seguro (SWG), CASB y DLP pero, debido al crecimiento de la tecnología conjuntamente con nuestras necesidades, resulta crucial poder incorporar nuevos módulos de DLP (Data Loss Prevention) a la solución ya en uso, de manera que quede garantizada la protección integral frente a posibles brechas en el uso de aplicaciones y servicios en la nube por parte de la empresa.

Veolia no es ajena a estas tendencias y en su afán por contar con las soluciones más eficientes y seguras, decide publicar la presente RFP para solicitar propuestas con el detalle descrito en este pliego y poder hacer frente las nuevas amenazas.

2. CONDICIONES GENERALES DE SUMINISTRO

La solución a suministrar, así como servicios asociados, se ha separado en dos lotes:

- **LOTE 1 -** Licencias de la herramienta de protección del servicio de navegación y prevención de fugas de información
- **LOTE 2** - Servicio de operación, mantenimiento y respuesta a incidentes (nivel 1 y 2)

Para la presente licitación, se contratarán las licencias con necesidad de navegación a Internet, con la posibilidad de que un usuario pueda tener más de 1 dispositivo con la misma identidad contabilizando solo 1 licencia. Las empresas del grupo Veolia se adherirán a la licitación de conformidad a lo establecido en el Pliego de Condiciones Generales.

2.1. ALCANCE Y REQUERIMIENTOS

Los requerimientos necesarios para el alcance anteriormente descritos que debe satisfacer esta licitación están descritos a continuación y serán conformes a la siguiente normativa:

- Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

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

2.2. LUGAR DE EJECUCIÓN. ÁMBITO Y ALCANCE DEL CONTRATO

El lugar de ejecución serán las oficinas de Veolia en Barcelona donde estará el FTE dedicado al servicio.

El alcance y ámbito de aplicación será el equipamiento desde el cuál se securiza la navegación a Internet de la infraestructura y equipos de usuario de las empresas del Grupo Veolia en España y todas sus filiales.

Por requisitos de buenas prácticas de operación del sistema, forma parte igualmente del alcance, la conexión e integración de todos los datos del sistema con el servicio de operación y monitorización para la prestación de servicios de ciberseguridad con/desde el servicio de respuesta a incidentes de nivel 1 y nivel 2 de Veolia en España.

Se incluye dentro del alcance de este procedimiento:

Lote 1 - Licencias de la herramienta de protección del servicio de navegación y prevención de fugas de información:

- Contratación de licencias
- Actualización de licencias.

Lote 2 - Servicio de operación, mantenimiento y respuesta a incidentes (nivel 1 y 2):

- Operación, mantenimiento y respuesta a incidentes nivel 1 y nivel 2
- Puesta en servicio completo incluyendo traspaso de conocimientos, formación y documentación.
- Soporte técnico del producto.

En el apartado *3. Condiciones Técnicas* y *4. Condiciones Operativas* del presente pliego se define y se detalla lo que se incluye en cada lote.

Se deben incluir en la oferta todos los módulos, licencias y equipamientos para cubrir todos los requisitos técnicos y funcionales.

Si durante la vigencia temporal del Contrato regido por el presente Pliego se incorporase a la gestión de Veolia alguna instalación adicional, ésta quedará incluida automáticamente en el ámbito del presente Pliego.

3. CONDICIONES TÉCNICAS LOTE 1

En este lote se incluyen las licencias de la herramienta de servicio de navegación deseadas, que tiene que ofrecer la Solución, y deben de ser:

