Àrea d'Innovació, Governs Locals i Cohesió Territorial
Direcció de Serveis de Tecnologies i Sistemes Corporatius

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACIÓN DE LOS SERVICIOS DE CIBERSEGURIDAD DE LOS SISTEMAS INFORMÁTICOS DE LA DIPUTACIÓN DE BARCELONA: SERVICIOS DE MONITORIZACIÓN Y AUDITORÍAS DE CIBERSEGURIDAD. DIVIDIDO EN 2 LOTES

(Exp. 2021/0001954)

Índice de contenidos

1. Antecedentes

La Dirección de servicios de tecnologías y sistemas corporativos (DSTSC) de la Diputación de Barcelona tiene como misión proporcionar todos los servicios e infraestructuras de informática y telecomunicaciones de la corporación, tanto para el ámbito interno, como también en relación con el soporte a los entes locales. De este modo se asegura una dirección única para el tratamiento lógico de la información y sus redes de transmisión, independientemente de su formato físico.

Entre otras tiene asignadas las siguientes funciones:

- Llevar a cabo los criterios fijados por la corporación en materia de tecnologías de la información (informática, telecomunicaciones y, en general, aquellas tecnologías relacionadas con el tratamiento automatizado de la información) y proponer los recursos necesarios que hay que habilitar para esta finalidad.
- Coordinar las tareas administrativas del ámbito TIC de todas las unidades de la corporación y, de forma particular, aquellas que tienen interrelación, y proponer las medidas adecuadas para una máxima normalización.
- Controlar y hacer el seguimiento de aquellas tareas en materia TIC realizadas para la corporación mediante recursos externos.
- Proponer y gestionar las actuaciones a desarrollar por la corporación en materia TIC que, dentro de los supuestos de la cooperación y asistencia, se realicen para los entes locales de la demarcación de Barcelona.
- Desarrollar y gestionar los proyectos TIC que se produzcan a propuesta de las áreas, direcciones y servicios.
- Coordinar la formación y reciclaje del personal corporativo en materia TIC.
- Informar el gasto económico que generen las áreas, direcciones y servicios de la corporación y sus organismos autónomos en materia TIC.
- Asesorar los organismos autónomos de la corporación en materia TIC, cuando así se requiera y tutelar, si procede, la homogeneidad en el tratamiento de los sistemas de información comunes.

En relación con este expediente en concreto la DSTSC promueve la contratación de los servicios de monitorización y auditorías de ciberseguridad de los sistemas informáticos de la Diputación de Barcelona, con el objetivo de mejorar la protección ante las ciberamenaces a las cuales están expuestos.

En la actualidad los sistemas informáticos de las organizaciones suponen la base del funcionamiento y conocimiento. Cada vez resulta más necesario aumentar la seguridad de estos sistemas, ante software maliciosos o ataques de robo de datos, y hacer frente a los incidentes de seguridad las 24 horas del día.

Ante un incidente de seguridad es importante disponer de un servicio que permita la monitorización de los acontecimientos de seguridad generados a partir de las transacciones que realizan los servidores y los equipos de comunicaciones, ubicados en los diferentes CPD de la Diputación de Barcelona, y que permita reaccionar inmediatamente. Este tipo de servicio se ofrece desde centros especializados llamados SOC (Security Operation Center).

De lo contrario, para cumplir los requerimientos del Esquema Nacional de Seguridad hay que realizar periódicamente auditorías de seguridad de los sistemas para verificar su protección

ante unas amenazas que van cambiando continuamente de forma y que cada vez logran mayor nivel de sofisticación.

Estas auditorías tienen que permitir detectar tanto las vulnerabilidades a ataques provenientes de fuera de la red corporativa, como las que se puedan producir desde el interior y que puedan poner en peligro la disponibilidad de los servicios y la seguridad de los datos.

Las especificaciones que figuran en el presente documento se ajustan a lo que se prevé en el artículo 126, Reglas para el establecimiento de prescripciones técnicas, de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se trasponen al ordenamiento jurídico español las Directivas del Parlamento Europeo del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

2. Objeto

El objeto del presente pliego es la contratación de los servicios de ciberseguridad de los sistemas informáticos de la Diputación de Barcelona: servicios de monitorización y auditorías de ciberseguridad, dividido en 2 LOTES.

3. Alcance

El objeto del contrato se ha dividido en dos lotes, a los que les corresponde, respectivamente, el alcance siguiente:

- **Lote 1: Servicios de Monitorización**. El servicio incluye todos los elementos necesarios para garantizar una rápida respuesta a las alertas de seguridad. En concreto:
  - Herramienta de correlación avanzada de logs de diferentes sistemas SIEM. Acrónimo inglés que hace referencia a la expresión Security Information and Event Management y que tiene como finalidad principal poder hacer una rápida respuesta a las alertas de seguridad.
  - Configuración del sistema SIEM. Hay que garantizar que la configuración sobre el software SIEM sea la más eficiente para garantizar la detección de alertas y para actuar de manera adecuada.
  - Monitorización de la seguridad 24x7. El análisis de los acontecimientos y la vigilancia en sistemas externos tiene que permitir dar una rápida respuesta a cualquier alerta y definir la configuración de los equipos de forma que se reduzca al máximo su vulnerabilidad.
  - Formación continúa de técnicos y trabajadores. La sensibilización de técnicos y trabajadores es clave para garantizar la seguridad de los sistemas informáticos.

- **Lote 2: Auditorías de Ciberseguridad**. Alcanzará las tareas siguientes:
  - Auditoría de seguridad externa. Auditoría para encontrar vulnerabilidades en los sistemas informáticos desde un acceso externo (desde internet).
  - Auditoría de seguridad interna. Auditoría para encontrar vulnerabilidades en los sistemas informáticos desde un acceso interno (desde la misma red interna).
  - Soporte a la solución de las vulnerabilidades detectadas.Soporte y asesoramiento en las acciones necesarias para solucionar los problemas detectados.

4. Descripción del Servicio

En relación al contenido del presente epígrafe, se divide en dos apartados, uno para cada uno de los lotes identificados como parte del objeto del contrato, donde cada apartado estará subdividido en los subapartados que se han considerado necesarios para facilitar su comprensión y fijar, sin ningún tipo de margen a la interpretación, las características de las prestaciones a ejecutar.

