Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Servicios de Técnica de Sistemas Infraestructuras de Seguridad

Pliego de Condiciones técnicas

Septiembre de 2016

Mediterráneo, 14 · 01010 Vitoria-Gasteiz · Posta-kutxatila / Apartado: 809 · 01080 Vitoria-Gasteiz · Tel. 945 01 73 00* · Fax. 945 01 73 01 · www.ejie.eus

Versión	Fecha	Resumen de cambios	Elaborado por:	Aprobado por:
1.00	16/9/2016	Primera versión		Juanjo Carrasco Juan Pedro Alvarez

Índice

1 Necesidad e idoneidad de la contratación

EJIE, Eusko Jaurlaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, es la Empresa pública de servicios de las tecnologías de la información y las comunicaciones (TIC), cuya razón de existir es contribuir a la consecución de un Sector Público Vasco, moderno y eficiente, en el Marco Legal establecido por el Gobierno, con la seguridad y calidad necesarias y con el debido respeto al medio ambiente.
EJIE tiene como meta final la consecución de la satisfacción de sus clientes, siendo el instrumento común de prestación de servicios TIC en el Sector Público Vasco, y comprometiéndose en:

- Construir y mantener con eficiencia y calidad la infraestructura de los Sistemas de Información, posibilitando su continuidad y seguridad.
- Garantizar la interoperabilidad entre las distintas administraciones.
- Servir de apoyo a las necesidades de planificación y realización de la función informática del Sector Público Vasco, asegurando la cobertura de sus demandas con el compromiso y profesionalidad adecuados a las relaciones contractuales que se establezcan.

Por tanto EJIE debe ser, un instrumento común de referencia para la prestación de servicios TIC en el Sector Público Vasco:

- Aportando valor añadido.
- Proporcionando soluciones competitivas.
- Transmitiendo confianza a sus clientes.
- Contando con personas cualificadas y comprometidas.

Se puede obtener información más detallada y extensa en nuestra dirección de Internet http://www.ejie.eus

EJIE posee un servicio de Proyectos Tecnológicos dedicado a la realización de proyectos de Infraestructura y Gobierno de las tecnologías y un servicio de Consultoría, fundamentalmente dedicado a la definición de la Arquitectura Técnica de las Infraestructura y Sistemas de Información. Para la realización del servicio de Proyectos Tecnológicos EJIE posee para cada una de las tecnologías estratégicas de un Coordinador Tecnológico y para la realización del servicio de Consultoría de esos mismos Coordinadores, así como Técnicos y Consultores de Sistemas generalistas.
Así mismo, posee unos servicios de Explotación y Albergues que gestiona, en base a procesos basados en las buenas prácticas ITIL. Para la Gestión de esos procesos EJIE dispone de Responsables y gestores de ellos.

La necesidad del servicio objeto de esta contratación se encuadra en la realización de las tareas cotidianas de Soporte técnico de las infraestructuras de seguridad descritas en el presente pliego, bajo las directrices y supervisión del Coordinador Tecnológico y del Responsable de Seguridad de EJIE.

2 Objeto del contrato

El objeto de este pliego es la contratación de un **Servicio de Técnica de Sistemas de Infraestructuras de Seguridad,** durante un periodo de 1 año ampliable hasta 1 año más para la prestación de diferentes tareas de gestión de tecnologías sobre los sistemas del Gobierno Vasco y otras entidades en el ámbito de la Administración Pública Vasca.

Definición de servicios de técnica de sistemas de infraestructura de seguridad: se realiza en el apartado características de los servicios.

Los objetivos que deben primar en el suministro de estos servicios son:

- Garantizar un servicio de calidad y seguridad.
- Optimizar la disponibilidad y utilización de los recursos puestos en juego.
- Flexibilidad para asumir nuevas competencias y tecnologías.
- Integración con los procesos operativos de EJIE.

El contenido detallado del servicio se encuentra en los siguientes apartados.

La prestación de los servicios solicitados implicará que la empresa adjudicataria cumple con el acuerdo del nivel de servicios establecido en el presente pliego.

Así mismo, este servicio tendrá también como objetivo que se cumplan los ANS generales de cada proceso en el que participa.

2.1 Duración del contrato

Los servicios objeto del presente pliego tienen una duración prevista de un año, desde la formalización del mismo y transcurrido el período de transición, contemplándose una prórroga expresa de hasta un año, con un preaviso de dos meses.

En todo caso los servicios deberán estar plenamente operativos para iniciarse el 1 de enero de 2017. El plazo máximo del plan de transición del servicio es de un mes. Este período de transición se realizará sin coste alguno para EJIE.

2.2 Presupuesto y valor estimado

El presupuesto máximo del presente contrato es de doscientos cuarenta mil euros anuales (240.000,00 €).

El valor estimado es de quinientos cincuenta y dos mil euros (552.000,00€) IVA excluido. Existe una modificación que puede llegar a realizarse que conllevaría un aumento de un máximo del 15% del presupuesto máximo.

La facturación será mensual por la doceava parte del importe del precio de adjudicación.