- Netskope Prime Advantage o Secure Web Gateway. Se requiere securizar la navegación web que realiza el usuario con el equipo corporativo.
- Advanced Threat Protection. Se requiere proteger los servicios que tenemos contratados en nube a un tercero.
- Advanced User and Entity Behaviour Analytics. Se necesita este módulo para detectar anomalías en el comportamiento de los usuarios y para poder elaborar un scoring de riesgo del usuario en función de las acciones que él mismo realiza, detectando malos comportamientos de manera repetitiva.
- Endpoint Data Loss Prevention (en adelante **End. DLP**). Se requiere este módulo para prevenir fugas de información con técnicas más sofisticadas. También se quiere disponer de las capacidades File Fingerprinting o Exact Data Match.
- Advanced Data Loss Prevention (en adelante **Adv. DLP**). Se requiere este módulo para tener capacidades avanzadas del módulo DLP con más identificadores de dato, más normativas regulatorias y capacidades de Inteligencia Artificial y Machine Learning.
- Netskope Premium Support. Este módulo es requerido para tener soporte con fabricante y poder abrir casos de soporte.

3.1.1. ACUERDOS DE NIVEL DE SERVICIO (ANS) Y PENALIZACIONES LOTE 1

Dentro del Lote 1, para evitar problemas con la solución tecnológica y para asegurar la continuidad en el servicio, se han definido unos acuerdos de

nivel de servicio (ANS) y unas penalizaciones, que se definen a continuación:

- Seguimiento a la incorporación de nuevas licencias en la consola.
    - **Descripción.** Siempre que las nuevas licencias sean compradas con el proveedor asignado al contrato de la licitación, el proveedor tendrá que asegurarse que las licencias son añadidas a la consola
    - **Tiempo máximo.** 3 días desde la recepción del pedido por parte del fabricante
    - **Penalización.** Compensación del 3% del precio anual de las licencias
- Dar seguimiento de las incidencias relativas a la consola de administración
    - **Descripción.** En el caso de que haya alguna incidencia, el proveedor tendrá que dar un seguimiento diario (informes, correos…) a todas las incidencias relativas a la consola de administración. En el caso de que no haya ninguna incidencia, no tendrá que hacer nada.
    - **Tiempo máximo.** 2 días sin actualizar el estado de la incidencia por parte de proveedor
    - **Penalización.** 3% del precio anual de las licencias
- Notificación de posibles incidencias relativas a problemas con mantenimientos de la Solución.
    - **Descripción.** El proveedor tendrá que informar al cliente de los mantenimientos que va a realizar el fabricante que pudieran conllevar incidencias a la infraestructura del cliente
    - **Tiempo máximo.** 1 semana antes del mantenimiento programado por parte de fabricante
    - **Penalización.** 2% del precio anual de las licencias
- Monitorización del servicio en el caso de que los POPs balanceen y no estemos en el POP más cercano en función de nuestra región geográfica.
    - **Descripción.** El proveedor tendrá que informar al cliente cuando el fabricante, por el motivo que sea, balancee el POP asignado por cercanía geográfica y dar seguimiento a la misma
    - **Tiempo máximo.** 1 día después del balanceo
    - **Penalización.** 2% del precio anual de las licencias

Los días se contabilizarán en base a la ventana horaria del servicio definida anteriormente.

Todos los plazos están calculados en base a días hábiles.

4. CONDICIONES OPERATIVAS LOTE 2

En este lote, se van a identificar todas las cuestiones que puedan estar relacionadas con el servicio de operación y mantenimiento que necesitamos de la Solución. El proveedor prestará un servicio integral orientado a la identificación temprana de incidentes, la reducción de falsos positivos, la priorización de alertas y el soporte especializado al equipo SOC/CSIRT del Cliente.

Con el servicio deseado, se prevé implantar un modelo dinámico y de protección continua (antes, durante y después de posibles incidentes) que tenga como objetivos los siguientes:

- Evolucionar hacia un modelo acorde a los desafíos y objetivos estratégicos actuales y futuros.
- Proporcionar una detección, análisis, gestión y comunicación continua de amenazas relacionadas con la navegación web, la exfiltración de datos y cualquier actividad anómala que comprometa la seguridad de la organización.
- Proporcionar visibilidad y control sobre el estado de seguridad de los sistemas permitiendo proteger los activos que los soportan, asegurando de esa forma una correcta prestación de los servicios de explotación.
- Prevenir la fuga de información de los equipos de trabajo a dominios externos y/o de otras empresas.
- Establecer mecanismos que permitan anticipar los posibles acontecimientos que puedan ocurrir en los sistemas y que ayudan a prevenir posibles ataques.
- Gestionar y administrar todo el ciclo de vida de los incidentes y posibles amenazas.
- Impulsar modelos y técnicas de análisis de ciberamenazas y medidas de protección.

