PLIEGO DE PRESCRIPCIONES TÉCNICAS DE LA LICITACIÓN:

"SERVICIO DE LA OFICINA TÉCNICA DE SEGURIDAD TIC DE LA APB"

Port de Barcelona

ÍNDICE

1. Objeto y alcance del Pliego

Actualmente la Autoridad Portuaria de Barcelona, en adelante la APB, dispone de un entorno tecnológico cada vez más amplio y complejo, tanto por las nuevas aplicaciones que ya están en producción como por aquellas que se están desarrollando y que estarán disponibles en breve.

Dada la necesidad de proteger a la APB de pérdidas o robos de información y de ataques que impidan el normal funcionamiento de los sistemas informáticos, se hace necesaria la contratación del servicio de la **OFICINA TÉCNICA DE SEGURIDAD TIC (OTS)** y la gestión del servicio relacionado.

1.1. Objeto

El presente pliego de condiciones tiene por objeto fijar las bases para la contratación del servicio de la **OFICINA TÉCNICA DE SEGURIDAD TIC DE LA APB**, en temas relacionados con la seguridad TIC de los sistemas y la protección de datos personales.
La OTS debe ser un instrumento de prevención y de detección de amenazas en la seguridad de los sistemas informáticos de la APB. De igual manera, debe ser el órgano responsable de la definición e implementación de las políticas de seguridad TIC que regirán en la APB.
Los principales objetivos que la APB pretende conseguir con la adjudicación de este pliego son:

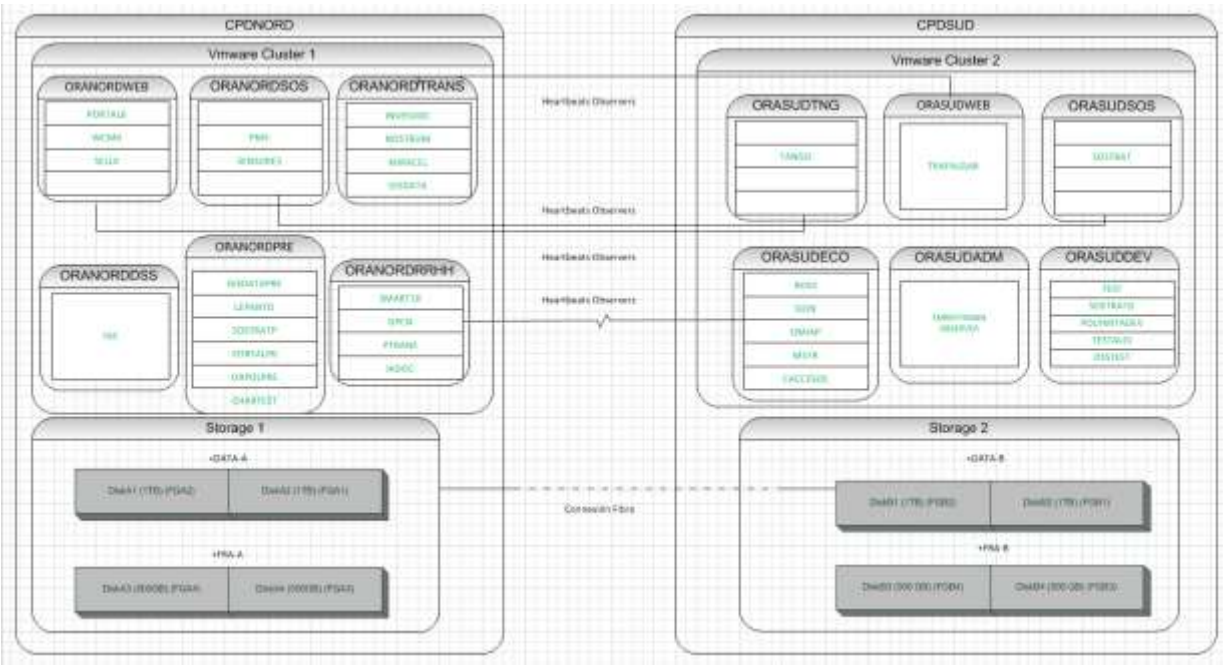
- Definir la estrategia de seguridad TIC de la APB.
- Definir, actualizar y mejorar las políticas en materia de seguridad TIC.
- Perfeccionar las medidas de seguridad TIC existentes en la APB, prestar apoyo al desarrollo de la función TIC y monitorizar el estado de la seguridad TIC en la APB.
- Proporcionar soporte experto en materia de seguridad TIC en los proyectos de desarrollo, mantenimiento y evolución de los sistemas de información que dan servicio a los entornos de la APB mejorando las políticas actualmente definidas en materia de seguridad TIC.
- Dar soporte a posibles auditorías externas y llevar a cabo la comunicación con diferentes organismos.

2. Situación actual

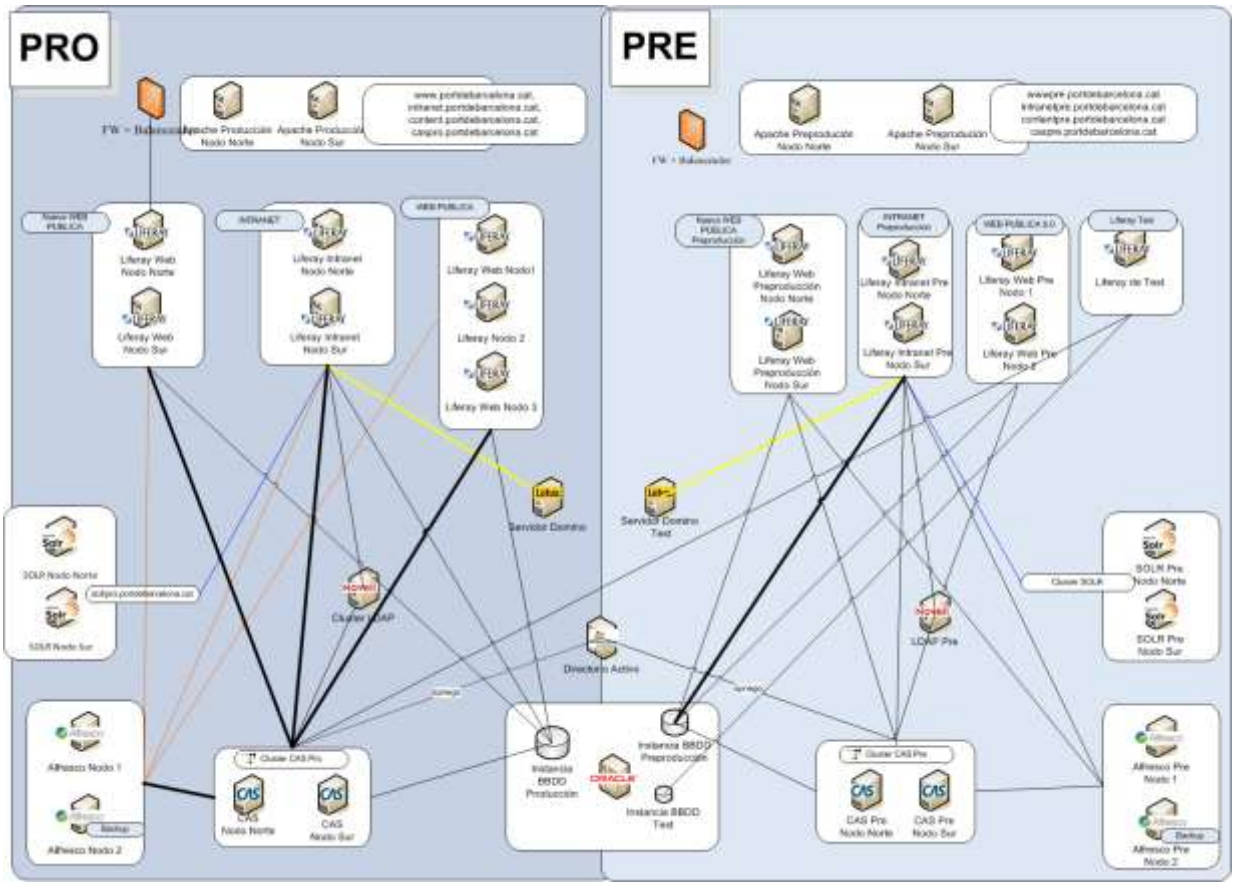
La APB se somete anualmente a una auditoría de seguridad que identifica potenciales vulnerabilidades en las plataformas, controles de seguridad y contramedidas implementadas.