LOTE 1. Servicios de monitorización

El servicio tiene que permitir, a partir del análisis de los datos de los diferentes sistemas informáticos, reaccionar inmediatamente a acciones de software maliciosos, ataques de robo de datos, suplantaciones de identidad y, en general, a cualquier ciberataque que pueda suponer una alerta o un incidente de seguridad en los sistemas informáticos. El servicio también incluye la formación continua de técnicos informáticos y usuarios, tal como se determina al subapartado 4.6. Formación Continúa.

4.1. Herramienta SIEM

La empresa contratista instalará un sistema SIEM en el Centro de Proceso de Datos (CPD) que determine la Diputación de Barcelona capaz de cubrir todas las funcionalidades necesarias para la detección de alertas a partir de la gestión de acontecimientos de diferentes sistemas.

Los diferentes sistemas de donde hay que recuperar datos variará durante la duración del contrato, ya sea por obsolescencia de los equipos, por ampliación de la capacidad, por la creación de nuevos servicios o por la ampliación del ámbito a analizar. Actualmente este es el entorno de trabajo que podríamos considerar estable en el tiempo:

- **Active Directory de Microsoft** (5 equipos).
- **Firewall Palo Alto** (3 equipos).
- **Firewall de Correo Cisco Ironport** (3 equipos).
- **ADC Netscaler** (2 equipos con 8 instancias).
- **TMG de Microsoft** (4 equipos).
- **IIS de Microsoft** (2 equipos).
- **NAS** (5 equipos).
- **Apache** (2 equipos).

La empresa contratista asumirá el coste de todo el hardware y de las licencias de software necesarias, así como la instalación, configuración, administración y mantenimiento del sistema.

Ni el logs de los diferentes equipos a monitorizar, ni ninguna copia de estos datos, procesadas a través del servicio SIEM, podrán salir de ningún servidor de la red corporativa.

Requerimientos técnicos

La empresa contratista proporcionará todo el hardware necesario para la ejecución del SIEM y todos los elementos necesarios para la conexión en la red interna. El hardware se instalará al CPD de la Diputación de Barcelona.

La capacidad del hardware y software tendrá que estar correctamente dimensionada para analizar hasta 3.000 acontecimientos por segundo (APS).

Requerimientos funcionales del SIEM:

- Monitores en tiempo real (disponibilidad, salud, comportamiento).
- Generador de informes (personalización, automatización).
- Gestor de inventario. Inventario automático de activos.
- Gestor de incidencias y reacción a ellas.
- Recolección de información.
- Motor de correlación: lógica, cruzada y de inventario.
- Generador y gestor de reglas de correlación.
- Gestores para modificar prioridades, realizar ajustamientos y crear políticas de recolección.
- Cumplimiento de normas de seguridad, paneles de métricas y medidas de riesgo.
- Interfaces de busca y análisis forense.
- Módulo de cumplimiento. Capacidad de relación acontecimiento-control de normativa.
- Permitir conocer los valores de SLA (Service Level Assurance) de la seguridad de la red en tiempo real.
- Módulo de gestión de identidades.
- Escaneo de vulnerabilidades.
- Minería de datos.
- Escaneo de nuevos activos en la red.
- Registro de alertas.
- Acceso a los datos por los técnicos de la DSTSC.

4.2. Configuración SIEM

El contratista ejecutará tareas de configuración sobre el software SIEM, ya sea de manera proactiva para mejorar la monitorización y seguridad, o de manera reactiva a raíz de análisis de una alerta de seguridad. Entre otros:

- Configuración y creación de plugins.
- Configuración de un catálogo de directivas de seguridad. Política de correlación.
- Realizar cualquier tarea de carácter preventivo y correctivo necesaria para el correcto funcionamiento.
- Actualizar la equipación a las versiones recomendadas por el fabricante y garantizar su correcto funcionamiento.
- Análisis de viabilidad y de riesgos.
- Definición de los requerimientos y procedimientos de salvaguardia y recuperación del sistema, así como el mantenimiento y la supervisión de su cumplimiento.
- Gestión y control de los usuarios administradores o de sistema, así como de su seguridad, roles y perfiles.
- Modificaciones en la recopilación y tratamiento de acontecimientos.
- Diseño y mantenimiento de mecanismos de filtraje y correlación y propuestas de nuevas políticas.
- Análisis forense de los incidentes de seguridad.

Será responsabilidad del contratista la ejecución y documentación de las tareas realizadas con una descripción de los cambios realizados.

Las tareas propuestas por los técnicos de la DSTSC se harán llegar categorizadas al contratista. El contratista iniciará las tareas proactivas de mantenimiento y las categorizará debidamente.

Una tarea estará finalizada si está plenamente documentada y tiene el visto bueno funcional y técnico de la DSTSC. Toda tarea que no reciba el visto bueno de la DSTSC será devuelta al contratista acumulando los tiempos de ejecución, a todos los efectos y responsabilidades establecido en los ANS que correspondan.

Se establecen tres categorías de criticidad:

Crítica. Tareas que hay que ejecutar de manera inmediata.

Urgente. Tareas que hay que ejecutar de manera preventiva.

Importante. Tareas de mantenimiento de la configuración.

4.3. Monitorización 24x7

El contratista tendrá que monitorizar, de forma continuada (24x7), el análisis de los acontecimientos y mantener la vigilancia en sistemas externos para dar una rápida respuesta a cualquiera alerta y definir la configuración de los equipos de forma que se reduzca al máximo su vulnerabilidad.

En los apartados siguientes, se describen qué acciones de monitorización hay que realizar y cual tiene que ser la gestión de las alertas.

4.3.1. Acciones de monitorización

Las diferentes acciones de monitorización tienen que permitir detectar las alertas de seguridad en el menor tiempo posible para poder actuar de manera inmediata. Una **alerta de seguridad** es cualquier situación que suponga una amenaza concreta sobre la seguridad de los sistemas informáticos de la Diputación de Barcelona.

La monitorización engloba tres acciones: análisis de datos SIEM, vigilancia externa y descubrimiento de activos. Estas acciones se describen en los apartados siguientes:

Análisis datos SIEM

La configuración del SIEM tiene que permitir detectar situaciones de riesgo. El contratista dispondrá de mecanismos para detectar la criticidad de la amenaza descartando falsos positivos y actuando en consecuencia.