- Elevar los estándares operativos y buenas prácticas en la gestión operativa, a través de las mejoras derivadas de la experiencia y know-how del sector, así como también a través de la labor de ingeniería, benchmarking y transferencia tecnológica del ámbito externo a la misma.
- Contribuir a asegurar un servicio, con altos estándares de seguridad y confiabilidad, a través de:
    - Aseguramiento de la disponibilidad de las infraestructuras operativas
    - Adecuada gestión del mantenimiento en el ámbito de la seguridad
    - Generación de información oportuna y de calidad del entorno tecnológico
- Ser capaz de responder a un marco regulatorio y/o normativo.

Para conseguir estos objetivos, el servicio gestionado ha de encargarse de implementar las acciones que correspondan en cada momento para garantizar el correcto funcionamiento de la solución y, por tanto, el cumplimiento de su función dentro del esquema general de seguridad de Veolia.

4.1. CARACTERÍSTICAS GENERALES DEL SERVICIO LOTE 2

A continuación, se detallan los aspectos generales del servicio que se desea.

Tipo de Servicio	Modalidad
Gestión y mantenimiento de la solución tecnológica	**11x5x365**

El objeto principal de este servicio es proteger en todo momento la infraestructura de las sociedades del Grupo Veolia en España de cualquier amenaza cibernética. Este servicio se medirá según los siguientes aspectos:

Tipo de Servicio	Modalidad
Servicio de detección y protección	**11x5**
Gestión de Incidencias (ticketing)	**11x5**

4.2. GESTIÓN OPERATIVA DE LA SOLUCIÓN LOTE 2

Dentro de la operativa del servicio, se debería de contemplar lo siguiente:

1. Monitorización y Detección de Actividades Inusuales
    a. Supervisión continua de los eventos generados por las plataformas de seguridad (Proxy/SWG, CASB, DLP, navegadores protegidos, firewalls, etc.).
    b. Identificación y reporte de comportamientos anómalos o indicios de amenazas, tales como:
        i. Accesos a sitios maliciosos o de riesgo.
        ii. Transferencias de datos no autorizadas.
        iii. Anomalías en patrones de navegación.
        iv. Intentos de evasión de controles de seguridad.
    c. Aplicación de reglas de detección basadas en inteligencia de amenazas (Threat Intelligence).
2. Clasificación y Priorización de Incidentes
    a. Clasificación inicial de todos los eventos detectados conforme a su criticidad, naturaleza y posibles impactos.
    b. Categorización bajo el marco del Cliente (criticidad, impacto, probabilidad, tipología).
    c. Evaluación de riesgo y priorización para optimizar la respuesta operativa.
3. Depuración de Falsos Positivos
    a. Revisión, correlación y filtrado de eventos para identificar falsos positivos.
    b. Ajuste de reglas y políticas con el fin de mejorar la calidad de las detecciones.
    c. Coordinación con el Cliente para afinar continuamente el modelo de alertado.
4. Análisis Avanzado y Generación de Alertas en colaboración con el departamento de Ciberseguridad de Veolia en España.
    a. Análisis en profundidad por parte de analistas especializados del servicio de respuesta a incidentes de nivel 1 y nivel 2 del proveedor.
    b. Determinación por parte del proveedor de qué eventos constituyen alertas relevantes dentro del contexto del Cliente.
    c. Comunicación proactiva al servicio de respuesta a incidentes de Veolia en España de las alertas confirmadas.