Adicionalmente a las auditorías de seguridad, en abril de 2013, el CESICAT realizó un informe sobre la seguridad de los procesos de la APB y en la actualidad se está desarrollando un Disaster Recovery Plan.

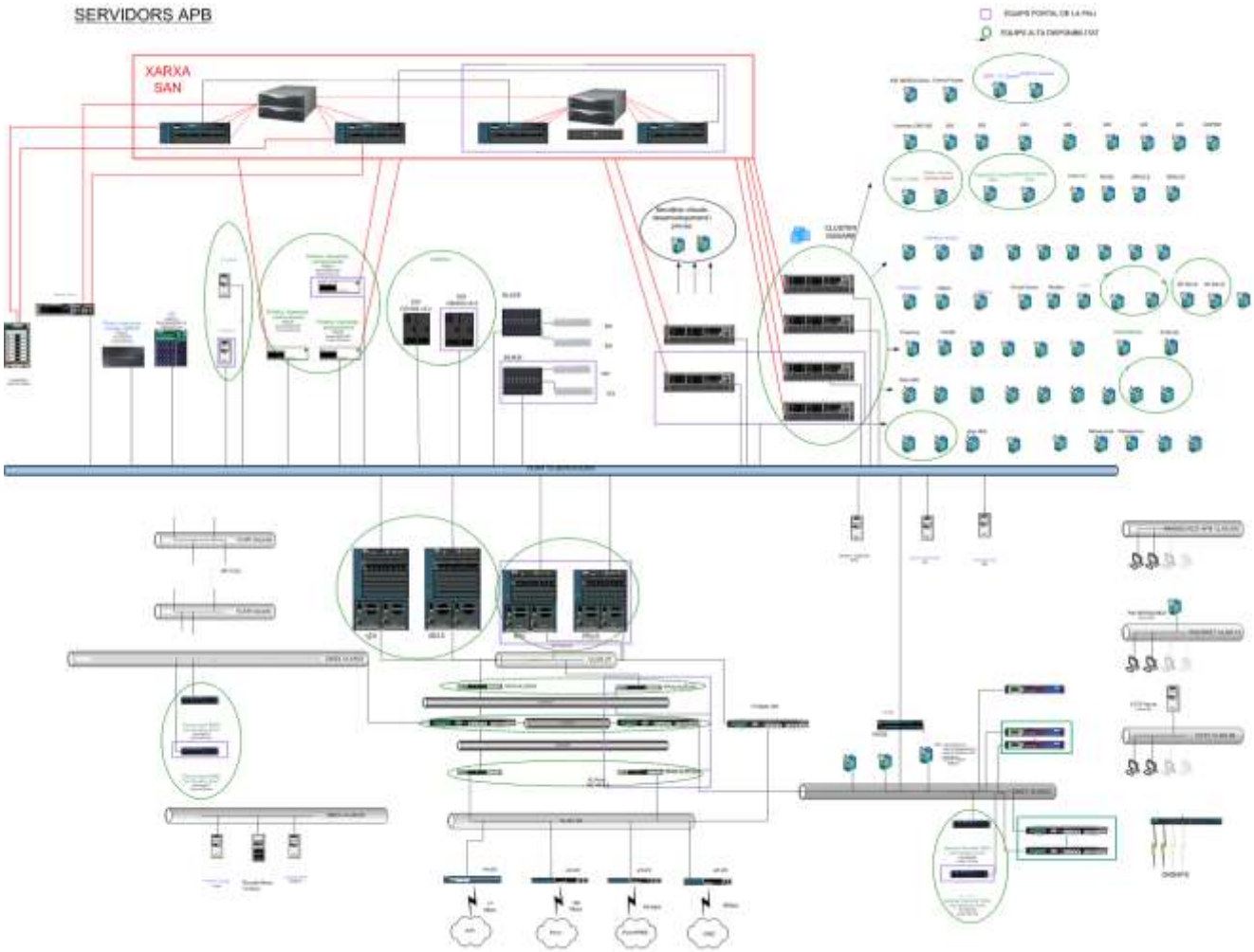
2.1. Repositorio de datos



2.2. Detalle arquitectura



2.3. Servidores de backend



2.4. Auditorías de seguridad anual

La auditoría de seguridad se define como el conjunto de procedimientos y técnicas para evaluar y controlar un sistema informático con el fin de asegurar que sus actividades son correctas y de acuerdo a las normativas existentes en la organización.
Esta se considera de vital importancia para el buen funcionamiento de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean fiables y con un buen nivel de seguridad.
En los últimos años, se han realizado dos auditorías de seguridad en la APB en los años 2011 y 2013. En cada una de ellas se han auditado aspectos diferentes de la seguridad TIC. Concretamente, en la auditoría del año 2011 se evaluaron:

- Arquitectura de red y protección perimetral.
- Control de acceso a la información.
- Plataforma operativa y servicios virtualizados.
- Instancias de BBDD.

En la auditoría realizada en el año 2013, se auditaron:

- Aplicación news.portdebarcelona.cat

- Maqueta de microinformática para Windows 7 utilizada en la APB.
- Correo electrónico corporativo y su integración con los clientes , dispositivos y red interna de la APB.