Será responsabilidad de la contratista mantener la configuración del SIEM más eficiente (logs, correlaciones, avisos...) para detectar alertas.

Vigilancia externa

El contratista tendrá que revisar sistemas externos para detectar si suponen amenazas para los sistemas de Diputación de Barcelona. Tendrá que ejecutar las acciones siguientes:

- Monitorización de páginas web y de la web profunda relacionadas con la filtración de datos
- Detección y alerta de posibles filtraciones de credenciales de usuario.
- Detección y alerta de posibles ataques o actividades fraudulentas contra la Diputación de Barcelona a Internet.
- Recuperar información de alertas globales, de alertas relacionadas con otras administraciones públicas y realizar la gestión de indicadores de compromiso.

Descubrimiento de activos en la red

Escaneo continuado de la red para detectar nuevos equipos. La empresa contratista valorará el riesgo de cada nuevo equipo detectado y actuará en consecuencia.

4.3.2. Gestión alertas

Una vez el sistema de monitorización detecte una alerta de seguridad tendrá que actuar en consecuencia de su gravedad.

Para cualquier alerta tendrá que realizar las siguientes acciones:

- Notificación a los técnicos de la DSTSC.
- Registro.
- Ejecución acciones de análisis forense.

Se definen tres niveles de alertas:

- Alto. Supone un riesgo alto y hace falta una actuación inmediata. Se tratará como un **incidente de seguridad**.
- Medio. Requiere una actuación a corto plazo.
- Bajo. No supone un riesgo inmediato en la seguridad.

Durante la fase de puesta en marcha se definirán los niveles de alerta en la configuración del SIEM y se fijarán los procedimientos a seguir para las comunicaciones y tareas a realizar. Estos niveles y procedimientos se irán revisando durante la ejecución del contrato para mejorar su eficiencia.

Todas las alertas quedarán registradas siguiendo la metodología propuesta por el CCN-CERT para la gestión de incidentes de seguridad en el Esquema Nacional de Seguridad (ENS), detallada en las Guías CCN-STIC-403 y CCN-STIC-817.

El contratista tendrá que proporcionar un sistema para poder consultar las alertas registradas.

4.4. Canal de comunicación

La DSTSC utiliza Prolin Service Desk como herramienta de seguimiento de las peticiones. Todas las tareas realizadas por la empresa contratista tendrán que quedar registradas y documentadas en este sistema.

Cualquier cambio de situación de una incidencia o petición que haga la empresa contratista tiene que quedar reflejado en el Service Desk.

En el caso de incidencias críticas o urgentes se utilizará el teléfono en primera instancia, que tendrá que estar disponible 24x7 y utilizando el catalán o castellano como lengua. Posteriormente la petición se anotará también en el Service Desk.

Si el contratista utiliza una herramienta propia para la gestión interna de las tareas, se facilitará la integración.

Si la integración con la herramienta del contratista no es posible, la Diputación de Barcelona proporcionará un usuario de acceso a su sistema con el único objetivo de garantizar la actualización de los datos. En cualquier caso la gestión del cumplimiento del ANS será a cargo del contratista y no se podrá obtener a partir del sistema de la Diputación de Barcelona.

4.5. Acceso remoto

La DSTSC dispone de un servicio VPN que tendrá que ser utilizado para acceder remotamente al sistema de información objeto del contrato en caso de conexión desde fuera de sus instalaciones.

Requiere disponer de certificado digital reconocido, para identificarse personalmente, y la tramitación de la solicitud de acceso firmada electrónicamente para cada uno de los miembros del equipo asignado por el contratista. Aparte del control del acceso y de la autenticación del usuario hará falta que se puedan registrar acciones efectuadas sobre el sistema administrado.

La conexión necesaria para este acceso remoto tendrá que estar operativa en el momento de inicio del contrato.

Los gastos que se deriven del uso de este enlace las tendrá que asumir el contratista.

4.6. Formación continúa

La empresa contratista realizará acciones que sirvan para concienciar a técnicos y usuarios de la importancia de seguir buenas prácticas que impidan perder datos personales.

Los contenidos de las acciones tendrán que ser diseñados conjuntamente con técnicos de la DSTSC. Anualmente se ejecutarán 3 acciones:

- **Sesión a técnicos informáticos**. Una sesión anual de una duración de 2 a 3 horas sobre ciberamenaces actuales y las buenas prácticas que hay que realizar para reducir el riesgo. La sesión irá dirigida a técnicos de la Diputación de Barcelona y, por lo tanto, entrará en temas de programación de páginas web, configuración de dispositivos o políticas de seguridad. La sesión se realizará en la ciudad de Barcelona preferentemente de manera presencial. Si no se pudiera realizar de manera presencial se realizará a través de una plataforma proporcionada por la DIBA.
- **Sesión a usuarios**. Cuatro sesiones anuales de una duración de 2 horas sobre ciberamenaces actuales y las buenas prácticas que hay que realizar para reducir el riesgo. La sesión irá dirigida a usuarios finales de los sistemas informáticos de la corporación y, por lo tanto, tratará temas de gestión de contraseñas, uso del correo, uso de los dispositivos móviles o uso de redes Wifi. La sesión se realizará en la ciudad de Barcelona preferentemente de manera presencial. Si no se pudiera realizar de manera presencial se realizará a través de una plataforma proporcionada por la DIBA.
- **Campaña de correo malicioso**. Cuatro campañas anuales de envío de correo malicioso (Phishing) a un mínimo de 500 usuarios que sirvan para analizar su respuesta y mejorar la concienciación. La campaña incluye:
    - Definición de la campaña: destinatarios, mensaje, plazos, etc.
    - Envío correos.
    - Informe con el análisis de las respuestas y la comparativa entre campañas.
    - Recopilación de datos en formato electrónico que permita el análisis estadístico.

LOTE 2. Auditorías de ciberseguridad

El servicio tiene que permitir descubrir las vulnerabilidades presentes en la infraestructura tecnológica de la Diputación de Barcelona, comprobar los efectos que la explotación de estas vulnerabilidades pueden producir en las diferentes dimensiones de la seguridad de la información - disponibilidad, integridad y confidencialidad-, documentar tanto los riesgos de la

situación actual como las soluciones a corto, mediano y largo plazo. El servicio también incluye el soporte en la implementación de las soluciones.