   d. Aportación de recomendaciones inmediatas de contención cuando aplique.
5. Valoración del Impacto y Gestión del Incidente
   a. Determinación de la veracidad, alcance e impacto de la alerta.
   b. Análisis técnico detallado del incidente, incluyendo:
      i. Vector de amenaza.
      ii. Usuarios, dispositivos o datos afectados.
      iii. Evaluación de posible fuga de información.
      iv. Acciones correctivas y preventivas sugeridas.
   c. Elaboración de un informe completo tras la finalización de la investigación.
6. Coordinación entre el servicio del proveedor y el SOC de respuesta a incidentes de nivel 1 y nivel 2 de Veolia en España
   a. Comunicación de alertas investigadas al servicio de respuesta a incidentes de nivel 1 y nivel 2 de Veolia en España.
   b. Colaboración en la determinación de si una alerta se considera incidente de seguridad.
   c. Soporte al servicio de respuesta a incidentes de nivel 1 y nivel 2 de Veolia en España durante la gestión y resolución del incidente.
   d. Participación en reuniones técnicas o de coordinación cuando se requiera.
   e. Enlace con grupos de investigación externos en caso de ataques avanzados (Threat Intelligence, CERT nacionales, etc.).
7. Gestión Operativa del Incidente
   a. Seguimiento del ciclo de vida del incidente hasta su cierre.
   b. Preservación y custodia de evidencias digitales.
   c. Mantenimiento de una base de datos histórica de incidentes y patrones de ataque.
   d. Propuesta continua de mejoras en procesos, detecciones, políticas y configuraciones.
8. Optimización de Políticas y Configuraciones
   a. Proposición de políticas y configuraciones derivadas de los informes presentados.
   b. Diseño de nuevas políticas configuraciones derivadas de las nuevas amenazas
   c. Optimización de las políticas y configuraciones ya existentes.

9. Seguimiento operativo del servicio (Semanal)
    a. Revisión continua de políticas de seguridad relacionadas con navegación web, DLP y protección contra fuga de datos.
    b. Adaptación a mejores prácticas del sector, recomendaciones del proveedor y alineación con las políticas corporativas.
    c. Identificación y propuesta de nuevas reglas, controles o umbrales de detección.
    d. Asesoramiento para mejorar la postura de seguridad del Cliente.
10. Generación de Informes y KPIs con el formato y contenido acordado mutuamente con el cliente
    a. Informe Operativo Semanal: Incluyendo, como mínimo:
        i. Indicadores clave de la plataforma (volumen de eventos, detecciones, tendencias).
        ii. Alertas generadas y su estado.
        iii. Incidentes creados, resoluciones y tiempos de respuesta.
        iv. Tickets generados y resueltos.
        v. Fallos, problemas o ineficiencias detectadas en el servicio.
        vi. Recomendaciones técnicas y operativas.
    b. Informes Mensuales de Estado y Dirección
        i. Estado general de la seguridad derivada de la navegación web y de la protección de datos.
        ii. Seguimiento de ANS y KPIs.
        iii. Acciones correctivas, preventivas y de mejora.
        iv. Tendencias de amenazas y evolución del riesgo.
        v. Valoración ejecutiva del servicio para la Dirección.
    c. Informes trimestrales al equipo técnico
        i. Informe trimestral con un listado de las políticas propuestas en el punto 8 separando las políticas aceptadas y rechazadas por parte del cliente.
    d. Informes de Incidente Grave
        i. Documentación completa del incidente, acciones realizadas y resultados de la mitigación.

Con el objetivo de tener buena visibilidad y seguimiento de todas las peticiones o incidencias que se puedan derivar del servicio, todas las peticiones, incidencias de navegación o lo que se pueda derivar del lote 2

que no tenga nada que ver con los módulos de DLP, se tendrá que gestionar a través del sistema de ticketing interno de Veolia en España, que actualmente es el Remedy. En cambio, toda la operativa derivada de los módulos contratados de DLP, la plataforma escogida para canalizar dicha operativa sería el Service Desk del cliente.