A continuación se detallan algunas de las recomendaciones emitidas por una consultora externa como resultado de la última auditoría de seguridad TIC realizada en abril de 2013:

- Utilizar una instancia de base de datos independiente para cada aplicación, de modo que si una de ellas se viera comprometida, los datos almacenados por otras aplicaciones no se verán comprometidas -> Medida ejecutada parcialmente
- Realizar una securización de la propia instancia de base de datos -> Medida pendiente de ser ejecutada
- No utilizar usuarios con rol de administrador en los accesos a la base de datos y servidores al exterior -> Medida ejecutada parcialmente
- Separar correctamente privilegios entre aplicaciones, servidores y bases de datos -> Medida ejecutada parcialmente
- No basar la seguridad únicamente en la ofuscación de datos ->Medida pendiente de ser ejecutada

El adjudicatario tendrá acceso a los informes de las auditorías realizadas.

2.5. Requerimientos normativos

2.5.1. Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero, determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos. El ENS está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Será aplicado por las AA.PP. para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestiones en el ejercicio de sus competencias.

Esta normativa es de obligado cumplimiento para la APB.

2.5.1.1. Elementos del Esquema Nacional de Seguridad

Los elementos principales del ENS son los siguientes:

- Los principios básicos a considerar en las decisiones en materia de seguridad TIC.
- Los requisitos mínimos que permitan una protección adecuada de la información.
- El mecanismo para lograr el cumplimiento de los principios básicos y de los requisitos mínimos mediante la adopción de medidas de seguridad TIC proporcionadas a la naturaleza de la información y los servicios a proteger.
- Las comunicaciones electrónicas.
- La auditoría de la seguridad.
- La respuesta ante incidentes de seguridad TIC.
- La certificación de la seguridad TIC.
- La conformidad.

2.5.2. Política de Seguridad de la Información

En el siguiente enlace se encuentra el detalle de la Política de Seguridad de la Información recientemente publicada en el BOE: http://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3482.pdf. Aunque esta política de seguridad no es de obligatorio cumplimiento para la APB, puede servir como marco de referencia.

También ha de servir como referente de aplicación para la APB, aunque en un nivel superior y más genérico, la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

http://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630.

2.6. Informe del CESICAT

En el mes de abril de 2013 el Centre de Seguretat de la Informació de Catalunya (en adelante, CESICAT) realizó un informe del estado de la seguridad TIC de los procesos y requerimientos propios de la APB. A continuación se muestran las iniciativas de mejora de medidas de seguridad TIC que el CESICAT identificó como prioritarias para garantizar el funcionamiento de los procesos críticos de la APB.

1. Procesos Estratégicos
   - 1.1. Planificación General APB
   - 1.2. Organización APB
   - 1.3. Control de Gestión APB
   - 1.4. Comunicación interna y externa
2. Procesos de Negocio
   - 2.1. Procesos Comerciales
     - 2.1.1. Planificación márqueting operativo
     - 2.1.2. Desarrollo de Negocio
     - 2.1.3. Promoción y comercialización
     - 2.1.4. Atención al cliente
   - 2.2. Procesos Operativos
     - 2.2.1. Planificación, construcción y gestión del territorio
       - 2.2.1.1. Planificación operativa
       - 2.2.1.2. Infraestructura y conservación
       - 2.2.1.3. Explotación y gestión del territorio
     - 2.2.2. Gestión de servicios portuarios
       - 2.2.2.1. Gestión de Servicios Directos
       - 2.2.2.2. Regulación y control de los Servicios autorizados y concesionados
       - 2.2.2.3. Coordinación mesura de la eficiencia y liderazgo de la mejora de los Procesos portuarios
       - 2.2.2.4. Facturación
     - 2.2.3. Gestión de la seguridad y el medio ambiente
3. Procesos de Soporte
   - 3.1. Gestión económico-financiera
   - 3.2. Auditoria interna
   - 3.3. Consultoría organización
   - 3.4. Gestión de Sistemas de Información
   - 3.5. Gestión de Persones
   - 3.6. Gestión de Servicios Generales
   - 3.7. Asesoría Jurídica

2.7. Disaster Recovery Plan

En la actualidad se está confeccionando un Disaster Recovery Plan (DRP) que incluye:

- Una secuencia general de arranque de los sistemas siguiendo un orden establecido en las diferentes capas de arquitectura.
- Secuencias de arranque para las diferentes aplicaciones de negocio, que deberán estar referenciadas a documentos de explotación.
- Secuencia de pruebas de las diferentes aplicaciones de negocio, que ayude a verificar el correcto funcionamiento.
- Definición de equipos de actuación para cada uno de los sistemas / servicios y listado de proveedores de servicio incluyendo SLAs.
- Estrategia de continuidad de los sistemas de la APB en la que se identifiquen los diferentes escenarios de indisponibilidad y el plan para su recuperación.

A continuación se muestra el listado de procedimientos de operación de las infraestructuras básicas objeto del DRP:

Infraestructura	Arquitectura	Procedimientos técnicos
Infraestructura básica	Red de switching/routing interno	Switches de interconexión entre Data Center, edificios, plantas, wifi
	Comunicación externa	Routers Perimetral
		Líneas de comunicación
		Firewalls
		Servicio DNS
		Fortimail
		Balanceadores de carga
	Telefonía	Servicios de Telefonía
	Red SAN y sistemas de Backup	Red SAN
		Cabinas de disco BULL
		Cabinas disco HITACHI
		Sistema de Backup
	Entornos virtualizados	Host VMWare para virtualización servidores
		Host VMWare para virtualización Escritorios Virtuales
	Entornos no virtualizados	AS400
		Otros servidores físicos
	BBDD	Plataforma Oracle
		Plataforma SQL Server
	File Servers	Servicio ficheros, ¿ALFRESCO?
	Entornos de validación	Active Directory, LDAP y CAS

3. Alcance del servicio

El alcance del servicio estará basado en tres pilares: la realización de una auditoría y consultoría inicial, la provisión de servicios recurrentes, y servicios o proyectos a demanda, que se llevaran a cabo durante el periodo de vigencia de este contrato.

3.1. Auditoría y consultoría inicial

En esta fase de como máximo 2 meses de duración que se inicia inmediatamente después de la adjudicación y contratación, el adjudicatario deberá reunir toda la información necesaria para la correcta prestación del servicio. El fin de esta fase supondrá el inicio de la oficina técnica de seguridad.

El adjudicatario del servicio deberá realizar una auditoría del estado de la seguridad TIC de la APB y proponer acciones de mejora basadas en esa auditoría. Además deberá actualizar el informe del estado de seguridad TIC realizado por el CESICAT, descrito en el apartado 2.6 del presente pliego.

En la auditoría inicial se cubrirán como mínimo las siguientes tareas:

- Determinación de las necesidades de protección de la APB.
- Adquisición del conocimiento pleno de la infraestructura de la APB.
- Identificación de las amenazas.
- Valoración del riesgo.
- Valoración del estado actual de seguridad.