4.7. Auditoría de seguridad externa

El servicio de auditoría de seguridad externa anual tendrá el siguiente alcance:

- Test de intrusión de servicios externos en todo el rango de direcciones públicas de la DIBA.
- Test de intrusión en pàgines web de la DIBA de 10 dominios diferentes.

La auditoría de seguridad externa se realizará desde dependencias de la empresa contratista y, de manera coordinada, con los técnicos de la DSTSC. Esta auditoría se realizará en el formato de "caja negra", es decir, sin información previa ni credenciales de usuario, e intentará recopilar información, comprobar los diferentes sistemas de autenticación implementados, comprobar el uso que se hace de la gestión de las sesiones y como las aplicaciones gestionan la validación de los datos (inyecciones de código).

El resultado de la auditoría externa documentará las vulnerabilidades detectadas siguiendo el estándar CVE.

La criticidad de las vulnerabilidades seguirá el estándar CVSS.

El informe de la auditoría también se entregará en formato electrónico para permitir el análisis estadístico.

4.8. Auditoría de seguridad interna

El servicio de auditoría de seguridad interna anual tendrá el siguiente alcance:

- Test de intrusión de servicios externos
  - 4 redes de servidores de màscara 24.
  - Infraestructura SAP (20 servidores).
  - Infraestructura ORACLE (10 servidores).
- Test de intrusión en redes WIFI:
  - 4 SSID.

La auditoría de seguridad interna se realizará desde dependencias de la DIBA y de manera coordinada con sus técnicos. Esta auditoría se realizará tanto en el formato de "caja negra", es decir, sin información previa ni credenciales de usuario, como en el formado "caja blanca", en el que se proporcionarán unas credenciales válidas, e intentará recopilar información, comprobar los diferentes sistemas de autenticación implementados, comprobar el uso que se hace de la gestión de las sesiones y como las aplicaciones gestionan la validación de los datos (inyecciones de código).

El resultado de la auditoría interna documentará las vulnerabilidades detectadas siguiendo el estándar CVE.
La criticidad de las vulnerabilidades seguirá el estándar CVSS.

El informe de la auditoría también se entregará en formato electrónico para permitir el análisis estadístico.

4.9. Soporte a la solución de las vulnerabilidades detectades

La empresa contratista tendrá que ofrecer soporte y asesoramiento en las acciones necesarias para solucionar los problemas y vulnerabilidades detectados.

Este soporte y asesoramiento se realizará en las dependencias de la DIBA en el formato de 10 horas mensuales presenciales, obligatoriamente y sin coste adicional para la Diputación de Barcelona.

4.10. Horario del Servicio

- De 9 h a 14 h y de 15:30 h a 18:30 h de lunes a jueves no festivos en Barcelona ciudad.
- De 8:30 h a 14:30 h viernes no festivos en Barcelona ciudad y durante el horario de verano aplicable a la Diputación de Barcelona.

5. Modelo de prestación de servicio

En este apartado se definen las líneas básicas de cómo se quieren recibir los servicios pedidos.

5.1. Equipo de trabajo

A nivel general y referido a los dos lotes en los que está dividido el objeto del contrato, el contratista tiene que tener presente, en relación con el equipo de trabajo, las directrices siguientes.

En relación con los integrantes del equipo de trabajo que la empresa contratista tiene que disponer en su plantilla para la prestación del servicio, con independencia de su porcentaje de dedicación final, se tendrán que corresponder con los perfiles siguientes:

- Responsable del contrato
- Referente técnico
- Técnicos
- Delegado de protección de datos

La empresa contratista tendrá que estar en disposición de dar cobertura inmediata en caso de enfermedad, vacaciones o cualquier otra contingencia que afecte su personal, a fin de que en ningún supuesto el servicio quede sin cubrir.

5.1.1. Responsable del contrato

Realizará las tareas de coordinación, seguimiento y control de la gestión del contrato. Por parte de la DSTSC se designará un coordinador que realizará funciones análogas.

Será función del Responsable del contrato de la empresa contratista conocer en profundidad los servicios cubiertos por el contrato y asegurar que todo el personal de la empresa contratista que participa en el servicio tenga los conocimientos adecuados y asuma los compromisos de servicios adquiridos y vele por el cumplimiento de todos los requerimientos incluidos en el contrato.

A título de ejemplo, el Responsable del contrato realizará las funciones siguientes:

- Definición del plan de servicio que servirá como guía para la ejecución de los servicios durante la vigencia del contrato. Los componentes del plan tendrán que incluir las métricas de satisfacción, recursos necesarios y una agenda de las actividades planificadas y las reuniones de seguimiento. Este plan de servicios se revisará periódicamente para repasar los objetivos, y será acordado y supervisado por la DSTSC.
- Supervisión de la puesta en marcha para cumplir con el plan presentado, de acuerdo con los requisitos que determine el coordinador de la DSTSC.
- Supervisión de la calidad. Se preparará un informe de seguimiento que resumirá los servicios proporcionados, permitiendo la evaluación y seguimiento del último periodo realizado sobre el plan de servicio.
- Supervisión de los riesgos. Manteniendo actualizada la lista de riesgos del servicio y de los derivados de los posibles cambios no efectuados.
- Supervisión de los incidentes, problemas, consultas, peticiones, etc.
- Gestión del escalado. Los incidentes (o cualquier otra acción) que necesiten ser escalados a recursos técnicos o a niveles de responsabilidad superiores dentro de la propia empresa o en el caso de subcontratación a otras empresas, serán gestionados estrechamente para acelerar su resolución.

5.1.2. Referente técnico

Será el interlocutor único con los técnicos de la DSTSC y quien coordinará los técnicos de la empresa contratista que puedan intervenir en cualquier actividad solicitada. Asumirá las funciones siguientes:

- Coordinar las relaciones entre el equipo técnico y los técnicos de la DSTSC.
- Comunicar periódicamente el estado del servicio.
- Transmitir al equipo técnico las directrices para el correcto desarrollo del servicio.
- Supervisar la aplicación de los procedimientos que solicite la DSTSC.
- Asistir a las reuniones periódicas de seguimiento del servicio.
- Gestionar las tareas o procedimientos, aplicando medidas correctivas en caso de desviación.
- Garantizar la calidad de los procedimientos y tareas.
- La gestión de las intervenciones planificadas.
- Elaborar los informes técnicos de seguimiento y bajo demanda.
- Analizar el servicio para proponer mejoras.