En el caso de que cambiara algunas de las dos herramientas por parte del cliente, el proveedor tendrá que adaptarse al nuevo sistema de ticketing.

4.3. ACCIONES DE MEJORA DENTRO DEL SERVICIO

Las siguientes tareas adicionales se valorarán muy positivamente:

- Integración con el sistema de gestión de eventos de seguridad centralizado de Veolia en España, el servicio de seguridad gestionada, SOAR y herramientas corporativas para automatizar flujos de respuesta.
- Soporte para la correlación entre eventos de navegación, endpoint (EDR) y actividad de usuarios (UEBA).
- Revisión y ajuste de listas blancas y negras.
- Coordinación con equipos de cumplimiento para asegurar alineación con normativas (RGPD, ENS nivel medio, ISO 27001 y 2230).
- Revisión trimestral de estrategia de detección y mejora del servicio.
- Propuesta de casos de uso para satisfacer la mejora contínua de la herramienta y el servicio así como también la detección de los riesgos emergentes (por ejemplo IA).

4.4. ACUERDOS DE NIVEL DE SERVICIO (ANS) PARA PETICIONES E INCIDENCIAS DEL LOTE 2

A continuación, se especifica la modalidad y los mínimos niveles de servicios (ANS) que el Prestador del Servicio deberá garantizar para los servicios de seguridad gestionada.

Se ha definido una clasificación de incidencias que sea evolutivo desde un nivel N1 (bajo) al N4 (crítico):

La clasificación de incidencias se regirá por el Impacto y la Urgencia que puedan tener dichas incidencias. Es decir, los criterios a aplicar para la priorización en la gestión/resolución de las incidencias son el resultado de la combinación entre estos dos factores:

Impacto (afectación que tiene una incidencia sobre los procesos de negocio)

Niveles de impacto	
Crítico	• Parada total de un servicio/aplicación CRÍTICO. • Degradación o alteración (confirmada o posible) de un sistema CRÍTICO con afectación a la operación.
Alto	• Degradación o alteración (confirmada o posible) de un sistema CRÍTICO sin afectación al servicio. • Parada total o degradación de un servicio/aplicación NO crítico con afectación.
Medio	• Degradación o alteración (confirmada o posible) en el funcionamiento de un sistema No crítico con afectación al servicio. • Parada total o degradación de un servicio/aplicación No crítico sin afectación masiva.
Bajo	• El resto de los incidentes y peticiones de servicio.

Urgencia (rapidez con la que se necesita resolver una incidencia):

Niveles de urgencia	
Crítica	• El usuario o departamento no puede realizar ninguna de las funciones principales que tiene asignadas. • El usuario o departamento no puede realizar otras actividades hasta la resolución de la incidencia.
Alta	• El usuario o departamento no puede realizar alguna de las funciones principales que tiene asignadas. • El usuario o departamento puede continuar con otras actividades hasta la resolución de la solicitud.

Media	• El usuario o departamento puede realizar las funciones principales que tiene asignadas pero presenta dificultades (lentitud, errores puntuales,…). • El usuario o departamento puede continuar con otras actividades hasta la resolución de la solicitud.
Baja	• Se ven afectadas funciones secundarias del usuario o departamento que no impiden el desempeño de sus principales funciones.

La siguiente tabla permite determinar el nivel de servicio a aplicar en función de los parámetros antes establecidos:

I U	Crítica	Alta	Media	Baja
Crítico	**Crítica**	**Crítica**	**Alta**	**Media**
Alto	**Crítica**	**Alta**	**Media**	**Baja**
Medio	**Alta**	**Alta**	**Media**	**Baja**
Bajo	**Media**	**Media**	**Media**	**Baja**

Así mismo, para cada uno de los niveles de servicio requeridos se define el siguiente indicador ANS:

Tiempo de Respuesta a incidencias: Tiempo transcurrido entre el registro de entrada o bien de la comunicación de la incidencia (ticketing, llamada, etc.) o bien de la notificación directa de la misma por parte de la herramienta, por el Prestador del Servicio (monitoreo activo) y el inicio de la primera acción registrada. Se considera acción registrada aquella en que el usuario recibe un "input" después del registro de entrada de la incidencia, ya sea en la herramienta de ticketing o mediante algún otro método pactado con Veolia al inicio del servicio.