El adjudicatario del presente pliego deberá proveer a la APB del soporte necesario en materia de seguridad TIC, realizando todas aquellas actuaciones de prevención y resolución que se requieran debidas a:

- Actualización del plan director de seguridad TIC de la APB.
- Definición, implantación y evolución de las políticas de seguridad TIC.
- Iniciativas de seguridad TIC formuladas por la OTS en consenso con la APB o directamente identificadas por la propia APB.
- Adaptación al marco regulatorio vigente.

Todas aquellas actividades que puedan ser llevadas a cabo en paralelo debido a la ausencia de dependencias entre ellas, deberán hacerse simultáneamente.

3.2. Servicios recurrentes de la OTS

Los servicios mínimos requeridos son los que se detallan a continuación. Estos servicios supondrán un coste fijo mensual, puesto que se deben proporcionar de manera constante a lo largo de la duración del contrato.

3.2.1. Servicio de monitorización

Este servicio se centra en la ejecución de actividades relacionadas con servicios SOC (Centro de Operaciones de Seguridad). El SOC se activará justo después de la auditoría inicial y gestionará y administrará las vulnerabilidades y amenazas de una forma proactiva y reactiva, mediante la monitorización de las redes de comunicación y equipos que albergan los sistemas informáticos, así como el acceso a los datos de la APB. Igualmente ofrecerá asesoría y planteará opciones innovadoras para llevar un control de las comunicaciones y detección de vulnerabilidades, con el objetivo de que no se vea afectado el servicio en los sistemas de información, tanto desde el interior de la red de la APB como desde el exterior.

Las actividades mínimas incluidas en el servicio de monitorización son:

- Monitorización del estado de la seguridad TIC:
    - Monitorización de la infraestructura.

  - Cumplimiento de las políticas de seguridad TIC.
  - Detección y Gestión de vulnerabilidades.
  - Alerta temprana ofrecido a través de la red social interna o por otros medios.
- Gestión de logs.
- Instalación de sondas, correlación de eventos de seguridad TIC y generación de alertas.
- Análisis de vulnerabilidades.
- Consultoría y asesoría en seguridad TIC.
- Respuesta a incidencias de seguridad TIC.
- Identificación de gaps de seguridad del software.

Actualmente, la APB no dispone de un SIEM (Security Information and Event Management). El adjudicatario deberá proponer el uso de un SIEM, preferiblemente en formato SaaS, ayudará en la puesta en producción del SIEM y se responsabilizará de la administración del mismo. Con la implantación de un SIEM, la APB pretende disponer de:

- una plataforma de monitorización junto con los dispositivos y equipos necesarios para su funcionamiento, licencias y servicios para su administración y mantenimiento
- una consola única que permita definir políticas y métricas de riesgo
- un interfaz de alto nivel con posibilidad de obtener informes de seguridad y gestionar incidencias
- una plataforma que pueda recibir eventos de dispositivos comerciales y de aplicativos desarrollados a medida, adaptándose a sus características
- una arquitectura en alta disponibilidad y tolerante a fallos que incluya los siguientes elementos: sensores recolectores, servidor de gestión, base de datos y consola web
- módulos y elementos de hardware y software necesarios para su funcionamiento (correlación de logs, etc.), con al menos las siguientes funcionalidades:
  - IDS, o sistema de detección de intrusos
  - Detección de anomalías
  - Escáner de vulnerabilidades
  - Monitor de uso de la red
  - Monitor de disponibilidad de servicios
  - Sistema de inventariado automático
  - Detector de ataques de nivel 2
  - Analizador forense

Todos los servicios recurrentes tanto del SOC como del SOC con SIEM se pagarán desde el momento en que estén operativos. Concretamente, el pago del SOC se iniciará posteriormente a la auditoría inicial y el pago del SOC con SIEM a partir del momento en que se instale el SIEM.

3.2.2. Servicio de gestión de incidencias de seguridad

Proceso responsable de registrar todas las incidencias que afecten a la calidad del servicio y restaurarlo a los niveles acordados de calidad en el más breve plazo posible.
El adjudicatario deberá gestionar cualquier incidencia que cause o pueda causar una interrupción del servicio, en el mínimo tiempo posible, consiguiendo soluciones perdurables y estables en el tiempo.

La gestión de incidencias incluye:

- Registro, clasificación y notificación de incidentes de seguridad TIC
- Primer nivel de resolución de las incidencias de seguridad TIC reportadas por el servicio de Service Desk de la APB o por el área de Sistemas de Información
- Escalado de las incidencias a los fabricantes en el caso de no poder alcanzar una solución de las mismas, según normativas.
- Seguimiento de la incidencia en caso de escalado.

- Documentación de la incidencia a través de todo su ciclo de vida hasta su resolución definitiva.

- El adjudicatario del servicio tendrá acceso a las herramientas de monitorización y Service Desk propias de la APB, pero podrá utilizar además sus propias herramientas si lo considera necesario. A ser posible se deberá utilizar la herramienta estándar de ticketing de la APB (Proactivanet).

Las actuaciones a realizar ante una incidencia de seguridad TIC recibida dependerán de su tipología:

- En caso que la incidencia no requiera intervención del servicio de mantenimiento (fabricantes o proveedores de los equipos), será resuelta directamente por los recursos técnicos de gestión y administración, mediante el acceso in-situ o remoto a los sistemas.
- En el resto de casos se activarán los procedimientos de gestión de la resolución de incidencias con los servicios de mantenimiento correspondientes (fabricantes o proveedores de los equipos), manteniendo un constante registro del estado de las incidencias abiertas. El adjudicatario del servicio mantendrá una comunicación continua con los responsables de los sistemas para garantizar la resolución de las incidencias en el menor tiempo posible. En caso que sea necesario se pondrá en contacto directamente con el fabricante del sistema. Dentro de la responsabilidad del adjudicatario del servicio está la Gestión de Proveedores que se describe más adelante en este pliego.

Se requiere que el adjudicatario del servicio realice un análisis a posteriori de las incidencias de seguridad TIC producidas con el fin de detectar las posibles causas de las mismas.
El adjudicatario del servicio propondrá de manera proactiva acciones de mejora, destinadas a resolver posibles deficiencias detectadas, que disminuyan las incidencias producidas y evitar que se conviertan en problemas.
A modo de ejemplo, se considerará como mínimo el siguiente catálogo de incidencias de seguridad TIC:

- Accesos o intento de accesos no autorizados.
- Código malicioso.
- Denegación de servicio.
- Mal uso de los recursos informáticos de la APB

3.2.3. Servicio de gestión de peticiones de seguridad

Proceso responsable de registrar todas las peticiones de seguridad que afecten a la calidad del servicio y restaurarlo a los niveles acordados de calidad en el más breve plazo posible.
La gestión de peticiones incluye:

- Registro, clasificación y notificación de peticiones de seguridad TIC
- Evaluación y/o análisis las peticiones de cambios o propuestas de mejora.
- Aportación del conocimiento técnico del área que permita mejorar la prestación del servicio desde una perspectiva de mejora continua.
- Documentación de la petición a través de todo su ciclo de vida hasta su implantación definitiva
- A ser posible se deberá utilizar la herramienta estándar de ticketing de la APB (Proactivanet).