5.1.3. Técnicos

Tendrán que ser capaces de ejecutar, con el nivel de calidad suficiente, las tareas derivadas del servicio.

Los técnicos adscritos al servicio tendrán que poder asumir puntas de trabajo para cubrir convenientemente todas las necesidades que se planteen en cada momento, de forma que el servicio no se vea afectado por aumentos esporádicos de tareas a realizar.

Este equipo trabajará normalmente en las instalaciones del contratista, pero puntualmente su presencia podrá ser requerida sin que suponga un coste adicional.

Los técnicos asumirán el resto de las tareas identificadas en el presente pliego de prescripciones técnicas. A título de ejemplo:

- Resolución de incidencias, consultas, adaptaciones, etc.
- Operaciones ordinarias de mantenimiento y administración.
- Documentación de los sistemas, configuraciones, despliegues, adaptaciones, etc.
- Actualizaciones de versiones (parches, menores, mayores), así como cualquier otra tarea derivada del despliegue en los diferentes entornos identificados a nivel de servicio.

5.1.4. Delegado de protección de datos

Tendrá las funciones siguientes:

- Asesorar sobre la aplicación de los principios de privacidad desde el diseño y por defecto del proyecto.
- Informar y asesorar al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que los incumben en virtud del RGPD y otras disposiciones de protección de datos de la Unión o de los estados miembros.
- Supervisar el cumplimiento del que dispone el RGPD, otras disposiciones de protección de datos de la Unión o de los estados miembros y de las políticas del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Cooperar con los responsables de protección de datos de la Diputación de Barcelona en cuestiones relativas al tratamiento objeto del presente pliego, incluida la evaluación de impacto relativa a la protección de datos, la consulta previa ante la autoridad, y, si procede, sobre cualquier otro asunto.
- Ejercer sus funciones prestando la debida atención en los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

5.1.5. Reglas especiales respecto del personal laboral de la empresa contractista

A todos los efectos y en relación con el equipo de trabajo determinado, en su conjunto, el contratista tiene que tener presente:

- Corresponde exclusivamente al contratista la selección del personal que, reuniendo los requisitos exigidos en los pliegos, formará parte del equipo de trabajo adscrito a la ejecución del contrato, sin perjuicio de la verificación por parte de la DSTSC del cumplimiento de aquellos requisitos.
- El contratista velará por la estabilidad del equipo de trabajo, y porque los cambios en su composición sean puntuales y obedezcan a razones justificadas, en orden a no alterar el buen funcionamiento del servicio, informando en todo momento a la DSTSC.
- El contratista asume la obligación de ejercer de forma real, efectiva y continúa, sobre el personal integrante del equipo de trabajo encargado de la ejecución del contrato, el poder de dirección inherente a todo empresario. En particular, asumirá la negociación y el pago de los salarios, la concesión de permisos, cuando proceda, las obligaciones legales en materia de prevención de riesgos laborales, el ejercicio de la potestad disciplinaria, así como los derechos y obligaciones derivados de la relación contractual entre empleado/empleador.

- La empresa contratista tendrá que velar especialmente porque los trabajadores adscritos a la ejecución del contrato desarrollen su actividad sin extralimitarse en las funciones desarrolladas respecto de la actividad delimitada en los pliegos objeto del contrato.
- En caso de que los técnicos no satisfagan los mínimos de formación, de eficiencia, de metodología, aptitud y eficacia deseados, la DSTSC podrá pedir su sustitución a la contratista, que lo tendrá que hacer efectiva en un tiempo máximo de dos semanas.
- En el caso excepcional de que se tenga que realizar algún cambio, el sustituto tendrá que reunir, como mínimo, los mismos requisitos exigidos en el sustituido. Cualquier modificación de los técnicos tendrá que ser comunicada a la DSTSC con una antelación mínima de 1 semana y tendrá que presentar un plan de traspaso de conocimiento al nuevo miembro del equipo que se tendrá que concretar en un máximo de 2 semanas, que se entenderá el tiempo máximo a partir del cual el nuevo recurso se incorpore al equipo de trabajo.
- El contratista tendrá que informar a la DSTSC de cualquier contingencia que afecte a su personal y tendrá que disponer de personal para dar cobertura inmediata si se considera necesario.
- Cualquier ausencia planificada del personal de la contratista tendrá que ser aprobada por la DSTSC.

5.1.6. Perfiles asignados y de su nivel de dedicación

A continuación se detallan, para cada uno de los lotes en los que se divide el objeto del presente contrato, el número de perfiles requeridos y su dedicación efectiva.

LOTE 1: Servicios de monitorización

Responsable del contrato

Esta persona tendrá que tener una dedicación efectiva ordinaria del 5% de su jornada laboral, según el convenio colectivo aplicable, de acuerdo con la cláusula 1.3 del PCAP, aplicado sobre el cómputo total anual de horas.

Aun así tiene que tener presente que en cualquier momento tiene que poder responder a consultas sobre el servicio y podrá requerirse su presencia, sin que esto suponga ningún coste económico adicional a la Diputación de Barcelona. Es imprescindible que esta persona disponga de un teléfono móvil destinado a su localización.

Referente técnico

Esta persona tendrá que tener una dedicación efectiva ordinaria del 10% de su jornada laboral, según el convenio colectivo aplicable, de acuerdo con la cláusula 1.3 del PCAP, aplicado sobre el cómputo total anual de horas.

Aun así tiene que tener presente que en cualquier momento tiene que poder responder a consultas sobre el estado de incidencias o peticiones y podrá requerirse su presencia, sin que esto suponga ningún coste económico adicional a la Diputación de Barcelona. Es imprescindible que esta persona disponga de un teléfono móvil destinado a su localización.