2.3 Modificaciones previstas

El Gobierno Vasco, el pasado 2015, aprobó en consejo de gobierno, la iniciativa de convergencia en TI del sector público vasco. En la fase de puesta en marcha de nuevas infraestructuras, el potencial incremento de las mismas conllevaría la necesidad de ampliar los servicios de seguridad (servicios objeto de contratación) durante el despliegue inicial de dichas infraestructuras.

Por lo tanto la modificación se aplicaría a:

- Mismos servicios objeto de contratación para nuevas infraestructuras.
- El límite de la modificación prevista es de un máximo del 15% del precio de adjudicación.

3 Alcance de los Servicios

1. Tecnologías

El alcance de los Servicios abarca las Infraestructuras de Seguridad de las que EJIE es responsable, y que se encuentran especificadas en el Anexo1 – *Entorno Tecnológico*.

El servicio deberá recepcionar las nuevas tecnologías que vayan surgiendo a lo largo del contrato, fijándose para cada una los plazos y la capacitación con la que se deberán asumir.

EJIE dispone de Soportes Avanzados, que denominaremos de Tercer Nivel, con sus principales proveedores y/o mantenedores de infraestructuras. El servicio gestionará estos Soportes con los que EJIE cuenta, coordinando conjuntamente las acciones que garanticen el correcto funcionamiento de los Sistemas.

2. Disponibilidad

El servicio se ofrecerá en base a lo establecido en el apartado “horario de servicio”.

3. Ámbito

En el **entorno de la seguridad** este servicio se suministrará para los CPDs que gestiona Ejie actualmente, ubicados en Vitoria-Gasteiz, uno en avenida del Mediterráneo 14 y el otro en la calle Donostia -San Sebastián 1 o a cualquier otro que EJIE pudiera disponer, en cualquier caso ubicado en la CCAA de Euskadi.

4 Características del Servicio

El Servicio se compone de **estas funciones principales**:

- Soporte Técnico de las Infraestructuras de Seguridad
- Mejora continua y Gobierno de las tecnologías
- Auditorías de seguridad y concienciación

Las tareas a realizar por el Servicio dentro de cada una de esta tres funciones se detallan en los siguientes apartados.

4.1 Soporte Técnico

Esta función se encuadra en el Área de Sistemas y Telecomunicaciones de EJIE:

Los procesos principales para el servicio de Soporte Técnico son los siguientes:

- Gestión de Incidencias
- Gestión de Problemas
- Gestión de peticiones
- Gestión del conocimiento

4.1.1 Gestión de Incidencias e incidentes de seguridad

En las incidencias propias de las infraestructuras de seguridad, se encarga de restaurar la operación normal del servicio tan rápido como sea posible y minimizar el impacto adverso de las operaciones de negocio, asegurando que se mantienen los mejores niveles de calidad y disponibilidad del servicio.

En el resto de incidencias de seguridad, es responsable de supervisar que todas las incidencias de seguridad que se registren estén asignadas a algún grupo de soporte y reciban tratamiento para ser resueltas dentro de los niveles de servicio acordados en el SLA.

Los roles dentro del proceso de Gestión de Incidencias que asumirá el servicio es el de “Gestor de Incidencias de Seguridad”.

Responsabilidades

- **Coordinar y gestionar las incidencias de infraestructura de seguridad**
- Efectuar el seguimiento del proceso en el segundo nivel: Monitorizar la eficacia de la Gestión de Incidencias de seguridad, asegurando que las incidencias se resuelven dentro de los niveles objetivos definidos.

- Realizar recomendaciones de mejora y elevarlas al Responsable del proceso de Gestión de Incidencias.
- Crear, clasificar y actualizar los registros de incidencias con comentarios sobre las acciones que se van emprendiendo.
- Relacionar los CI's con la incidencia.
- Relacionar incidencias entre sí.
- Escalar al Gestor de Primer Nivel las incidencias que presenten conflicto en su asignación y no tenga modo de saber a qué grupo corresponde a priori.
- Realiza informes periódicos sobre la eficiencia y actividades del servicio.
- Asegurar la integridad y precisión general de las incidencias cerradas.
- Detectar y proponer una investigación de problema en la Gestión de Problemas por cada incidencia que requiera un análisis de su causa raíz

Disponibilidad de perito acreditado

Bajo demanda y ante un incidente de seguridad que lo requiera EJIE podrá solicitar servicios de un perito acreditado para la realización de un informe pericial que pueda ser necesario en la gestión de algún incidente de seguridad.

En la oferta se incluirán los servicios de la realización de **UN INFORME AL AÑO** por parte de un perito acreditado.

Se desea que los informes obtenidos cumplan con la normativa UNE 197001:2011 ("UNE 197001:2011. Criterios generales para la elaboración de informes y dictámenes periciales").

El perito debe estar suficientemente acreditado y cumplir con las competencias para el análisis forense de las evidencias electrónicas definidas en la norma UNE 71506:2013 ("Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas.").