3.2.4. Gestión del servicio

Además de los servicios indicados en los puntos anteriores, se realizarán las siguientes tareas:

- Análisis de activos y de riesgos periódicos, que permitan identificar riesgos relevantes y medidas de seguridad TIC implementadas para reducirlos.

- Mantenimiento de un cuadro de mando integral de seguridad TIC que el adjudicatario elabore y consensue con la APB.
- Validación de requisitos de seguridad TIC en sistemas en producción y en sistemas de nueva creación, colaborando en su ciclo de vida completo.
- Valoración de las diferentes peticiones de seguridad que realice la APB.

El contenido de los servicios y, en general, de las prestaciones requeridas, se podrá modificar, siguiendo el procedimiento previsto en el presente pliego, para su adecuación a los cambios normativos y estructurales, que se produzcan con posterioridad a la adjudicación del contrato, siempre que la modificación guarde relación con el objeto del contrato y no suponga mayor coste para el adjudicatario.

3.3. Servicios a demanda para la OTS

Línea variable de servicios y/o proyectos, que se corresponderá a actuaciones a demanda, estas no se conocen de antemano, y variarán en función de las necesidades de la APB durante la duración del contrato, o en función de las propuestas de mejora que realice el adjudicatario de este servicio. La facturación de esta línea variable se efectuará contra la bolsa de horas dedicada a este finalidad.

Los servicios serán prestados por personal con un perfil de consultor similar a cualquiera de los incluidos en el equipo mínimo de prestación del servicio (detallado más adelante en este pliego), dependiendo de la prestación a realizar en cada caso concreto y con experiencia en las materias demandadas.

Algunos de los servicios que pertenecen a este ámbito serían:

- Auditorías de seguridad.
- Servicio de formación en seguridad
- Elaboración de normativas, políticas y procedimientos internos de seguridad TIC.
- Análisis forense de determinadas incidencias de seguridad TIC, por ejemplo tras un ataque de DoS.
- Asesoría y consultoría en protección de datos de carácter personal.
- Soporte en posibles procesos sancionadores.
- Consultoría y soporte en administración electrónica.
- Soporte puntual a la gestión de identidades.
- Actuaciones sobre los sistemas en los que se detecten alertas de seguridad en los sistemas de la APB.
- Proyecto de implementación de un SIEM. El SIEM implantado podrá ser una herramienta de mercado o bien propia del adjudicatario.

3.3.1. Bolsa de horas para los servicios a demanda

La APB contratará una bolsa de horas para llevar a cabo los servicios bajo demanda. Toda necesidad de servicio bajo demanda, será gestionada como un proyecto.

Todos los trabajos que se facturen contra la bolsa de horas deberán seguir los siguientes pasos:

- Deberán tener su origen en una petición de proyecto.
- El adjudicatario deberá realizar 2 valoraciones del trabajo:
    - Valoración de carga de trabajo (horas que facturará contra la bolsa de horas).
    - Tiempo de ejecución y puesta en producción del trabajo. En este caso aplicaran los SLA establecidos (Planificación de peticiones), o bien la planificación propuesta por

el adjudicatario si este considera que no aplica el SLA, en este caso deberá contar con la aprobación de la APB.

- El adjudicatario deberá contar con la validación por parte de la APB tanto de la carga de trabajo como de la planificación.
- Todos los trabajos deberán quedar reflejados en el control de cambios (Bitácora Excel, wiki,etc.) al finalizar su ejecución, independiente del entorno (preproducción, producción), y contar con su correspondiente documentación.
- Sin el cumplimiento de estos requisitos los trabajos no serán facturables.

Todas las tareas del servicio de monitorización, del servicio de gestión de incidencias de seguridad, del servicio de gestión de peticiones de seguridad, y la propia gestión del servicio, van contra el coste fijo del servicio.

3.3.2. Servicio de auditorías de seguridad

El objetivo de este servicio es garantizar el correcto grado de madurez de la seguridad TIC de los sistemas de la APB, de manera que se garantice la continuidad del servicio y se minimicen los riesgos como perdida de datos o confidencialidad. Este proceso se basa en la realización de una auditoría con una frecuencia anual cuya duración será de un máximo de 2 meses cada una.

Las actividades propias de este servicio son:

- Auditorías de controles generales de Tl.
- Auditorías de seguridad de la infraestructura.
- Auditorías de vulnerabilidades del software.

El adjudicatario deberá especificar que dedicación por parte de personal de la APB se requiere.

3.3.3. Servicio de formación en seguridad

El servicio que se presta está orientado a la concienciación y formación de usuarios y el departamento de sistemas en materia de seguridad de la información, y a la correcta comprensión de la legislación y normativa que aplicable a la APB por el tipo de información que maneja.

Comprende actividades tales como:

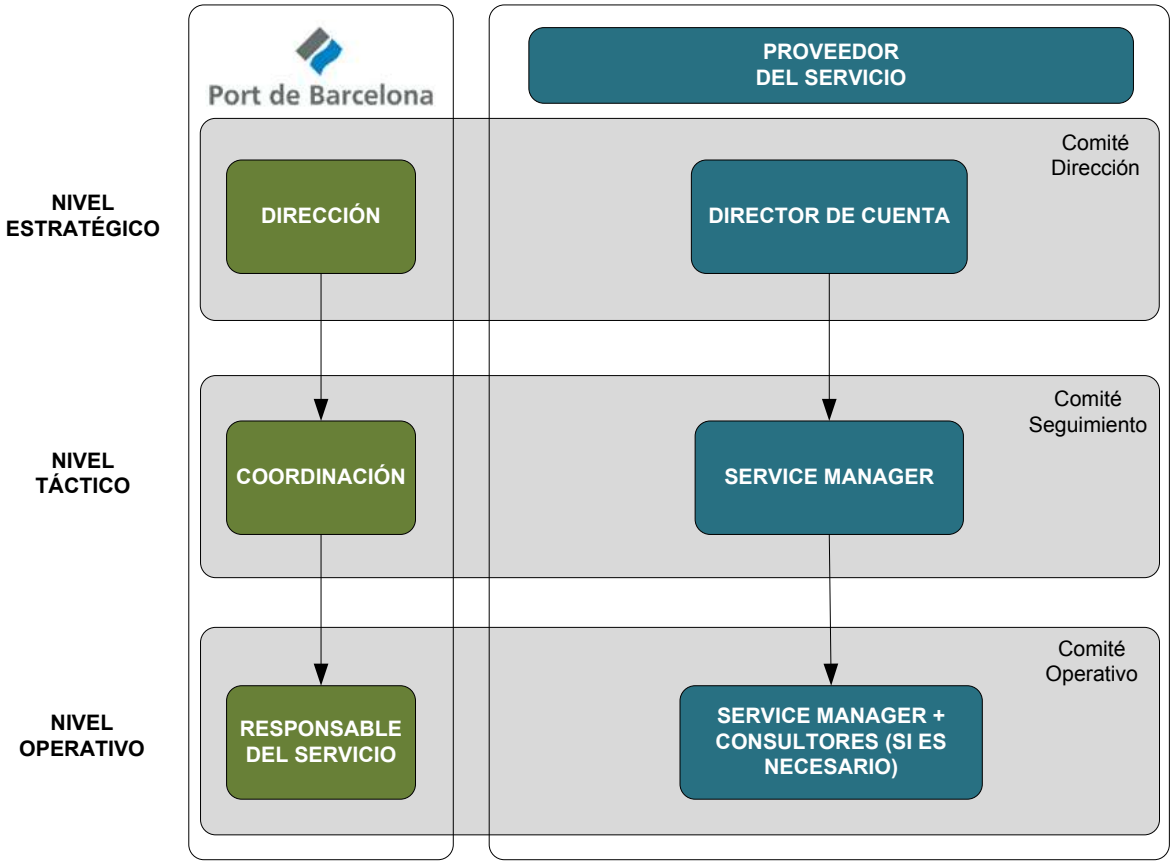
- Desarrollo de material de formación relacionado con la seguridad de la información, legislación y normativa relacionada.
- Convocatoria de sesiones formativas.
- Coordinación con departamentos internos.
- Formación en las aplicaciones que se puedan desarrollar como consecuencia de este pliego.
- Impartir cursos sobre:
    - Seguridad de la información.
    - Normativa: LOPD, ENS, etc.
    - Estándares y códigos de buenas prácticas: ISO 27000, lTlL, etc.