Técnicos

La empresa contratista tendrá que disponer de un mínimo de 6 técnicos, con una dedicación efectiva ordinaria del 10% de su jornada laboral, según el convenio colectivo aplicable, de acuerdo con la cláusula 1.3 del PCAP, aplicado sobre el cómputo total anual de horas.

Delegado de protección de datos

Esta persona tendrá que tener una dedicación efectiva ordinaria del 1% de su jornada laboral, según el convenio colectivo aplicable, de acuerdo con la cláusula 1.3 del PCAP, aplicado sobre el cómputo total anual de horas.

LOTE 2: Auditorías de ciberseguridad

Responsable del contrato

Esta persona tendrá que tener una dedicación efectiva ordinaria del 10% de su jornada laboral, según el convenio colectivo aplicable, de acuerdo con la cláusula 1.3 del PCAP, aplicado sobre el cómputo total anual de horas.

Aun así tiene que tener presente que en cualquier momento tiene que poder responder a consultas sobre el servicio y podrá requerirse su presencia, sin que esto suponga ningún coste económico adicional a la Diputación de Barcelona. Es imprescindible que esta persona disponga de un teléfono móvil destinado a su localización.

Referente técnico

Esta persona tendrá que tener una dedicación efectiva ordinaria del 20% de su jornada laboral, según el convenio colectivo aplicable, de acuerdo con la cláusula 1.3 del PCAP, aplicado sobre el cómputo total anual de horas.

Aun así tiene que tener presente que en cualquier momento tiene que poder responder a consultas sobre el estado de incidencias o peticiones y podrá requerirse su presencia, sin que esto suponga ningún coste económico adicional para la Diputación de Barcelona. Es imprescindible que esta persona disponga de un teléfono móvil destinado a su localización.

Técnicos

La empresa contratista tendrá que disponer de un mínimo de 3 técnicos, con una dedicación efectiva ordinaria del 15% de su jornada laboral, según el convenio colectivo aplicable, de acuerdo con la cláusula 1.3 del PCAP, aplicado sobre el cómputo total anual de horas.

Delegado de protección de datos

Esta persona tendrá que tener una dedicación efectiva ordinaria del 1% de su jornada laboral, según el convenio colectivo aplicable, de acuerdo con la cláusula 1.3 del PCAP, aplicado sobre el cómputo total anual de horas.

5.2. Seguimiento del Servicio

En relación con los dos lotes en los que está dividido el objeto del contrato, el contratista tendrá que seguir las indicaciones siguientes.

Mensualmente, habrá una reunión de seguimiento para trabajar por la mejora constante del servicio. Esta reunión se hará entre los días 10 y 15 de cada mes y asistirá por parte de la empresa contratista el responsable del contrato y el referente técnico. En esta reunión se revisará el informe mensual, se generarán propuestas de mejora y, en general, se hará un seguimiento de todo el que tenga que ver con la prestación del servicio.

Para cada lote como adscripción de personal hemos pedido 1 responsable de contrato y técnicos

En relación con las reuniones a realizar durante el plazo de vigencia del contrato, sea cual sea su periodicidad y motivo de su convocatoria, se podrán realizar tanto en modalidad presencial como telemática, siempre a criterio de los técnicos de la DSTSC. El contratista

dispondrá de los medios necesarios para adecuarse a cualquier de los dos formatos, sin que esto genere ningún coste adicional para la Diputación de Barcelona.

A continuación se detalla la información que tendrá que constar en este informe de servicio, como mínimo, para cada uno de los lotes en los que se ha dividido el objeto del contrato.

LOTE 1: Servicios de monitorización

El informe mensual del servicio tiene que contener, como mínimo, la siguiente información:

- Alcance de la monitorización realizada.
- Tareas ejecutadas. Indicando nivel, tiempo de ejecución y cumplimiento de ANS.
- Alertas del periodo: tipología y nivel.
- Incidentes de seguridad en el periodo.
- Acciones de formación.
- Propuestas de tareas a realizar para mejorar la monitorización.
- Propuestas de mejora del servicio.
- Situación económica del contrato indicando las facturas presentadas.

LOTE 2: Auditorías de ciberseguridad

El informe mensual del servicio tiene que contener, como mínimo, la siguiente información:

- Estado de la ejecución de las auditorías anuales.
- Tareas realizadas en el apoyo a la solución de las vulnerabilidades.
- Propuestas de mejora del servicio.
- Situación económica del contrato indicando las facturas presentadas.

6. Puesta en marcha

En relación con los dos lotes en los que está dividido el objeto del contrato, el contratista tiene que tener en cuenta lo siguiente.

La fase de puesta en marcha del servicio es el periodo de tiempo que transcurre entre la formalización del contacto y la puesta en marcha de todos los servicios contratados.

Será responsabilidad de la contratista la ejecución de las diferentes fases que conforman la puesta en marcha del sistema de información.

La DSTSC asignará un interlocutor que trabajará conjuntamente con la empresa contratista en la fase de puesta en marcha.

El coste que implique o que derive de cualquier de las actuaciones derivadas de la puesta en marcha se tiene que entender incluido en el presupuesto total del contrato.

En cuanto a las especificidades requeridas para cada uno de los dos Lotes en los cuales se divide el objeto del contrato, el contratista tiene que seguir las prescripciones siguientes.

LOTE 1: Servicios de monitorización

El plan de puesta en marcha tiene que permitir a la empresa contratista cumplir los ANS establecidos a partir del decimoquinto día laborable de la fecha de inicio de la prestación efectiva del servicio. A partir de este día se aplicarán las penalidades correspondientes.

Al inicio de la ejecución del contrato, la empresa contratista tendrá que presentar el plan de puesta en marcha que incluya los mecanismos necesarios para ofrecer el servicio con los niveles de calidad requerido.

Durante esta fase se realizarán las siguientes tareas:

- Instalación del hardware y software SIEM.
- Configuración del SIEM. La Diputación de Barcelona utiliza actualmente un AlienVaut USM All-in-one 150. Como mínimo, todas las reglas de correlación en el sistema actual tendrán que quedar configuradas en el nuevo sistema.
- Puesta en marcha de la monitorización.
- Definición protocolos de actuación delante alertas.

