PLIEGO DE PRESCRIPCIONES TÉCNICAS

QUE HAN DE REGIR LA CONTRATACIÓN POR PARTE DE LA EMPRESA SUEZ SPAIN DEL SUMINISTRO, INSTALACIÓN, PUESTA EN MARCHA 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.

(Referencia: 2020_C12_1500)

ÍNDICE

1. ANTECEDENTES 4

2. OBJETO DEL CONTRATO. 5

3. LUGAR DE EJECUCIÓN. ÁMBITO Y ALCANCE DEL CONTRATO....5

4. REQUERIMIENTOS/CONDICIONES TÉCNICAS DEL CONTRATO. 6

4.1. REQUERIMIENTOS DEL SISTEMA A INSTALAR....6

REQUERIMIENTOS MÍNIMOS EXIGIDOS....7

OTROS REQUERIMIENTOS FUNCIONALES:....7

4.2. REQUERIMIENTOS DE LA PUESTA EN MARCHA Y SERVICIO DE SEGURIDAD GESTIONADA PARA LA OPERACIÓN DEL SISTEMA. 9

4.2.1. ENTREGA DE LOS EQUIPOS....9

4.2.2. IMPLEMENTACIÓN, PRUEBAS Y PUESTA EN MARCHA....9

4.2.3. DOCUMENTACIÓN DE LA IMPLANTACIÓN. 10

4.2.4. SERVICIO DE SEGURIDAD GESTIONADA (SOC 1 y 2) 10

4.2.4.1. ASPECTOS ORGANIZATIVOS....11

4.2.4.2. CARACTERISTICAS GENERALES DEL SERVICIO....11

4.2.4.3. GESTIÓN INFRAESTRUCTURA PLATAFORMA 12

4.2.4.4. GESTIÓN DE LA SOLUCIÓN 12

4.2.4.5. ACUERDO DE NIVEL DE SERVICIO (ANS) 14

4.2.4.5.1. GESTIÓN Y MANTENIMIENTO DE LA SOLUCIÓN TECNOLÓGICA....14

4.2.4.5.2. GESTIÓN DE LA CIBERSEGURIDAD 15

4.2.4.5.3. PETICIONES....17

4.2.4.6. FASE DE DEVOLUCIÓN DEL SERVICIO 18

4.2.4.7. PENALIZACIONES 18

4.3. EQUIPO DE TRABAJO 20

4.3.1. SERVICE MANAGER....20

4.3.2. TÉCNICOS EXPERTOS 20

1. ANTECEDENTES

La principal actividad de SUEZ Spain es la gestión del Ciclo Urbano del Agua, desde su captación, la potabilización, la distribución, el mantenimiento de la red de saneamiento, el control de vertidos y la depuración del agua residual. Finalmente, el agua tratada es devuelta a cauce público, para su uso ambiental y riego.

Además, SUEZ Spain se caracteriza por ser una empresa comprometida, medioambiental y socialmente responsable. Prueba de ello es que SUEZ Spain ya tiene implantado unos "Sistemas de Gestión" certificados de acuerdo a las normas de calidad (ISO 9001), medioambiental (ISO 14001), Gestión Energética (ISO 50001), Prevención de Riesgos Laborales (ISO 45001), gestión de la Inocuidad del Agua (ISO 22000) y gestión de la continuidad de negocio (ISO 22301), para garantizar el cumplimiento, por encima de lo que la legislación en vigor exige y en conformidad a los estándares de calidad y medioambientales especificados en los mencionados sistemas de gestión, por lo que los proveedores de SUEZ Spain tendrán que conocer las políticas definidas e implantar buenas prácticas en esta línea y ajustarse a dichos procedimientos.

Actualmente las sociedades y los servicios que las sustentan se enfrentan a nuevas amenazas, riesgos transversales, interconectados y transnacionales como son: los desastres naturales, el terrorismo internacional y la cibercriminalidad.

En consecuencia, las empresas, sobre todo las prestadoras de servicios esenciales deben ser capaces de protegerse para evitar devastadores efectos, que van más allá de los económicos.