Indicadores ANS		Prioridad	Valor máximo	Valor Objetivo
Tiempo de Respuesta	**N4**	**Critica**	**≤ 2 horas**	**≤ 45 min**
	N3	**Alta**	**≤ 8 horas**	**≤ 2 horas**
	N2	**Media**	**≤ 12 horas**	**≤ 8h**
	N1	**Baja**	**Next Bussines day**	**Next Bussines day**

Se calculará el tiempo de respuesta para cada incidencia como el tiempo trascurrido desde el registro de la misma hasta el primer “input” que recibe el cliente (una vez el Prestador del Servicio ha hecho un primer análisis de la incidencia); sin considerar la confirmación del propio registro como “input”.

En lo que se refiere al “valor objetivo” establecido para cada uno de los niveles de prioridad indicados en la tabla anterior, el servicio prestado se deberá aproximar al máximo a dichos tiempos de respuesta, los cuales se consideran referente para un servicio de gran calidad. No obstante, en el cálculo de los ANSs y posibles penalizaciones únicamente se tendrá en consideración los “valores máximos” establecidos para los tiempos de respuesta.

En cualquier caso, tras la resolución de la incidencia, se deberá documentar la intervención en la herramienta de ticketing para dar por resuelto el incidente.

Para controlar estos ANSs, se hará en función de la herramienta de ticketing que se utilice. En el apartado 4.1.2 del presente pliego se ha descrito en qué herramienta de ticketing tendrá que ir cada tipo de incidente, por lo que los ANSs se controlaran en cada herramienta:

- Remedy: Se configuraran unos tiempos de respuesta de referencia en la propia herramienta para que se cumplan los ANS anteriormente definidos
- Service Desk: El servicio de seguridad gestionada del cliente será el encargado de definir los SLAs anteriormente descritos en la propia herramienta, por lo que se tendrá control de los tiempos de respuesta

4.1.4. PENALIZACIONES PARA PETICIONES E INCIDENCIAS

Este servicio estará supeditado a los ANSs de servicio (definidos en el apartado 4.1.3 del presente pliego) que definirán la calidad que el Prestador del Servicio preste. Los ANSs se seguirán mensualmente y supondrán una calificación objetiva del desarrollo del servicio.

Cuando el Prestador del Servicio incumpla los ANSs establecidos, se podrán aplicar penalizaciones económicas según los criterios que se indican a continuación:

Indicadores ANS	**Prioridad**	**Valor máximo**	**% de Cumplimiento mensual**	**Penalización** **(% sobre la facturación mensual)**

N4	**Critica**	**≤ 2 horas**	**95 %**	**P4= 10%**
N3	**Alta**	**≤ 8 horas**	**90 %**	**P3= 5%**
N2	**Media**	**≤ 12 horas**	**85 %**	**P2= 2%**
N1	**Baja**	**Next Bussines day**	**80 %**	**P1= 1%**

Notas importantes:

- El % de cumplimiento se obtendrá dividiendo, según su prioridad (N1, N2, N3, N4), las incidencias que han cumplido con los tiempos esperados (Valor máximo) entre el total de incidencias registradas con dicha prioridad en el mes objeto de evaluación.
- Las penalizaciones mensuales (P1, P2, P3, P4) que resulten del cálculo de los diferentes ANS por nivel de prioridad (N1, N2, N3, N4) serán independientes y se acumularán en el mes, pudiendo llegar al extremo de penalizar todas (hasta un 19 % de la factura mensual).

Así, la penalización mensual total (PT) a aplicar será el valor que resulte de aplicar la siguiente fórmula: PT= P1 + P2 + P3 + P4.