4.1.2 Gestión de Problemas

El proceso de Gestión de Problemas se centra en la resolución definitiva de fallos y errores en la infraestructura de seguridad, más que en la restauración del servicio, como en el caso de Gestión de Incidencias. Su objetivo es descubrir la causa raíz de un malfuncionamiento, previniendo así las incidencias.

Dentro de este proceso están todas las labores proactivas que aseguren la estabilidad de los sistemas, como pueden ser su optimización y monitorización.

Es responsable de supervisar que todos los problemas de seguridad estén asignados a algún miembro de su grupo u otros grupos de soporte y reciban tratamiento para ser resueltos dentro de los niveles de servicio acordados en el SLA.

Los roles dentro del proceso de Gestión de Problemas que asumirá el servicio son los de "Gestor de Problemas de seguridad".

Responsabilidades

- Revisión prioridades de los problemas.
- Registrar nuevas investigaciones de problemas de manera proactiva.
- Recomendar acciones a seguir en base a los resultados de investigaciones de problemas y errores conocidos.
- Solicitar peticiones de cambio (RFC's) para resolver Errores Conocidos.
- Coordinar la asignación de las investigaciones de problemas y errores conocidos.
- Supervisar las investigaciones de los problemas y errores conocidos
- Revisar las peticiones de investigaciones de problemas
- Revisar las investigaciones de problemas y errores conocidos terminados
- Revisar y validar soluciones de errores
- Emitir informes al responsable del proceso
- Escalar a los Gestores las mejoras identificadas en el proceso

4.1.3 Gestión de Peticiones

Con la Gestión de Peticiones aseguramos que las peticiones que nos hace el grupo de Telecomunciaciones y Seguridad y el área de Seguridad de EJIE son recogidas, clasificadas y ejecutadas.

Dentro del proceso de la Gestión de Peticiones el servicio debe realizar las siguientes tareas:

- Aceptar y confirmar las peticiones de servicio asignadas
- Establecer una fecha fin para la petición
- Devolver aquellas peticiones que estén incorrectamente asignadas
- Proporcionar información sobre el progreso de la ejecución de las peticiones
- Informar cuando una petición haya sido finalizada
- Proporcionar toda la información necesaria según las políticas y reglas establecidas

4.1.4 Gestión del Conocimiento

Proceso responsable de recoger, analizar, almacenar y compartir conocimiento e información dentro de la organización. El servicio tiene la responsabilidad cuando una nueva tecnología le es encomendada de la aceptación y posterior mantenimiento y evolución de la documentación técnica necesaria para el correcto soporte de los sistemas de información administrados, siguiendo las directrices marcadas por EJIE.

El servicio deberá colaborar en el mantenimiento de la documentación de los sistemas identificados en el anexo I. Los apartados de referencia son:

- Manuales de Administración, instalación, operación, arquitectura …
- Normativas de implantación para los Sistemas de Información que usan ese software.
- Política y Procedimientos de Backup y Recuperación.
- Disponibilidad de servicios, niveles de servicio, requisitos de tiempos de recuperación, horario de servicio, ventana de mantenimiento y cambios.
- Relación con los soportes, teléfonos, condiciones, modo de acceso.
- Gestión Proactiva, inventario de Incidencias, monitorización.
- Gestión de Parches y Versiones.

El servicio también colaborará en el mantenimiento del catálogo de **notas técnicas del área de seguridad**.

4.2 Mejora continua y Gobierno de las Tecnologías

EJIE cuenta con Coordinadores Tecnológicos en las infraestructuras. Estos Coordinadores tecnológicos fijarán las pautas de la Mejora Continua y el Gobierno de las Tecnologías y liderarán el trabajo de este servicio, formando equipos de trabajo cuya misión se expone en los siguientes apartados.

El objetivo a conseguir es el de vigilancia y optimización de las configuraciones de las tecnologías de su competencia para que el rendimiento de los Sistemas de Información que las utilicen sea el adecuado.

Este servicio deberá formalizar, llevar a cabo y automatizar aquellas tareas de mantenimiento, "tuning" y optimización que le sean encomendadas asegurando el correcto rendimiento de las infraestructuras que se detallan en el Anexo 1.

Así mismo, como parte de sus labores, se identificarán **acciones proactivas de mejora** en los sistemas administrados que den lugar a un incremento en la calidad del servicio suministrado por EJIE a sus clientes y usuarios. Estas acciones serán estructuradas en planes de mejora cuando así lo requiera y podrán contar con la colaboración de otros grupos de EJIE **siempre y cuando los beneficios para EJIE lo justifiquen**. Planes de adecuación y mejoras de calidad del servicio, que se definirán en función de la ejecución del contrato, y se fijarán semestralmente.

Estas mejoras serán entregadas en los informes de seguimiento mensual para su valoración.