LOTE 2: Auditorías de ciberseguridad

El plan de puesta en marcha tiene que permitir a la empresa contratista cumplir los ANS establecidos a partir del vigésimo día laborable de la fecha de inicio de la prestación efectiva del servicio. A partir de este día se aplicarán las penalidades correspondientes.

Durante esta fase se realizarán las siguientes tareas:

- Captura de conocimiento por parte de los técnicos de la empresa contratista.
- Planificación temporal auditoría externa.
- Planificación temporal auditoría interna.

7. Acuerdos de Nivel de Servicio (ANS)

En relación a los dos lotes en los que está dividido el objeto del contrato, el contratista tiene que tener en cuenta lo siguiente.

Los ANS permiten obtener indicadores para evaluar el grado de cumplimiento del servicio.

El cálculo del ANS se tendrá que hacer por parte de la empresa contratista, con una periodicidad mensual y considerando el horario de la prestación de los servicios y el mes natural.

No computarán los periodos de tiempos en que el contratista está pendiente de respuesta, reuniones, datos o concreción de requerimientos por parte de los técnicos o usuarios de la Diputación de Barcelona o de terceros proveedores siempre y cuando estos no tengan una relación contractual directa con la empresa contratista principal, dado que en aquel caso el tiempo computará como tiempo propio de la contratista a todos los efectos previstos en este Pliego.

Las peticiones solo se considerarán finalizadas si se encuentran completamente documentadas y tienen el visto bueno funcional y técnico de la DSTSC, en caso contrario serán devueltas a la empresa contratista acumulando los tiempos de resolución, a todos los efectos y responsabilidades establecidas en los ANS.

Los tiempos de respuesta y de resolución de incidencias no se podrán ver afectados por aumentos esporádicos del número de incidencias, ni por la coincidencia con otras tareas previstas en el presente pliego.

El tiempo de respuesta es el transcurrido entre la comunicación de la incidencia al contratista, por el canal previsto, hasta que la empresa contratista asume la resolución de la incidencia asignando los recursos necesarios para poder cumplir el tiempo de resolución.

En cuanto a las especificidades requeridas para cada uno de los dos lotes en los cuales se divide el objeto del contrato, el contratista tiene que seguir las prescripciones siguientes.

LOTE 1: Servicios de monitorización

Ejecución de tareas

Tiempos de resolución: Es el tiempo transcurrido entre la comunicación de la tarea al contratista o la detección de la alerta que lo ha generado hasta que la tarea queda ejecutada y documentada por la empresa contratista.

Nivel de calidad: Los tiempos máximos para la finalización de la tarea son:

- Crítica. 2 horas
- Urgente. 8 horas
- Importante. 72 horas

Registro y notificación de las alertas de Seguridad

Tiempo de registro y notificación: Es el tiempo transcurrido entre la detección de la alerta y el registro y la notificación a la DSTSC

Nivel de calidad: El tiempo máximo por el registro y la notificación es de 15 minutos

Ejecución de acciones de análisis forense

Tiempo de ejecución: Es el tiempo transcurrido entre la detección de la alerta y la ejecución de acciones de análisis forense.

Nivel de calidad: El tiempo máximo para la finalización de las acciones es:

- Alerta nivel alto: 2 horas
- Alerta nivel mediano: 8 horas

LOTE 2: Auditorías de ciberseguridad

Parada de servicios por malas prácticas en las auditories

Nivel de calidad: En ningún caso, la ejecución de las auditorías puede provocar la parada de un servicio en producción.

8. Penalidades

En relación con los dos lotes en los que está dividido el objeto del contrato, el contratista tiene que tener en cuenta lo siguiente.

En el caso de incumplimiento de los ANS por parte de la empresa contratista, y en el supuesto que la Diputación de Barcelona opte por la no-resolución del contrato, se prevén las penalidades que se indican junto a cada ANTS.

La contabilización de las penalidades se realizará mensualmente, con efectos a la facturación del mes calculado y sobre la parte fija de aquel periodo.

La cantidad máxima de penalidad se fija en un 50% del importe mensual (IVA excluido). La cuantía no podrá ser superior al 10% del presupuesto del contrato, IVA excluido, ni el total de las mismas podrá superar el 50% del precio del contrato.

Caso de incumplimiento de los acuerdos de nivel de servicio las facturas tendrán que contemplar las penalidades según lo previsto en esta cláusula. En concreto, para las penalidades derivadas del incumplimiento sobre los ANS establecidos se aplicará el siguiente procedimiento:

- Durante la reunión de seguimiento mensual entre el contratista y los técnicos de la DSTSC para evaluar la correcta ejecución de la prestación se analizará, entre otros factores, el desempeño de los ANS.
- Caso que las partes detecten, acepten y validen los incumplimientos, el contratista los recogerá en un apartado específico del informe mensual que tiene que entregará a la DSTSC.
- La Diputación de Barcelona, una vez adoptado el acuerdo administrativo interno correspondiente, notificará al contratista la cantidad exacta que este tendrá que descontar en la factura correspondiente al primer periodo de facturación abierto.
- Caso que el contrato hubiera finalizado (sea cual sea el motivo de esta circunstancia), las cantidades pendientes en concepto de penalidades se descontarán de la garantía definitiva.

En cuanto a las especificidades requeridas para cada uno de los dos lotes en los que se divide el objeto del contrato, el contratista tiene que seguir las prescripciones siguientes.

LOTE 1: Servicios de monitorización

Ejecución de tareas

Las penalidades asociadas al incumplimiento del tiempo de resolución en la ejecución de tareas serán:

Por hora o fracción de tiempo de resolución que superan el nivel de calidad	**Penalidad**
Por tareas críticas	300 €
Por tareas urgentes	200 €
Por tareas importantes	50 €

Registro y notificación de las alertas de Seguridad

Las penalidades asociadas al incumplimiento del tiempo de registro y notificación serán de:

Por cada 15' cumplidos de retraso	**Penalidad**
Por alertas de nivel alto	200 €
Por alertas de nivel medio	50 €
Por alertas de nivel bajo	10 €

Ejecución de acciones de análisis forense

Las penalidades asociadas al incumplimiento del tiempo de ejecución de las acciones de análisis forense serán de:

Por hora de retraso en la finalización de las acciones	Penalidad
Por alertas de nivel alto	200 €
Por alertas de nivel medio	20 €

Formación continúa

Las penalidades asociadas al incumplimiento de los plazos de las acciones de formación serán:

Por cada acción realizada fuera de plazo	Penalitadad
Sesión a teécnicos informáticos	1.000 €
Sesión a usuarios	750 €
Campaña de correo malicioso	750 €

LOTE 2: Auditorías de ciberseguridad

Parada de servicios por malas prácticas en las auditories

Las penalidades asociadas a la parada de servicios en producción por malas prácticas en la realización de las auditorías serán:

Por cada servicio parado	Penalidad
Si afecta a más de 1.000 usuarios	3.000 €
Si afecta entre 100 i 1.000 usuarios.	2.000 €
Si afecta a menos de 100 usuarios	1.000 €

9. Devolución del Servicio

En relación con los dos lotes en los que está dividido el objeto del contrato, el contratista tiene que tener en cuenta lo siguiente.