En todo caso, cuando se den algunas de las circunstancias siguientes,

- Incumplimientos tres (3) meses seguidos en los indicadores N4 o N3
- Incumplimientos en los indicadores N4 o N3 en seis (6) meses del cómputo anual (12 meses)

Veolia estará facultada para:

(i) resolver el contrato, o bien

(ii) continuar con la imposición de penalizaciones en los términos previstos anteriormente.

5. FASE DE DEVOLUCIÓN DEL SERVICIO LOTE 1 Y LOTE 2

Con el fin de facilitar el posible cambio de Prestador del Servicio objeto de la presente Oferta, una vez finalizado el periodo de contratación y con el fin de minimizar el impacto en la continuidad y calidad de los servicios y facilitar la recepción al nuevo Prestador (o a Veolia) el Prestador del Servicio diseñará un plan de finalización (Devolución) de ejecución del Servicio. Este plan de

finalización (devolución) de ejecución del Servicio deberá ser presentado en la oferta que se presente para esta licitación.

El Plan de Devolución deberá ser actualizado durante la vida del Servicio en caso de cambios en la organización del mismo, en el material de referencia contractual o para reflejar otros cambios que afecten la reversión.

Durante este periodo de Devolución del Servicio el Prestador del Servicio se compromete a colaborar y aportar en su caso los recursos humanos y materiales necesarios para la realización de todas aquellas actividades encaminadas a la planificación y ejecución del cambio.

Con esto se pretende que el Prestador del Servicio transfiera el conocimiento y experiencia existente, de modo que pueda ser utilizado como un recurso disponible para el personal de Veolia o de terceras empresas (previa autorización del cliente).

La fase de devolución del Servicio tiene como objetivos principales los siguientes:

- Asegurar la continuidad y estabilidad del Servicio durante el periodo de devolución.
- Transferir el conocimiento del Servicio al cliente o al nuevo Prestador del Servicio que éste asigne para la prestación posterior del Servicio facilitando al futuro proveedor toda la colaboración necesaria para realizar la transferencia del servicio, el traspaso de conocimiento, y la habilitación de la operación.
- Generar toda la documentación actualizada de procedimientos, manuales, infraestructuras y desarrollos informáticos asociados al objeto del contrato.

En el caso de que Veolia identifique dependencias y condicionantes entre contratos, el proveedor deberá respetarlos con el fin de minimizar el impacto de la transición en los ámbitos y realizar la transición de forma coordinada.

La Devolución del servicio será realizada durante la propia duración del contrato y se prolongará, como máximo, durante **DOS (2) meses.**

6. EQUIPO DE TRABAJO

6.1. EQUIPO DE TRABAJO LOTE 1

Para el lote 1 se requiere únicamente el contacto del comercial del proveedor para cuando se necesite contratar nuevas licencias o renovar licencias ya existentes. No se pide ningún FTE dedicado, simplemente el soporte del equipo comercial del proveedor cuando se necesite.

6.2. EQUIPO DE TRABAJO LOTE 2

Para esta licitación, se requiere como mínimo 1 FTE experto dedicado en la oficina del cliente en Barcelona con una presencia semanal mínima de 3 días laborables para poder abordar todas las tareas del servicio anteriormente definidas siempre cumpliendo con los ANS también definidos anteriormente. Este FTE, es muy importante que cuente con soporte experto a disposición por parte del servicio para cualquier apoyo técnico que pueda necesitar.

Las ofertas incluirán una descripción detallada de los medios técnicos, procedimientos y medios personales destinados a la prestación de este servicio. También la experiencia, calificación de los técnicos y casos de éxito que tenga la empresa que lanza la oferta.

La cualificación de las personas destinadas a formar parte del equipo de trabajo que preste este servicio será acorde con las tareas a realizar.