4.2.1 Configuración de los sistemas

Será objetivo de esta función mantener la configuración de los distintos sistemas de seguridad. Para ello se dotarán de las herramientas necesarias para tal fin que pondrá EJIE a su disposición:

- Revisión de las infraestructuras de seguridad existentes en la actualidad y propuesta de evolución.
- Integración de las herramientas con la CMDB de manera automatizada con distintos niveles de integración, serán la fuente autoritativa de configuración
- Colaboración en el desarrollo de pilotos y en la implantación de nuevos productos e infraestructuras de seguridad.
- Ejecución de una Gestión de parches de los distintos productos y equipos de seguridad
- Definición y supervisión de políticas de actualización de los sistemas de seguridad.
- Herramientas administrativas de configuración

Será responsabilidad de esta función la definición de la planificación anual de Parches antes de la segunda quincena de Enero, así como el aseguramiento de su cumplimiento.

El servicio deberá definir y mantener un cuadro de mando, que se revisará mensualmente, donde se especifique claramente el estado actual de los sistemas encargados en cuanto a versiones y parches.

4.2.2 Operativa de Seguridad

Se realizarán las tareas necesarias en las distintas tecnologías e infraestructuras de seguridad:

- Monitorización de la seguridad
  - Seguimiento diario de alarmas e informes generados por la herramienta SIEM. Ver apartado más adelante.
  - Ingeniería asociada a la correlación de eventos de seguridad y generación de alarmas.
  - Seguimiento mensual de indicadores
  - Planteamiento de actividad anual
- Operación de las infraestructuras de seguridad:
  - Equipos y sistemas de seguridad definidos en anexo 1
  - Actualización de patrones y firmas
- Protección contra virus y código malicioso:
  - Consola antivirus EPO:
    - La consola está gestionada, a nivel general, por un servicio ajeno al presente expediente.
    - Sí es objeto de contratación la configuración y propuesta de reglas de protección que permita gestionar la seguridad de servidores y puestos de trabajo de la RCAGV.
  - Coordinación con el CAU y la gestión de incidencias graves
    - Se debe proporcionar asesoramiento al CAU y a otros servicios de EJIE en medidas de protección contra código malicioso.
- Detección de vulnerabilidades:
  - Escaneos regulares y bajo demanda (ver apartado específico)
- Optimización de reglas de cortafuegos, tanto de perímetro como de datacenter.
- Vigilancia alerta temprana
  - Proactivamente investiga y monitoriza en Internet información de seguridad.
- Gestión de usuarios/roles de las infraestructuras de seguridad
  - Creación y administración de usuarios administradores
  - Revisión mensual sobre usuarios y permisos asociados
- Gestión de identidades de acceso

4.2.3 Administración

Será objeto de esta función la realización de tareas más proactivas dentro de los sistemas.

Dentro de las tareas a realizar destacamos las siguientes:

- Participación en la definición y ejecución de la estrategia de seguridad

- Mejora continua y Cuadros de mando
- Evaluación semestral sobre productos de seguridad:
    - Riesgos
    - Actuaciones/Alternativas
- Gestión de licencias
- Elaboración de los planes de Obsolescencia Tecnológica.
- Seguimiento de actuaciones planificadas
- Afinar el rendimiento de los sistemas de seguridad

4.2.4 SIEM

EJIE dispone de dos plataformas SIEM:

- Herramienta SIEM propia, desarrollada a medida, basada en la pila ELK ("Elasticsearch, Logstash y Kibana") de Elastic. Recientemente se ha incorporado también "Watcher" para integrarlo con la gestión de eventos.
- VMware vRealize Log Insight

Se realizarán las tareas de operación y administración de la plataforma SIEM:

- Seguimiento de paneles y eventos de la plataforma
- Incorporación de nuevas fuentes de logs y mantenimiento de las fuentes actuales
- Desarrollo de nuevos paneles de visualización de la información (Producto "Kibana")
- Incorporación y mantenimiento de nuevas alertas (producto "Watcher")
- Propuestas de evolución de la plataforma

4.2.5 Análisis y gestión de vulnerabilidades

EJIE necesita dotarse de un servicio que le permita gestionar el ciclo de vida completo de las vulnerabilidades de sus infraestructuras. El servicio debe permitir la realización de análisis de vulnerabilidades (a nivel de infraestructura) tanto sistemática como bajo demanda. Se puede ofertar un servicio que requiera infraestructura "on premise" en el CPD de EJIE o una solución mixta de "SaaS" y sondas ubicadas en la infraestructura local.

Tendremos dos fases en la gestión de vulnerabilidades:

- Período inicial
- Período productivo

4.2.5.1 Período inicial (como máximo hasta 1/5/2017)

Durante este período:

- Se debe proporcionar análisis de vulnerabilidades bajo demanda, no sistemático. Debe ser posible realizar un análisis de vulnerabilidades a un servidor que NO esté expuesto en Internet. Se podría utilizar un producto en un puesto conectado a la RCAGV.
- Se ejecutará con proyecto de diseño e implantación de la tecnología que permita proporcionar el servicio sistemático de análisis de vulnerabilidades. EJIE proporcionará la infraestructura básica (servidores, comunicaciones, sistema operativo, almacenamiento, etc), el adjudicatario todo el software necesario con sus licencias asociadas, además de sus servicios profesionales para finalizar con el producto en producción. Se presentará una planificación detallada del proyecto de implantación.