Seis meses antes de la finalización del contrato, la empresa contratista tendrá que presentar el plan de devolución del servicio que incluya los mecanismos necesarios para traspasar toda la información relacionada con el servicio prestado a Diputación de Barcelona. Este plan incluirá un mínimo de 80 horas de dedicación de recursos de la empresa contratista, sin coste adicional para la Diputación de Barcelona, para llevar a cabo las tareas identificadas.

Un mes antes de la finalización del contrato, el contratista presentará una actualización del plan de devolución del servicio.

La finalización del contrato exigirá también la eliminación segura de los datos personales y de toda la información que se haya utilizado para la ejecución del contrato. Se aportará certificación de su destrucción.

Las tareas de administración, para las que su tiempo de resolución finalice dentro del plazo de duración del contrato, tendrán que quedar cerradas. Si no es así se aplicarán las penalidades correspondientes.

10. Transición del Servicio

En relación con los dos lotes en los que está dividido el objeto del contrato, el contratista tiene que tener en cuenta lo siguiente.

La fase de transición del servicio se corresponde con el periodo de tiempo donde la nueva contratista (cuando se ha dado el caso que ha habido alternancia entre contratistas) tiene que realizar tareas relativas al traspaso de conocimiento y de carácter preparatorio, en cuanto a su equipo de trabajo, para asumir la fase de arranque y puesta en marcha del servicio con plena garantía de continuidad y en la fecha prevista de inicio de prestación del servicio.

Esta fase de transición del servicio se establece entre el momento de la formalización del contrato y el inicio de la prestación del servicio.

Entre los objetivos de esta fase destacan:

- Recoger el traspaso de conocimiento por parte del contratista saliente con el fin de garantizar la continuidad del servicio.
- Recogida cuidadosa de requerimientos para la planificación del arranque del servicio por parte del contratista alternativo.
- Preparación y pruebas de los accesos remotos al sistema de información, para su disponibilidad el día de inicio de la prestación efectiva del servicio.
- Preparación de los entornos necesarios para la prestación adecuada del servicio.

En este sentido, la empresa contratista se tendrá que comprometer a realizar una buena gestión y seguimiento de los servicios objete de este contrato, garantizando la prestación continuada en el tiempo, según los acuerdos de nivel de servicios (ANS) y con entregas de calidad, así como asegurar el traspaso de información (procedimientos de gestión, datos, documentos, etc.) y conocimiento entre contratistas en la fase de transición del servicio.

Sin embargo, y de manera adicional en el texto precedente, los contratistas (el entrante y el saliente) tienen que tener presente que tienen que prestar el servicio con la continuidad y la regularidad que ha acordado el órgano de contratación, según los criterios que figuran en los pliegos, sin otras interrupciones que las que se producirían si la gestión se prestara de forma directa. En caso de extinción normal del contrato, los contratistas tendrán que prestar el servicio hasta que empiece la ejecución del nuevo contrato o, en cualquier caso, hasta que el nuevo contratista se haga cargo, de manera efectiva, de la prestación del servicio (una vez finalizada su implantación y puesta en marcha definitiva), en los plazos que se establecen en el pliego de prescripciones técnicas particulares, sin modificar las restantes prestaciones del contrato, siempre que el anuncio de licitación del nuevo contrato se haya publicado antes de la fecha de finalización del contrato. El nuevo contratista podrá hacerse cargo del servicio de

una manera progresiva o gradual, a medida que vaya concluyendo la implantación y puesta en marcha de los diferentes elementos que conforman, como uno todo, el servicio objeto del contrato.

Cuando haya continuidad de contratista esta tendrá que entregar a la DSTSC una memoria técnica explicativa proponiendo mejoras en la prestación del servicio y en la funcionalidad del sistema objeto del contrato.

11. Transferencia tecnológica y de conocimiento

En relación con los dos lotes en los que está dividido el objeto del contrato, el contratista tiene que tener en cuenta lo siguiente.

El contratista está obligado a facilitar a las personas designadas por la DSTSC toda aquella información necesaria para disponer de un pleno conocimiento técnico de los trabajos realizados.

Sin embargo, el personal designado por la DSTSC a los servicios adjudicados podrá realizar todas aquellas consultas que considere oportunas para el correcto seguimiento y control de los trabajos realizados, como también, recibir, si procede, el traspaso de la información que sea necesaria para conocer y comprender el funcionamiento de los servicios desarrollados.

DILIGENCIA para hacer constar que el texto que antecede es traducción al castellano del Pliego de Prescripciones Técnicas de fecha 31 de mayo de 2021.

En caso de discrepancia entre dicho Pliego de Prescripciones Técnicas, en catalán, y esta traducción al castellano, prevalecerá el primero.

Metadades del document

Núm. expedient	2021/0001954
Tipus documental	Plec de clàusules o condicions
Títol	Pliego de prescripciones técnicas particulares para la contratación de los servicios de Ciberseguridad de los sistemas informáticos de la Diputación de Barcelona. Dividido en 2 lotes
Codi classificació	D0506SE01 - Serveis obert

Signatures

Signatari		**Acte**	**Data acte**
CPISR-1 C Luis Ramirez Pierna	Responsable directiu Servei Promotor	Signa	11/06/2021 12:06

Validació Electrònica del document

Codi (CSV)	**Adreça de validació**	**QR**
8825cfd0afb428a407e5	https://seuelectronica.diba.cat	