ANEXOS

ANEXO 1 - LISTADO DE EMPRESAS

NIF	SOCIEDAD
A02399392	Aguas de Albacete, S.A.
B74271339	Aguas de Avilés, S.L.
A93026680	Aguas de Benahavís, S.A.
A30383269	Aguas de Cieza, S.A.
A73086852	Aguas de Jumilla, S.A.
A30575674	Aguas de Lorca, S.A.
A14724355	Aguas de Montilla, S.A.
B13503263	Aguas de Puertollano, S.L.

A35499318	Aguas de Telde, Gestión Integral del Servicio, S.A.
A53296380	Aguas del Arco Mediterráneo, S.A. (AGAMED)
B03002441	Aguas Municipalizadas de Alicante, Empresa Mixta, S.A.
A18502591	Aguas Vega-Sierra Elvira, S.A. (AGUASVIRA)
A29453768	Aguas y Saneamientos de Torremolinos, S.A.
A08008849	Aigua de Rigat, S.A.
B55179618	Aigües Colomenques, S.L. (AICO)
A66098435	Aigües de Barcelona, E.M. de Gestió del Cicle Integral de l'Aigua, S.A.
A96124177	Aigües de Cullera, S.A.
A08068975	Aigües de Matadepera, S.A.
B22444806	Aigües de Sacalm, S.L.
A53555967	Aigües i Sanejament d'Elx, S.A.
A97727853	Aigües Municipals de Paterna, S.A.
A08021701	Aigües Sant Pere de Ribes, S.A.
A66138470	Aquae Security, S.A.U.
A10384386	Aquanex, Servicio Domiciliario del Agua de Extremadura, S.A.
A32390684	Aquaourense, Sociedade Provincial de Augas e MedioAmbiente, S.A.
G64386626	CETaqua, Centro Tecnológico del Agua, Fundación Privada
B43827971	Comaigua, S.L.
A17000084	Companyia d'Aigües de Palamós, S.A.
A08071664	Companyia d'Aigües de Sabadell, S.A.
B61835575	Drenatges Urbans del Besós, S.L.
B25308818	Empresa d'Aigües i Serveis de Cervera i la Segarra, S.L.
A96523329	Empresa Mixta Aigües de l'Horta, S.A.
B35642198	Empresa Mixta de Aguas de Antigua, S.L.
A18027722	Empresa Municipal de Abastecimiento y Saneamiento de Granada, S.A. (EMASAGRA)
A21006408	Empresa Municipal de Aguas de Huelva, S.A. (EMAHSA)
A30054209	Empresa Municipal de Aguas y Saneamiento de Murcia, S.A. (EMUASA)
A43049956	Empresa Municipal Mixta d'Aigües de Tarragona, S.A. (EMATSA)
G93217743	Fundación Centro Andaluz de Investigaciones del Agua, Fundación Privada
G70312020	Fundación Centro Gallego de Investigaciones del Agua, Fundación Privada
B66145772	Gestió Aigua Calella, S.L. (GESTAIGUA)
A41461856	Hidralia, Gestión Integral de Aguas de Andalucía, S.A.
A73468498	Hidrogea, Gestión Integral de Aguas de Murcia, S.A.
A08015570	Mina Pública d'Aigües de Terrassa, S.A.
A73312100	Sermubeniel, S.A.
B61497160	SIMMAR, Serveis Integrals del Maresme, S.L.
B24604373	Sociedad Mixta de Aguas de León, S.L.
A38285961	Teidagua, S.A.
U06335319	UTE Aguas de Alburquerque
U02789162	UTE Aquona Gestión de Aguas de Castilla, S.A.U - CHM Obras e Infraestructuras, S.A.
U65766925	UTE Depuración Valle Vinalopó
U13969639	UTE ETAP Rioseco

U75570259	UTE Idam Andratx
U22696959	UTE Instalaciones Urbide
U16484222	UTE Lanzarote Saneamiento
U75942672	UTE MA5
U65570772	UTE Saleal
U10358802	UTE Servicio de Aguas de Plasencia
B63152664	Veolia Spain S.L.