Se considera que 100h/año estarán de dedicadas a formación.

4. Definición de los requisitos del servicio

4.1. Modelo de relación

La APB desea establecer un sistema de comunicación y relación con el adjudicatario a distintos niveles que asegure el correcto seguimiento del servicio. En él se establecen los diferentes niveles y sus periodicidades, tareas y responsabilidades que cada actor debe asumir para el correcto funcionamiento del modelo.
Este sistema se fundamenta en un Modelo de Relación de tres niveles y con los comités que se detallan a continuación:



Comité de Dirección	APB	Adjudicatario
Interlocutores	• Directora de sistemas • Coordinador del servicio	• Director de cuenta • Service Manager
Frecuencia	• 2 veces al año. • A demanda de la APB.	
Objeto y propósito principal del comité	• Aspectos estratégicos del servicio (ampliaciones, reorientación del servicio, riesgos, ...). • Renovación anual del contrato de servicio (cuando aplique).	

Comité de Dirección	APB	Adjudicatario
Documentación asociada	• Informes ejecutivos de progreso del servicio. • Agenda y acta de la reunión	

Comité Seguimiento	APB	Adjudicatario
Interlocutores	• Coordinador del servicio • Responsable del servicio	• Service Manager
Frecuencia	• Trimestral	
Objeto y propósito principal del comité	• Revisión informes de control. • Incumplimientos y acciones correctoras. • Revisión de riesgos y acciones correctoras. • Revisión progreso mejora continua del servicio.	
Documentación asociada	• Informe de control y seguimiento. • Informe de SLAs. • Registro de riesgos. • Agendas y actas de reunión.	

Comité Operativo	APB	Adjudicatario
Interlocutores	• Responsable del servicio	• Service Manager • Consultores
Frecuencia	• Mensual	
Objeto y propósito principal del comité	• Definición de las políticas de seguridad TIC. • Realización de auditorías. • Evaluación de riesgos. • Analizar propuestas de mejora.	
Documentación asociada	• Informes de auditoría. • Agenda y acta de la reunión.	

Otras posibles reuniones:

- Coordinación con proveedores que presten servicios actualmente a la APB.
- Comité de cambios con afectación en los servicios (cambios de alcance).
- Reuniones a demanda según situación del servicio.

4.2. Equipo de trabajo

4.2.1. Equipo presencial

El equipo de trabajo presencial estará formado, como mínimo, por:

- Un Service Manager como responsable global del servicio y con conocimiento y experiencia como consultor de seguridad. Es la persona que deberá poner en marcha la OTS, adquirir el conocimiento de la arquitectura, analizar la seguridad de la APB y proponer los proyectos necesarios. Se estima que esta persona deberá tener una dedicación de 5 horas semanales.
- Consultores Sénior especialistas en diferentes áreas de seguridad, software, seguridad TIC del código, bastionado de sistemas, gestión y correlación de logs, LOPD, ISO, hacking ético, no necesariamente de manera simultánea. Se estima una dedicación de 8 horas semanales.

4.2.2. Equipo remoto

Además del equipo que prestará el servicio presencial, el adjudicatario deberá garantizar la monitorización y el escalado de incidencias propias de la red de la APB ante ataques externos en horario de 24 horas, por un grupo específico y especializado que prestará sus servicios de manera remota desde el Centro de Operaciones de Seguridad del adjudicatario (SOC) o de forma presencial si así fuera requerido por la APB. Este equipo deberá ser dimensionado por el adjudicatario en base a la información suministrada en el pliego así como a su experiencia por el tipo de actividades a realizar.

4.2.3. Sustitución de miembros del equipo

La APB valorará si el servicio se cumple adecuadamente o no y en su caso propondrá la sustitución de alguna persona del equipo en caso de que no se preste adecuadamente el servicio.

Esta exigencia se materializará por escrito al adjudicatario del servicio, aunque la relación habitual cliente / proveedor presupone que existen otros canales de comunicación más directos por los que obtendrá un preaviso (teléfono, e-mail, etc.).

El adjudicatario del servicio no podrá alterar la composición de los medios humanos sin autorización escrita de la Dirección de Sistemas de Información del APB, en respuesta a una petición motivada por parte del adjudicatario del servicio.

En cualquiera de las dos situaciones, se considerará que el nuevo recurso asignado necesitará 120 horas para adquirir los conocimientos de las aplicaciones y sistemas en las que tiene que trabajar. Estas horas no podrán ser facturadas dado que no son productivas, interrumpen la planificación, alargando los plazos previstos, y dado que la APB ya ha pagado esta adquisición de conocimientos al recurso humano asignado inicialmente por el adjudicatario del servicio.

4.3. Requisitos de Nivel de Servicio

Se definen los siguientes impactos para las incidencias, peticiones, cambios y problemas:

- **Impacto 1 (Crítico):** parada total de un sistema o equipo o pérdida de funcionalidad con afectación grave al negocio de la APB. También se considerarán de Impacto 1 todas aquellas incidencias que afecten a un porcentaje de usuarios igual o superior al 10%.
- **Impacto 2 (Alto):** degradación o pérdida parcial de la funcionalidad con un efecto moderado en el negocio de la APB.
- **Impacto 3 (Media/Baja):** incidencia leve, con bajo impacto en el negocio de la APB.