4.2.5.2 Período productivo

La plataforma debe estar operativa para el 1/5/2017.

El alcance deseado es de al menos 1000 direcciones de IP.

El servicio de la plataforma debe permitir:

- Realizar análisis de vulnerabilidades en base a una BBDD de vulnerabilidades actualizada. La plataforma, por lo tanto, debe actualizarse automática y periódicamente.
- Realizar análisis bajo demanda además de sistemático y periódico.
- Gestionar todo el ciclo de vida completo de las vulnerabilidades.
- Agrupar activos por diferentes criterios (tecnología, negocio, categorización en plan de continuidad de negocio, etc).
- Realizar análisis sistemáticos y periódicos, obteniendo informes que permitan tener información y evidencias de la situación de partida y la evolución, teniendo en cuenta las acciones de remediación y la aparición de nuevas vulnerabilidades.
- Los informes se podrán obtener a nivel global, pero también se podrán agrupar los servidores objeto de análisis por diferentes criterios como tecnología, o servicio que proporcionan.
- En los informes debe haber una propuesta de remediación.
- Los informes generados irán acompañados de informes ejecutivos para cada una de las tecnologías analizadas, en los que se incluirá el nivel de riesgo estimado junto con una estimación global de la propuesta de remediación. Se propone frecuencia trimestral para estos informes ejecutivos.

4.2.6 Acompañamiento a la mejora en seguridad de otras tecnologías

El objetivo del servicio es analizar el estado de las medidas de seguridad y buenas prácticas de gestión en algunas de las tecnologías más relevantes en EJIE. Se solicita realizar reuniones periódicas de análisis y seguimiento de la seguridad.

Se realizará este “acompañamiento” en **dos infraestructuras tecnológicas al año**.

Pasos:

- Se propondrá a EJIE un “argumentario de referencia” de medidas y buenas prácticas que se completará con el área de seguridad de EJIE.
- Posteriormente se realizará una entrevista inicial con el responsable de la tecnología objeto de análisis, para estimar el nivel de madurez y cumplimiento de todas las medidas establecidas en el argumentario de referencia.
- Se propondrá a EJIE una lista de áreas de mejora con una estimación de prioridad y nivel de esfuerzo (bajo/medio/alto). EJIE revisará la lista, para cerrar la propuesta.
- El adjudicatario realizará entrevistas de control trimestral del avance de las acciones de mejora propuestas. Cada trimestre se presentará un informe de avance de las acciones propuestas.

Características de las reuniones y seguimiento (ciclos anuales):

- Análisis inicial de situación: se analizará la situación de las medidas de seguridad en la tecnología en cuestión, junto con las iniciativas en curso y previstas, resultados de auditorías, etc.
- Propuesta de mejoras: en base a la información de las reuniones anteriores y al conocimiento obtenido del grado de madurez de la implementación de la tecnología, a los análisis de

vulnerabilidades que se haya realizado y al conocimiento adquirido sobre la situación de la seguridad en EJIE se realizarán propuestas de mejora y evolución de la seguridad.

- Seguimiento trimestral del progreso obtenido. Incorporación, si procede, de novedades en las propuestas en base a la situación actual.

4.3 Auditoría de seguridad y concienciación

4.3.1 Auditoría de seguridad

4.3.1.1 Auditoría de seguridad de servicios comunes (aplicaciones e infraestructura asociada)

Se realizarán anualmente **DOS auditorías de seguridad** de una infraestructura/aplicación/servicio común. Las fechas no estarán prefijadas, sino que serán propuestas por EJIE con una antelación de al menos un mes.

A nivel general las fases serán las siguientes:

- Análisis y establecimiento del alcance (se estima una jornada)
- Ejecución de la auditoría y redacción del informe (se estiman 8 jornadas).
- Confirmación de la remediación de las vulnerabilidades detectadas. Será EJIE el que proponga la fecha de ejecución, una vez ejecutadas las acciones previstas. (se estima una jornada)

Año	Auditoría	Auditoría	Observaciones	Plazo estimado
2017	2017-S1	WiFi	Infraestructura WiFi de EJIE	2 semanas
2017	2017-S2	Módulo de servicios comunes	Pendiente de concretar. Se seleccionarán módulos de servicios comunes. La tecnología utilizada es apache/java/weblogic/Oracle.	2 semanas
2018	2018-S1	Módulo de servicios comunes	Pendiente de concretar. Se seleccionarán módulos de servicios comunes. La tecnología utilizada es apache/java/weblogic/Oracle.	2 semanas
2018	2018-S2	Módulo de servicios comunes	Pendiente de concretar. Se seleccionarán módulos de servicios comunes. La tecnología utilizada es apache/java/weblogic/Oracle.	2 semanas

Auditoría 2017-S1 (WiFi EJIE)

Se necesita realizar una auditoría de la WiFi existente en el edificio de EJIE, desplegada con una infraestructura única y tres SSID.