En cumplimiento de la Directiva del Consejo 2016/148/CE. se dictó el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Según está Directiva, a todas las instalaciones que presten un servicio esencial le corresponden, entre otras, las siguientes obligaciones:

a) Adoptar medidas técnicas y de organización, adecuadas y proporcionadas.

b) Adoptar las medidas adecuadas para prevenir y reducir al mínimo los incidentes.

c) Suministrar al CSIRT de referencia y a la Autoridad competente toda la información que se le requiera para el desempeño de las funciones que les encomienda el Real Decreto-Ley de seguridad de las redes y sistemas de información.

La seguridad dentro del sector del agua está focalizada en identificar vulnerabilidades, minimizar riesgos y mejorar los controles para aumentar la eficiencia operacional y la productividad; y debe estar totalmente alineada con la política de CONTINUIDAD DEL NEGOCIO. La incorporación de la Seguridad Integral en el ámbito industrial como parte general y necesaria dentro de la empresa, asegura la correcta prestación del servicio.

Para ello se requiere disponer de ofertas para EL SUMINISTRO, INSTALACIÓN, PUESTA EN MARCHA 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. Los requisitos técnicos y operativos para el despliegue se detallarán más adelante.

Todos los sistemas deberán cubrir los requisitos funcionales definidos por SUEZ Spain conforme al detalle contenido en este Pliego de Prescripciones Técnicas (PPT).

2. OBJETO DEL CONTRATO.

La presente licitación tiene por objeto el **suministro, instalación, puesta en marcha y operación (servicio de seguridad gestionada SOC 1 y 2) 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**.

La descripción detallada de los suministros y servicios objeto de contratación se contiene en las cláusulas 4.1 y 4.2 del presente pliego

La rápida adopción de aplicaciones tipo SaaS, como Microsoft Office 365 o Salesforce, está llevando a las empresas a buscar cada vez más, soluciones de seguridad basadas en Cloud.

La tendencia es redefinir las conexiones de manera que el tráfico fluya directamente de las oficinas en remoto a Internet, en lugar de articular dicho flujo a través de costosos links MPLS a un data center de gestión centralizada.

Como resultado, las capas de seguridad de la empresa se colocan entre la sede remota e Internet aplicando las medidas de seguridad pertinentes antes de que éste llegue a su destino final.

Además de los servicios de Gateway seguro (SWG), resulta crucial poder incorporar funcionalidades de CASB y DLP a la solución adoptada, 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.

Suez Spain no es ajeno a estas tendencias y en su afán por contar con las soluciones más eficientes y seguras, decide publicar la presente RFP para solicitar propuestas de soluciones SWG/CASB/DLP para SaaS con las características y condiciones que se consignan a continuación.

3. LUGAR DE EJECUCIÓN. ÁMBITO Y ALCANCE DEL CONTRATO.

El alcance y ámbito de aplicación será el equipamiento desde el cuál se permita la navegación a Internet (equipos físicos, portátiles, dispositivos móviles, tablets, etc) de la infraestructura de Suez Spain y todas sus filiales. Además de la securización de las salidas a internet remotas de cada sede y Centros de Procesamiento de Datos. También, la **instalación, puesta en marcha, integración con el sistema de gestión de eventos de seguridad centralizado de SUEZ Spain y el servicio de seguridad gestionada (SOC nivel 1 y 2).**

La solución debe permitir la identificación, detección, protección y respuesta ante brechas de seguridad en el uso de aplicaciones y servicios en la nube.

Se incluye dentro del alcance del contrato:

- Instalación, configuración y puesta en marcha de la solución completa incluyendo traspaso de conocimientos, formación y documentación.
- Servicio de Seguridad gestionada (SOC nivel 1 y 2)

- Soporte técnico del producto.
- Actualización de licencias.

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

El licitador deberá incluir un diseño de la implementación y configuración conforme a la arquitectura de la infraestructura proporcionando un diseño real y verídico del sistema.

Así mismo, el licitador detallará en la oferta los requerimientos de máquina física o virtual (versión de S.O., Memoria RAM, Disco duro, número de cores, número de interfaces de red, etc.), así como las necesidades de cableado, corriente eléctrica, puntos de red local, etc. necesarios para realizar la implementación de la plataforma. Estos recursos serán suministrados por Suez Spain.