4.3.1. Tiempo de respuesta frente a incidencias

El tiempo de Respuesta frente a Incidencias se define como el tiempo entre que la Incidencia es abierta en el Service Desk de la APB y el inicio del análisis por un técnico especializado. Se medirá mensualmente.

Nivel de cumplimiento es el % de veces que van a cumplir los tiempos especificados en la tabla. P.ej. si en 1 mes en 4 incidencias de impacto crítico en entorno de producción se resuelven todas en menos de 15 min, nivel de cumplimiento 100%.

IMPACTO	PRODUCTIVO	NO PRODUCTIVO	NIVEL CUMPLIMIENTO
1	15 minutos	60 minutos	99%
2	45 minutos	120 minutos	97%
3	90 minutos	240 minutos	95%

4.3.2. Tiempo de resolución frente a incidencias

El tiempo de Resolución frente a Incidencias se define como el tiempo entre que la Incidencia es detectada mediante sondas, alarmas o bien informada por el usuario afectado y esta ha sido resuelta con plena capacidad operativa del elemento afectado. Se medirá mensualmente.

IMPACTO	PRODUCTIVO	NO PRODUCTIVO	NIVEL CUMPLIMIENTO
1	2 horas	4 horas	99%
2	6 horas	12 horas	98%
3	16 horas	24 horas	95%

4.3.3. Planificación de Peticiones

El contenido y prioridad de las peticiones que sean predefinidas, tendrán una documentación asociada, que deberá ser detallada por el adjudicatario. A estas se deberán asociar los Niveles de Servicio:

Planificación de la intervención, tiempo máximo que se tardará el adjudicatario en entregar la planificación para una petición realizada por la APB.

Los niveles de servicio para la Gestión de Peticiones son:

PRIORIDAD	COMPLEJIDAD	PLANIFICACIÓN DE LA INTERVENCIÓN
Urgente / Casos Especiales	Cualquiera	Inmediata
Alta		1d
Media		3d
Baja		5d

Para el resto de peticiones que no tengan una prioridad predefinida, el adjudicatario del servicio fijará un determinado nivel de servicio al que se deberá comprometer. Se medirán mensualmente.

ELEMENTO	INDICADOR DE SERVICIO	MÉTRICA	% MÍNIMO DE CASOS
Respuesta a la Petición	Tiempo de Respuesta	< 2 días hábiles	90%
	Con concepto de imputación, requisitos y planificación	< 5 días hábiles	100%
Modificaciones planificadas	Cumplimiento / Desviación en el plazo de entrega y puesta en marcha y	Fecha Entrega = Fecha Planificado	80%

	contado desde la fecha de registro de la petición	Desviación (días) < 20% del Planificado	100%
Defectos	Modificaciones, cambios, mejoras entregadas. No producirán errores	Cero defectos (no producirán errores)	95%

4.3.4. Gestión del servicio

ELEMENTO	INDICADOR DE SERVICIO	MÉTRICA	VENTANA DE MEDICIÓN
Gestión del Servicio	Rotación de personal	<= 2 personas	Duración contrato
	Período de Traspaso de conocimiento en caso de sustitución de alguno de los consultores de seguridad	>= 120h	Duración contrato
	Número de reuniones de Gestión de servicio establecidas en el modelo de relación convocadas y no realizadas por motivos atribuibles al adjudicatario. Se medirán los retrasos producidos y se sumarán.	Desviación de las reuniones respecto a lo previsto < 20%	Trimestralmente
	Número de reuniones de Gestión de servicio establecidas en el modelo de relación no realizadas en plazo por motivos atribuibles al adjudicatario. Se medirán los retrasos producidos y se sumarán.	Desviación de las reuniones respecto a lo previsto < 20%	Trimestralmente

4.3.5. Obligaciones del adjudicatario en materia de seguridad

El adjudicatario deberá garantizar la seguridad, disponibilidad, confidencialidad e integridad de los sistemas a gestionar y mantener, mediante el cumplimiento de las siguientes normas básicas:

- Cumplimiento de los estándares y políticas de seguridad TIC de la APB.
- Garantizar la confidencialidad, integridad y disponibilidad de la información almacenada y transmitida.
- Informar a la APB sobre su política de seguridad TIC, así como de la implementación y seguimiento por parte de su organización.
- Informar por escrito a la APB tan pronto con se detecten riesgos reales o potenciales de seguridad en el equipamiento.
- Acceso a cualquier equipo mediante un control de acceso lógico, garantizando la restricción a los usuarios autorizados.
- Garantizar la estricta aplicación de las normas de seguridad por parte de su personal.
- Ejecutar todas las actuaciones siguiendo procedimientos escritos que contemplen las normas de seguridad.

4.3.6. Documentación

4.3.6.1. DOCUMENTACIÓN PARA EL SERVICIO RECURRENTE

El adjudicatario proporcionará a la APB los informes siguientes:

Documento	Periodicidad
Registro de incidencias	Mensual
Registro de peticiones	Mensual
Registro de riesgos y vulnerabilidades	Mensual
Cuadro de mando del servicio recurrente	Mensual

4.3.6.2. DOCUMENTACIÓN REFERENTE A PROYECTOS

El adjudicatario proporcionará a la APB los informes siguientes:

Documento	Periodicidad
Informes auditoría	Mensual
Proyectos en curso	Quincenal
Cuadro de mando del servicio a demanda	Mensual

4.3.6.3. DOCUMENTACIÓN REFERENTE AL SERVICIO

El adjudicatario deberá explicitar en su oferta el contenido de cada uno de estos documentos así como de cualquier otro que presente y que no esté en esta lista.
Adicionalmente presentará los informes periódicos del estado de los servicios objeto de esta licitación, en el formato que se acuerde con la APB. Como mínimo, los informes que se deberán presentar serán:

Documento	Periodicidad
Memoria del servicio	Anual
Informe de cumplimiento de SLAs	Mensual
Informe de control y seguimiento	Mensual
Cuadro de mando de estado del servicio	Mensual
Agenda y acta de reunión	En función de la periodicidad de la reunión (como máximo 3 días después de la reunión)

Estos documentos deberán ser presentados en el formato que especifique la APB.

4.4. Condiciones para la prestación del servicio

Se describen a continuación diversas normas, prácticas de uso, que son de aplicación común al servicio de la oficina técnica de seguridad TIC.

4.4.1. Horario y lugar de trabajo

El horario de prestación del servicio del equipo presencial será de 9 a 18 horas en las dependencias de la APB para las actuaciones que la APB determine deban ser realizadas presencialmente. Los servicios del equipo de monitorización serán prestados en horario de 24x7.