Servicio solicitado:

- Análisis y verificación de los mecanismos de seguridad implementados.
- Test de intrusión: pruebas de penetración desde el exterior.
- Análisis de caja blanca de los dispositivos, revisión de configuración de los mismos.
- Análisis de la arquitectura de red
- Ataques de denegación de servicio (en horario fuera de oficina).
- Mapa de cobertura en el exterior del perímetro del edificio de EJIE.

Entregables:

- Resumen ejecutivo
- Detalle de pruebas realizadas especificando su objetivo.

- Resultados obtenidos, incluyendo el nivel de vulnerabilidades detectadas
- Propuestas de tratamiento, incluyendo estimación de esfuerzo y priorización

Auditoría 2017-S2, 2018-S1, 2018-S2 (módulos de Platea)

La plataforma "Platea" proporciona servicios comunes para administración electrónica. Se realizarán tres auditorías de los módulos que se seleccionen. La selección se realizará con el adjudicatario del expediente.

Análisis y establecimiento del alcance (1 jornada)

Se establecerá el alcance detallado, junto con el responsable del servicio auditado.

Ejecución de la auditoría (8 jornadas)

Auditoria Externa

Contempla la revisión de la seguridad mediante metodologías y conocimientos propios del equipo de trabajo. El objetivo es por una parte conocer si el servicio o la infraestructura es vulnerable (análisis de intrusión) y por otra el detectar posibles vulnerabilidades (análisis exhaustivo de vulnerabilidades).

Los accesos al servicio auditado se realizarán desde Internet.

Auditoria Interna

Revisión del servicio auditado desde el interior de la red corporativa.

No se contempla la realización de auditorías de código estático.

Informe de auditoría

Entregables:

- Resumen ejecutivo
- Detalle de pruebas realizadas especificando su objetivo.
- Resultados obtenidos, incluyendo el nivel de vulnerabilidades detectadas
- Propuestas de tratamiento, incluyendo estimación de esfuerzo y priorización

Confirmación de remediación (1 jornada)

Como fase posterior a la realización de la auditoría, y después de que EJIE ejecute las acciones de remediación que considere oportuno, será necesario confirmar que efectivamente se han remediado con éxito las vulnerabilidades.

El ofertante debe detallar las herramientas y tácticas empleadas, referencias utilizadas, contenido detallado del informe, etc.

4.3.2 Concienciación (Simulación de "phishing" y formación asociada)

Actualmente las medidas de seguridad tecnológica aportan una protección limitada frente a alguno de los ataques habituales realizados a través de Internet. Tanto los ataques de "phishing" masivos como los orientados a un objetivo concreto ("spear phishing") buscan atacar las organizaciones a través de las personas. Recientemente se han producido campañas masivas (p.e. "Cryptolocker") que pueden provocar un impacto significativo por la pérdida de información.

En este tipo de ataques se aprovecha el eslabón más débil de la cadena, que somos las personas como usuarios y administradores de las redes corporativas. Las buenas prácticas en el ámbito particular también redundan en la seguridad de las organizaciones.

Con el objetivo de conocer y reforzar la concienciación de la plantilla se solicita la **realización de campañas de "phishing" simulado** con las siguientes características, y como complemento la **realización de campañas de formación** asociadas al mismo objetivo.

El público objetivo es el personal del Gobierno Vasco (Departamentos y Organismos Autónomos) junto con el personal de EJIE, un **total de aproximadamente 7.500 personas.**

Puede ser necesario establecer **gestión** de este colectivo **en base a varios perfiles** que estableceríamos antes de comenzar el servicio. Proporcionaremos la información de usuario necesaria para estos servicios de concienciación, incluyendo el perfil asociado a cada persona.

Características de las campañas de "phishing" simulado

- No se requiere la realización de ningún análisis de información que exista en Internet sobre EJIE ni el Gobierno Vasco.
- En este servicio no se requiere la realización de ningún tipo de análisis de vulnerabilidades de los sistemas corporativos ni de los puestos de trabajo.
- Ámbito temporal: durante toda la vigencia del expediente.
- Campañas:
    - Deben diseñarse con alto nivel de calidad en lo correspondiente a diseño, variabilidad de la(s) simulación(es) y explotación de la información
    - Se presentará un **plan de campañas**. Se realizarán varias campañas diferentes (**no menos de 6 al año**) a lo largo de todo el período de contratación.
    - Se proporcionarán servicios de análisis y diseño de las campañas, que se prepararán con la colaboración de EJIE.
- Se elaborarán informes de resultado de las campañas:
    - Informes de detalle de cada una de las campañas, con información a nivel de perfil y totales
    - Informe ejecutivo de cada una de las campañas.
    - Informe global de todo el período del servicio.
    - Informe ejecutivo de todo el período del servicio.

Características de las campañas de formación

No se necesita formación general, sino específica y orientada a la protección frente a ataques de "phishing" en todas sus variantes.

El contenido debe estar en euskera y castellano.

Toda la formación propuesta se presentará en forma de "plan de formación online".