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

El lugar de ejecución serán las oficinas, plantas e instalaciones de Suez Spain en las cuales exista equipamiento que requiera de navegación a Internet.

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 SOC360 de Suez España.

4. REQUERIMIENTOS/CONDICIONES TÉCNICAS DEL CONTRATO.

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

- *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.*
- *Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.*
- *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.*
- *Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.*

4.1. REQUERIMIENTOS DEL SISTEMA A INSTALAR

El objetivo es contar con una solución que permita la identificación, detección, protección y respuesta frente a posibles brechas en el uso de aplicaciones y servicios en la nube y por tanto

la solución deberá contemplar como mínimo los siguientes requerimientos. El incumplimiento de los requerimientos mínimos exigidos a la solución será motivo de exclusión:

REQUERIMIENTOS MÍNIMOS EXIGIDOS

- Debe combinar las capacidades de Proxy SWG + InlineCASB + CloudDLP en la misma consola de forma centralizada (una única consola) y aparecer mínimo, en uno de los cuadrantes de Gartner.
- Debe permitir aplicar políticas basadas en el contexto (usuario, dispositivo, aplicación, instancia, contenido del documento, etc) no es suficiente con permitir o bloquear aplicaciones SaaS, debe ser capaz de inspeccionar en profundidad y entender las diferentes actividades en todo momento (login, logout, invitar, compartir, añadir, editar, ver, entre otras).
- Debe permitir detectar, analizar, bloquear si el dato es sensible, alertar y educar al usuario sobre el riesgo del uso de aplicaciones cloud.
- Debe permitir decodificar miles de aplicaciones cloud y detectar el tránsito del dato entre aplicaciones, para identificar posibles fugas de información.
- Debe de incorporar un módulo de UEBA que permita el análisis sobre el comportamiento de las acciones del usuario, así como de las aplicaciones a las que se conectan.
- Debe poder integrarse con los principales SIEMs del mercado

OTROS REQUERIMIENTOS FUNCIONALES:

La funcionalidad es la capacidad del software de cumplir y proveer las funciones para satisfacer las necesidades específicas de la empresa.

Para mantener el nivel de seguridad requerido es necesario incorporar una solución de securización integral con los siguientes requisitos funcionales:

- Debe disponer de una base de datos de Servicios SaaS, en la que se pueda ver el nivel de riesgo de los servicios consumidos desde la empresa en base a criterios marcados por organizaciones como la CSA (Cloud Security Alliance).
- Debe permitir implementar políticas para educar a los usuarios cuando consuman cierto tipo de aplicaciones en base a los riesgos del punto anterior.
- Debe permitir añadir nuevas capacidades como ZTNA (Zero Trust Network Access) o CSPM (Continuos Security Posture Management), en las que podríamos estar interesados en el medio plazo, deberían poder controlarse desde la misma consola.
- Debe proteger el dato dentro de las aplicaciones del cloud, no es suficiente con sólo proteger el tráfico web. Sin ninguna configuración adicional debemos de poder ver que datos se mueven en miles de aplicaciones cloud, identificando el fichero, tipo de

fichero, si el contenido de este coincide con algún perfil normativo (PCI, GDPR, HIPAA, etc), y la actividad que el usuario ha realizado en el fichero.

- Debe tener presencia tanto en España como en Latam, y a fin de minimizar latencias debe de prestarse sobre CPDs reales y no virtuales, y no sobre cloud pública. Es relevante que tenga CPD físico en Chile.

- Debe de permitir el control de las actividades en SaaS e SaaS (login con una cuenta corporativa o con una cuenta no corporativa, compartir con un usuario corporativo o hacia un usuario no corporativo), la aplicación de políticas en base a esas actividades con contexto distintos en base al tipo de documento sobre el que se esté actuando y el nivel de cumplimiento del dispositivo desde el que se esté accediendo (es corporativo, está bien plataforma, etc). En el caso extremo, debe también permitir el control de actividad y dar seguimiento y protección del dato incluso cuando la conexión se realice desde dispositivos no gestionados /no corporativos, cuando estos acceden a aplicaciones reguladas de la empresa.

- Debe permitir comprender las aplicaciones del Cloud para protegerse a bajo nivel de las nuevas amenazas, no se trata solo de permitir o bloquear un sitio web o una descarga.