Si por cualquier razón (por ejemplo una incidencia de seguridad) fuera necesario realizar trabajos por parte del equipo presencial fuera del horario habitual, en sábados o festivos, o en régimen de nocturnidad, o bien de manera presencial por parte del equipo remoto (SOC), la APB no aceptará ningún coste adicional provocado por la situación que correrá siempre a cargo del adjudicatario.

El adjudicatario deberá en todo momento poder garantizar los recursos humanos que satisfagan la demanda de requerimientos que se tenga durante la vigencia del contrato. Los medios de trabajo necesarios para el personal adscrito a la prestación del servicio, tales como, ordenadores, teléfonos móviles, tablets, licencias software de cualquier tipo, etc., correrán a cargo de la empresa adjudicataria. En particular, y dado que los servicios de la OTS a los que da cobertura este pliego necesitan una disponibilidad o localización en horario de 24x7, el adjudicatario debe proveer a su personal de teléfonos móviles para su localización inmediata fuera del horario de oficina presencial.

Servicio	Horario
Prestación del Servicio presencial	8 x 5
Prestación del Servicio remoto	24 x 7

Notas:

- Horario Prestación del Servicio presencial: dos días a la semana, 8 horas, entre las 08:00h y las 18:00h.
- Deberá mantenerse la cobertura y el nivel de servicio durante los festivos locales o autonómicos de las localidades de centros de operación del APB.

El lugar de prestación del servicio presencial será las oficinas de la APB en el edificio Est del World Trade Center de Barcelona.

4.4.2. Calidad

La APB se reserva el derecho de realizar o contratar tantas auditorias como considere necesarias notificando al adjudicatario del servicio con un mínimo de dos días de antelación. El adjudicatario deberá autorizar el acceso necesario a los Sistemas, entornos TIC y Aplicaciones, objeto de este pliego.

En el caso que las auditorias se apliquen para dirimir un incumplimiento, el adjudicatario deberá asumir los costes de la auditoria.

4.4.3. Formación continua

El servicio debe contemplar un plan de formación continuada para todos los recursos implicados en el servicio.

- Formación en los productos y tecnologías implantadas en la APB.
- Formación en los productos y tecnologías que la APB considere necesarias para la correcta realización del servicio.
- Formación necesaria para garantizar la continuidad del servicio en caso de substitución temporal o definitiva del recurso.
- Formación en las aplicaciones que se puedan desarrollar como consecuencia de este pliego.

4.4.4. Gestión de Proveedores

La coordinación con Proveedores será responsabilidad del adjudicatario del servicio. Las siguientes tareas se consideran dentro del ámbito de esta Gestión de Proveedores:

- Escalado y soporte a las incidencias de seguridad TIC, peticiones, consultas y cambios así como la comunicación con proveedores de servicios de la APB y responsables de la APB.
- Seguimiento de los casos abiertos al fabricante.
- Soporte técnico y funcional a proveedores que desarrollen proyectos, adapten soluciones, aplicaciones y sistemas para la APB, aportando su conocimiento de los entornos productivos de la APB y de las arquitecturas implantadas asociadas a éstos.
- Coordinación con proveedores en las implantaciones de los sistemas y aplicaciones que desarrollen éstos.

Se consensuará con la APB el procedimiento de gestión de incidencias a seguir en la interlocución con los proveedores que la APB tenga contratados.

4.4.5. Documentación de los trabajos

Toda la documentación se entregará en soporte magnético editable para facilitar su mantenimiento posterior y reproducción.

Se utilizarán los formularios proporcionados por la APB (modificables en el tiempo), y con el nivel de detalle adecuado, se proporcionarán ejemplos de buenas prácticas. Todo este material se proporcionará al adjudicatario al inicio del proyecto.

Se utilizarán los repositorios de datos y herramientas destinadas a tal efecto en la APB

4.4.6. Propiedad de la documentación y el software

El adjudicatario está obligado a guardar secreto respeto los datos o información previa que no siendo públicos o notorios estén relacionados con el objeto del contrato. En cuanto a la propiedad, toda la documentación que se genere a lo largo del servicio es propiedad de la APB. El adjudicatario no la podrá utilizar para otras finalidades sin el consentimiento expreso de la APB.

4.4.7. Confidencialidad

El adjudicatario de los servicios se compromete a cumplir los requerimientos de seguridad y continuidad aplicables al objeto del contrato especificados a:

La legislación vigente en general y, en particular, cuando se traten datos de carácter personal, el Reglamento de Seguridad del Real Decreto 994/1999 de la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD).

Las normas ISO/IEC/UNE 17799 de mejores prácticas de seguridad de la información y UNE71502 de Gestión de la seguridad de la información, adaptadas en la estructura administrativa, personal y entorno tecnológico del cliente y aplicadas de forma proporcional a los riesgos reales.

Los requerimientos de seguridad de webs que publique el IQUA (Agencia de Calidad de Internet).

4.5. Plan de devolución del servicio

Se desarrollarán las pautas por las cuales el adjudicatario estará obligado, a petición de APB o por incumplimiento, a devolver el control total o parcial del servicio contratado. Los servicios a prestar durante esta fase estarán incluidos en el precio del servicio de este pliego. El adjudicatario se obliga a realizar un retorno del servicio asumiendo el esfuerzo que pueda representar esta actividad y considerando como objetivo básico de esta fase la transferencia ordenada de los servicios y activos a la APB (o un tercer proveedor) con el menor impacto posible en el usuario.

El adjudicatario debe presentar un Proyecto de Devolución del servicio describiendo:

- Descripción detallada del estado de la seguridad.
- Período de ejecución del Proyecto de Devolución.
- Planificación del Proyecto de Devolución (fases e hitos), cuya duración no debe superar las 160 horas.
- Actividades a realizar y productos resultantes.
- Funciones y responsabilidades de la APB y del adjudicatario en el transcurso de este periodo.
- Equipos de trabajo del adjudicatario del servicio y de la APB necesarios.
- Compromisos del adjudicatario para soportar la finalización del Servicio.
- Garantías asumidas por el adjudicatario una vez finalizado el Proyecto: Calidades, soporte, SLAs, periodo de garantía de los trabajos y de los resultados obtenidos.

Durante la totalidad del Periodo de Devolución, los SLAs y Calidad solicitados deberán permanecer inalterables.

El adjudicatario deberá proponer un mecanismo de retorno del servicio que contemple la transferencia a la APB de:

- Los datos y la documentación del servicio que permitan a la APB transferir los servicios operativos a otro proveedor.
- Las herramientas y utilidades desarrolladas por el adjudicatario para la prestación de los servicios y que son necesarias para la operación de los mismos por otro proveedor.
- Los contratos de servicios con Proveedores que la APB pudiera considerar necesarios para dar continuidad a la prestación de los servicios por otro proveedor.

JESUS ALBERTO GONZALEZ ABIAN - 39680807B
Oct 9 2015 2:06 PM

C.Medrano

CRISTIAN MEDRANO ESTEBAN - 38125543F
Oct 9 2015 1:37 PM