Dicho plan se validará previamente con el responsable de seguridad de EJIE. Se realizarán **varias campañas** (**no menos de 3 al año**) a lo largo de todo el período de contratación. Se deben preparar al menos tres contenidos diferentes.

Es imprescindible que la formación, que será no presencial, sea **interactiva**. Se valorará la realización de alguna prueba, asociada a cada píldora formativa, para confirmar el correcto entendimiento de la formación.

Se presentarán informes de "asistencia" (la formación será a través de Internet, no presencial).

5 Requisitos del Servicio

5.1 Procedimientos y calidad

Los niveles de Servicio ofertados deberán cumplir como mínimo los indicados en este pliego. Adicionalmente el adjudicatario, en la ejecución del servicio, podrá ofrecer otros ANS que complementen a los anteriores. Estos ANS, junto con sus penalizaciones asociadas, serán revisados trimestralmente entre el adjudicatario y EJIE. El incumplimiento de dichos niveles será penalizado, según se acuerde con el adjudicatario (ANS/penalizaciones).

También serán revisados trimestralmente estos ANS y podrán ser actualizados si fuera necesario para mejorar la calidad del servicio que EJIE presta a sus clientes.

El licitador **deberá proponer un Plan de Calidad** que garantice la correcta ejecución del servicio prestado y seguimiento del mismo.

Este plan deberá contemplar al menos:

- Medidas de calidad a implementar en el servicio y sistemas de información para garantizar la calidad del servicio.
- Control de los Niveles de Servicio.
- Plan de formación.
- Planteamiento de actividades de mejora continua del servicio.
- Cuadro de Mando de Evolución del Servicio

5.2 Plan de calidad

Proceso	Descripción	Objetivo
Gestión de Incidencias	% de incidencias en horario habitual con prioridad Crítica y Alta atendidas antes de 1 hora.	>= 99%
Gestión de Incidencias	Cumplimiento plan entregables	100%
Gestión de Problemas	Tiempo medio para terminar un problema crítico o alto	<=15 días
Gestión de problemas	Cumplimiento plan entregables	100%
Gestión de peticiones	Cumplimiento plan entregables	100%
Gestión del conocimiento	Cumplimiento plan entregables	100%
Gestión del conocimiento	Revisión/mejora documental: documentos nuevos/revisados	3

Gestión del conocimiento	Análisis de repositorio documental actual y propuesta de evolución	<1/6/2017
Gestión del conocimiento	Ejecución de la evolución	<31/12/2017
Configuración de los sistemas	Cumplimiento plan entregables	100%
Operativa de seguridad	Cumplimiento plan entregables	100%
Administración	Cumplimiento plan entregables	100%
SIEM	Cumplimiento plan entregables	100%
Análisis y gestión de vulnerabilidades	Período transitorio: análisis bajo demanda realizados al mes	3
Análisis y gestión de vulnerabilidades	Período productivo: cumplimiento plan entregables	100%
Mejora continua y gobierno de las tecnologías	Mejoras implementadas al trimestre	2
Acompañamiento a la mejora seguridad	Cumplimiento plan entregables	100%
Auditorías servicios comunes	Cumplimiento plan entregables	100%
Concienciación:”phishing”	Campañas al año	6
Concienciación: formación	Campañas al año	3

5.3 Seguimiento

5.3.1 Organización

Seguimiento Interno (Quincenal)

Objetivo

Revisión del día a día del servicio, incidencias, interrupciones de servicio, riesgos, seguimiento del servicio…

Participantes por parte de EJIE

- Responsable de Seguridad
- Responsable de Comunicaciones

Entregables por parte del servicio

- Información relevante para el seguimiento del servicio
- Actas de reuniones.

Comité de Seguimiento (Mensual)

Participantes por parte de EJIE

- Responsable de Seguridad
- Responsable Proceso de Incidencias
- Responsable Proceso de Problemas
- Responsable de Comunicaciones

Comité de Gestión (Trimestral)

Objetivo

Seguimiento de la consecución de los objetivos del servicio.

Participantes por parte de EJIE

- Responsables de procesos TI
- Responsable de Seguridad.
- Responsable de Comunicaciones

Entregables

- Informe Mensual de seguimiento deberá contener al menos:
  - Seguimiento de SLA's indicando causas de incumplimientos si los hubiera.
  - Seguimiento de incidencias y problemas.
  - Seguimiento temas de seguridad
  - Acciones proactivas del servicio.
  - Planes de formación.
  - Cuadro de Mando de evolución del servicio.
- Actas de reuniones.

Si lo considera necesario cada coordinador podrá requerir reuniones de seguimiento específicas.