- Debe permitir la inspección de TLS1.3 para detectar datos y amenazas dentro de canales cifrados sin impactar en la aplicación cloud y web.
- Debe ir alineado con la estrategia de convergencia SASE donde se ofrezca una única solución modular para cubrir las necesidades a corto y largo plazo de la empresa.
- Debe permitir la importación y exportación de Indicadores de Compromiso (IOCs) de forma automática y ser aplicados únicamente en las instancias de las aplicaciones donde se quiere bloquear o permitir.
- Capacidad de integración y operación sobre distintas plataformas de SO.
- Deber ser una solución global para la totalidad de la red de la infraestructura.
- La solución debe garantizar la alta disponibilidad de todos sus componentes y Disaster Recovery.
- Debe proporcionar capacidad para integrarse con Active Directory y sistemas de doble factor de autenticación.
- La solución debe poder desplegarse sobre sistemas operativos estándares. Se valorarán negativamente soluciones cerradas propietarias

La solución propuesta debe contar con soporte por parte del fabricante 24x7 para el primer año desde la fecha de suministro con desplazamiento a las instalaciones de Suez Spain incluido sin coste adicional. En el caso que la solución tenga componentes hardware el soporte in situ

deberá quedar cubierto con el servicio 24x7 4h tiempo de respuesta. Para los casos de SW además del soporte, la solución propuesta deberá permitir el acceso a nuevas versiones del producto.

Transcurrido el primer año la solución propuesta debe contar con soporte por parte del fabricante 24x7 incluido actualización de licencias conforme a la partida valorada a tal efecto sin otro coste adicional hasta cubrir los tres años de duración del contrato.

4.2. REQUERIMIENTOS DE LA PUESTA EN MARCHA Y SERVICIO DE SEGURIDAD GESTIONADA PARA LA OPERACIÓN DEL SISTEMA.

Las actividades concretas a desarrollar en la puesta en marcha y servicio de seguridad gestionada serán:

4.2.1. ENTREGA DE LOS EQUIPOS

El suministro de las licencias y/o equipos que conforman el sistema objeto de licitación se efectuará para su instalación en SUEZ Spain. El plazo máximo de suministro será de 6 semanas a contar a partir de la formalización del contrato.

4.2.2. IMPLEMENTACIÓN, PRUEBAS Y PUESTA EN MARCHA

Además de la herramienta el adjudicatario deberá llevar a cabo las siguientes tareas de puesta en marcha y asistencia técnica a la explotación de la herramienta.

Montaje y pruebas de funcionamiento. La fecha límite para la ejecución de esta segunda fase será de 8 semanas a partir de la fecha de entrega de los equipos. El abono de la parte correspondiente a esta segunda fase será el 40% restante del importe de adjudicación, realizándose en los siguientes 30 días naturales contando a partir de la fecha de firma del acta de recepción definitiva una vez realizadas las pruebas de funcionamiento.

La propuesta deberá incluir un plan de despliegue de la solución en la que se detalle cómo van a desarrollarse los siguientes puntos:

- Configuración Inicial de la plataforma
- Configuración y generación de paquetes a distribuir
- Configuración de conectores necesarios de SCCM
- Configuración de conectores Active Directory
- Control del despliegue de los agentes que será efectuado por el Cliente
- Comprobación de conectividad de los agentes desplegados con las políticas
- Creación de Políticas básicas
- Migración de políticas actuales de la solución actual

- Creación de los perfiles de administración necesarios
- Integración con SIEM de Suez Spain

El plan deberá contar con un cronograma orientativo que permita estimar a grandes rasgos los plazos de ejecución del despliegue, sin perjuicio de que estos plazos sean objeto de ajuste posterior en función de las circunstancias imperantes en el momento del comienzo del proyecto.

4.2.3. DOCUMENTACIÓN DE LA IMPLANTACIÓN.

El licitador debe presentar una vez finalizadas las fases de implantación, pruebas, puesta en marcha e integración, la documentación técnica justificativa del cumplimiento de las especificaciones técnicas recogidas en el presente pliego de prescripciones técnicas particulares, configuración de parámetros de la herramienta, rendimiento de redes, equipamiento de control y servidores con análisis del tráfico de datos, pruebas de estrés por carga de tráfico a analizar o presencia de ataques o vulnerabilidades.

A la finalización del despliegue se requerirán de al menos dos jornadas de formación para la capacitación del personal técnico de Suez Spain y usuarios, para el traspaso de conocimientos sobre la implementación realizada, y la entrega de la documentación descriptiva de los pasos realizados durante la implantación, dónde consten las configuraciones llevadas a cabo.

El servicio incluirá la entrega de la documentación de diseño y arquitectura del sistema instalado y manuales de administración y usuario.

4.2.4. SERVICIO DE SEGURIDAD GESTIONADA (SOC 1 y 2)

Una vez definido el despliegue, el documento de propuesta deberá contar con la descripción del servicio de gestión de la solución que permitirá evolucionar todas las funcionalidades habilitadas en el despliegue, afinar las políticas iniciales y desarrollar nuevas políticas con la granularidad requerida por las necesidades de seguridad de SUEZ Spain de manera que puedan reducirse los riesgos en el entorno siempre cambiante del cloud mediante la aplicación de las medidas de seguridad oportunas de acuerdo a los estándares de calidad, eficiencia y eficacia más elevados del mercado.

Con este servicio se prevé implantar un modelo dinámico y de protección continua (antes, durante y después de posibles incidentes) que permita:

- Evolucionar hacia un modelo acorde a los desafíos y objetivos estratégicos actuales.
- 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.

- 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 las vulnerabilidades 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;
    - Optimizar el uso y la robustez de las soluciones y herramientas tecnológicas presentes en la compañía.
- Disponer de un marco de gestión adecuado a la empresa, actualizado y alineado con estándares internacionales.
- Establecer un marco de conocimientos de Ciberseguridad en los ámbitos técnicos y operativos.
- Ser capaz de responder a un marco regulatorio y/o normativo.

El servicio gestionado presenta las siguientes características:

Se valorará positivamente que el SOC esté integrado en la organización FIRST que engloba centros de respuesta ante incidentes a nivel global.

4.2.4.1. ASPECTOS ORGANIZATIVOS

A la hora de diseñar el servicio, deben tenerse en cuenta las siguientes características de la organización en la que se prestará:

a) 3500 equipos

b) Empresas mixtas del grupo Suez Spain

4.2.4.2. CARACTERISTICAS GENERALES DEL SERVICIO

a) Servicio 8x5

b) Recepción Incidencias Plataforma 24x7

c) Duración 36 meses

4.2.4.3. GESTIÓN INFRAESTRUCTURA PLATAFORMA

El servicio comprenderá el mantenimiento necesario de la solución desplegada entendiendo como tal la realización de las actualizaciones que sean necesarias para el funcionamiento de la plataforma y además:

a) Comprobación proactiva de la Plataforma y Agentes, Soporte y Mantenimiento, con la generación de tickets de seguimiento y aplicación de correcciones con el fabricante.

b) Mantenimiento de los perfiles de administración necesarios

4.2.4.4. GESTIÓN DE LA SOLUCIÓN

Además del mantenimiento necesario de la plataforma, 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 SUEZ Spain.

Detección

Actividades que permitan identificar puntos débiles que puedan ser objeto de ataque.

- Detección Básica
- Detección Avanzada
- Detección de anomalías

Protección

Control y gestión de los puntos débiles identificados.

- Aplicar contramedidas
- Bloqueo de IoCs
- Mejora continua

Entre estas acciones se cuentan:

1. Reportar cualquier comportamiento inusual detectado.
2. Clasificación del Incidente Seguridad
   - Se realizará la clasificación de todos los eventos detectados por la plataforma
3. Eliminación de falsos positivos
   - Tras la clasificación, se realizará una selección de los eventos para identificar lo que se consideran falsos positivos, y así poder identificar los

eventos que potencialmente puede considerarse como alertas de seguridad.

4. Generación de Alertas

   - El equipo de analistas especializado del SOC del Proveedor, analizará en profundidad los eventos que pueden considerarse como alerta de seguridad, y dentro del marco de Suez, informará de los que considere constituyen una alerta de seguridad de la debe de estar informado el Cliente. A priori se comunicarán dichas alertas al equipo de seguridad de Suez.

   - Generación de KPIs de valor que permita una visión global y ejecutiva del estado de la seguridad.

5. Valoración impacto Incidente de Seguridad

   - Una vez identificada una alerta de seguridad, el equipo del Proveedor determinará en la medida de lo posible su veracidad, impacto y posible mitigación.

   - Una vez finalizada la investigación, se analizará en profundidad, produciendo como resultado un informe detallado de la misma

6. Comunicación al SOC

   - Una vez identificada, investigada y analizada una alerta de seguridad, el proveedor, la comunicará al SOC de SUEZ, y éste, con la colaboración del proveedor determinará si dicha alerta se convierte en un incidente de seguridad o no.

   - La resolución del incidente de seguridad será liderado por el equipo de seguridad de Suez y participará activamente el SOC del Proveedor en dar soporte. Es probable que se vean involucradas otras áreas corporativas.

   - Facilitar enlaces con grupos de investigación.

7. Seguimiento del Incidente

8. Proteger la evidencia de un incidente

9. Mantener base de datos histórica de incidentes

10. Adaptaciones a las Best Practices de las políticas actuales y/o futuras

    Las políticas generadas para la puesta en marcha inicial han de mejorarse y complementarse con la generación de nuevas políticas y su adaptación a las “best practices” de la empresa, así como a las que proponga el proveedor y que serán consensuadas con SUEZ Spain.

11. Generación de informes:

    - Seguimiento operativo del servicio (Semanal)

El proveedor deberá generar con periodicidad semanal un informe con los indicadores más importantes de la solución ofertada que incluirá, entre otros aspectos, los detalles de uso, las alertas generadas, los incidentes de seguridad creados y resueltos, número de tickets generados y resueltos, incidencias que afecten al buen funcionamiento de la solución y las recomendaciones que se estimen oportunas.

Los aspectos y formato del informe deberán consensuarse entre el proveedor y SUEZ Spain.

- Informe del estado de la seguridad y sus posibles desviaciones para la Dirección (Mensual)
- Informe con el seguimiento de indicadores (ANS): Contendrá el detalle de los indicadores y la planificación de las acciones correctivas, preventivas y de mejora acordadas entre las partes, su grado de avance y de implantación, así como los resultados obtenidos y el impacto en la operativa del Servicio (Mensual).
- Informe de resultados de actuación sobre un ataque o incidente gestionado (Incidente clasificado como grave).

4.2.4.5. ACUERDO DE NIVEL DE SERVICIO (ANS)

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.

4.2.4.5.1. GESTIÓN Y MANTENIMIENTO DE LA SOLUCIÓN TECNOLÓGICA

Si la incidencia corresponde a una avería de hardware o de software, el equipo de servicio hará un escalado al fabricante para su resolución, de acuerdo con los parámetros incluidos en la prestación del servicio.

Si la resolución de la avería implica la presencia del personal del fabricante, el personal del servicio acompañará y supervisará en todo momento al mismo durante la presencia en las instalaciones de Suez Spain.

Tipo de Servicio	Modalidad
Gestión y mantenimiento de la solución tecnológica	24x7x365

4.2.4.5.2. GESTIÓN DE LA CIBERSEGURIDAD

El objeto principal de este servicio es proteger en todo momento la infraestructura de Suez Spain de cualquier amenaza cibernética. Este servicio se medirá según los siguientes aspectos:

Tipo de Servicio	Modalidad
Servicio de detección y protección	8x5
Gestión de Incidencias (ticketing)	24x7

En ambos casos, el modelo de gestión de incidencias es evolutivo desde un nivel N1 (bajo) al N4 (crítico):

El nivel de servicio dependerá de la priorización requerida en la gestión/resolución de las incidencias que, a su vez, se regirá por el Impacto y la Urgencia. 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 (grado de afección que la incidencia tiene en el servicio):

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 (grado hasta el que es posible demorar la solución):

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 Suez Spain 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 función de la prioridad de la incidencia se establecerá si se ha cumplido o no con el tiempo de respuesta esperado (valor máximo), tal como se indica en la tabla. El % de cumplimiento se obtendrá dividiendo, según su prioridad (N1, N2, N3 y N4), las incidencias que han cumplido con los tiempos esperados entre el total de incidencias abiertas en el periodo considerado (mensual).

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, tal como se traslada en el 4.2.4.7 del presente pliego.

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.

El servicio también requiere de la gestión de Problemas según ITIL (tales como incidencias repetitivas). El licitador propondrá en su propuesta técnica su mejor aproximación al tratamiento y gestión de problemas del servicio.

4.2.4.5.3. PETICIONES

El servicio también atenderá y ejecutará peticiones de cambio cursadas por la herramienta de ticketing y categorizadas convenientemente.

Las peticiones no serán atendidas en 24x7, ya que no es requerido. Por lo tanto, el servicio de atención será de 8x5 y estará sujeto a los siguientes tiempos de respuesta en función del grado de prioridad que Suez Spain le haya asignado a la petición de cambio:

Prioridad	Tiempo de Respuesta
Alta	8 hr.
Media	16 hr. (2 días)
Baja	24 hr. (3 días)

4.2.4.6. FASE DE DEVOLUCIÓN DEL SERVICIO

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 Suez Spain) el Prestador del Servicio diseñará un plan de finalización (Devolución) de ejecución del Servicio.

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 le Prestador del Servicio transfiera el conocimiento y experiencia existente, de modo que pueda ser utilizado como un recurso disponible para el personal de Suez Spain 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.
- Generar toda la documentación actualizada de procedimientos, manuales, infraestructuras y desarrollos informáticos asociados al objeto de contrato.

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

4.2.4.7. PENALIZACIONES

Este servicio estará supeditado a los ANSs de servicio 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 factura ción mensual)
				[1]	[2]	
Tiempo de Respuesta	N4	Critica	≤ 2 horas	90 %	66 %	P4= 5%
	N3	Alta	≤ 8 horas	90 %	66 %	P3= 2%
	N2	Media	≤ 12 horas	80 %	66 %	P2= 2%
	N1	Baja	Next Bussines day	80 %	66 %	P1= 2%

Notas importantes:

- Si en el cálculo del ANS mensual correspondiente a un nivel de prioridad concreto (N_i) el número total de incidencias registradas de dicho nivel es inferior o igual a 5, se aplicarán los criterios de % de Cumplimiento indicados en **[2].** Si el número de incidencias registradas es superior a 5, se aplicarán los indicados en la columna **[1]**.
- 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 **11 %** 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);

Suez Spain estará facultada para:

(i) resolver el contrato, o bien

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

4.3. EQUIPO DE TRABAJO

Las ofertas incluirán una descripción detallada de los medios técnicos, procedimientos y medios personales destinados a la prestación de este servicio.

La cualificación de las personas destinadas a formar parte del equipo de trabajo que preste este servicio será acorde con las tareas a realizar, y se ajustará a los siguientes roles y perfiles profesionales.

4.3.1. SERVICE MANAGER

El licitador propondrá en su oferta un Service Manager que permita abordar con garantías las tareas objeto del contrato. Sus funciones serán las siguientes:

- Dirigir y coordinar a los medios personales que presten los servicios de instalación y configuración de la solución propuesta, impartiendo al efecto las órdenes e instrucciones necesarias para la ejecución de los trabajos.
- Realizar las funciones de contacto y asesoramiento directo a SUEZ.
- Supervisión de las incidencias producidas durante la vida del contrato.
- Seguimiento del cumplimiento de los SLAs del contrato.
- Programación y seguimiento de reuniones.
- Supervisión de la documentación del proyecto.
- Conocimiento y experiencia en implantación de estas Soluciones/Servicios en Empresas de Utilities, en concreto Suministro y Tratamiento de Agua.

4.3.2. TÉCNICOS EXPERTOS

Los profesionales que como equipo principal sean responsables de la ejecución del trabajo, deberán disponer de la cualificación necesaria y de la titulación adecuada a la naturaleza de los trabajos, así como conocimiento y experiencia en implantación de estas Soluciones/Servicios en Empresas de Utilities, en concreto Suministro y Tratamiento de Agua.

Se valorará positivamente la experiencia de más de tres años gestionando soluciones de SWG o CASB en entornos no sectoriales como el anteriormente señalado.