5.3.2 Entregables

Entregables	Seguimiento interno	Comité de seguimiento (Mensual)	Comité de gestión – Informes ejecutivos Estrategia (Trimestral)	Según planificación servicio
Actas	-	Sí	Sí	-
Actividad en curso en el período	Sí	-	-	-
Cuadro de indicadores general • Servicio • SGSI	-	Sí	Sí	-

Entregables	Seguimiento interno	Comité de seguimiento (Mensual)	Comité de gestión – Informes ejecutivos Estrategia (Trimestral)	Según planificación servicio
Incidentes de seguridad	-	Sí	Sí	-
Incidencias: abiertas, cerradas, relevantes, etc. Se incluirán también los indicadores del plan de calidad.	-	Sí	Sí	-
Incidencias: informe por tipología	-	Sí	-	-
Perito análisis forense	-	-	-	Sí
Problemas: abiertas, cerradas, relevantes, etc. Se incluirán también los indicadores del plan de calidad.	-	Sí	Sí	-
Peticiones/tareas: abiertas, cerradas, relevantes, etc.	-	Sí	Sí	-
Gestión del conocimiento: análisis repositorio actual	-	-	Sí	Sí <1/6/2016
Gestión del conocimiento: progreso evolución	-	-	-	Sí <31/12/2016
Configuración de los sistemas: inventario de actividad del período	-	Sí	Sí	-
Operativa de seguridad: inventario de actividad del período	-	Sí	Sí	-
Operativa de seguridad: progreso optimización reglas cortafuegos	-	-	Sí	-
Administración: inventario de actividad del período	-	Sí	Sí	-
SIEM: inventario de actividad del período	-	Sí	Sí	-
Gestión de vulnerabilidades – período transitorio	-	Sí	Sí	-
Gestión de vulnerabilidades – período productivo	_	-	Sí	-
Mejora continua: detalle mejoras trimestre	-	-	Sí	-
Acompañamiento mejora seguridad	-	-	Sí	-
Auditoría servicios comunes	-	-	-	Sí
Concienciación y Phishing	-	-	-	Sí
% Dedicación de tiempos a cada apartado del servicio	-	Sí	Sí	-
Progreso del plan de formación propuesto	-	-	Sí	-

5.4 Metodología aplicable y entorno tecnológico

EJIE dispone de procedimientos y normativas propios para la gestión de los procesos que deberán cumplirse.

EJIE dispone de distintas plataforma BMC ITSM para el control de los procesos y gestión de las configuraciones que deberán ser utilizadas por el adjudicatario independientemente de las que se utilicen para su propia gestión.

- Herramientas de Gestión IT → BMC ITSM 8.1, Atrium CMDB

El servicio dispondrá de un portal de consumo propio sobre Microsoft SharePoint, que se pretende como herramienta central de gestión y colaboración.

El entorno tecnológico, abarca las Infraestructuras de Seguridad definidas en el apartado: Anexo 1 – Entorno Tecnológico.

6 Planificación y organización del servicio

6.1 Responsabilidades de dirección y gestión del servicio

Los roles del servicio de Técnica de Sistemas Infraestructuras de Seguridad y su relación a nivel funcional:

- Responsable de servicio
  - Interlocutor con el coordinador de infraestructuras de seguridad de Ejie
  - interlocutor con el gestor de incidencias
  - interlocutor con el gestor de problemas

La empresa adjudicataria deberá comunicar por escrito la designación de una persona de su organización, encargada de ejercer las facultades de **Responsable del servicio** contratado, responsabilizándose frente a EJIE de las personas que prestan el servicio y será el interlocutor con el Coordinador Tecnológico de EJIE para dicha tecnología.

Las personas asignadas a este servicio serán controladas por el responsable del servicio.

6.2 Carga de trabajo

Dentro de la oferta, basándose en los requerimientos especificados para el Servicio, en la estimación que se realiza en el Anexo 1 y del enfoque del servicio, se deberá hacer una propuesta base, que en el transcurso de la prestación del servicio podrá modificarse, tanto al alza como a la baja, dependiendo de las necesidades de EJIE en la prestación de sus servicios y que será revisada con una periodicidad semestral, siendo dichas modificaciones obligatorias para el adjudicatario.
En caso de producirse alguna variación, EJIE comunicará al menos con 1 mes de antelación las características de la misma. En todo caso sólo se facturará por los servicios efectivamente realizados.

También se deberá incorporar el coste por servicios extraordinarios que podrán ser debidos a dos causas principales:

- Implantación de sistemas de funcionalidad similar a las indicadas en el presente pliego pero de diferente tecnología
- Picos de trabajo

6.3 Prestación del servicio

El servicio se prestará **principalmente en las instalaciones de EJIE, dada la criticidad y especial necesidad y urgencia en la resolución de posibles incidencias y que se trata de servicios asociados a infraestructuras críticas para EJIE y clientes de EJIE.** La localización será separada de la plantilla de EJIE.

6.3.1 Horario del Servicio

El horario de prestación del servicio será el siguiente (pudiendo acomodarse a las necesidades del servicio):

- **Horario Habitual**
  - Jornada partida: Lunes a jueves: 8h a 17h. Viernes: 8h a 15h.
  - Jornada continua: Lunes a Viernes: 8h a 15h.

- **Horario extraordinario - Intervenciones fuera del horario habitual**
  - Por motivos de Servicio algunas intervenciones se realizarán fuera del horario habitual, en horario nocturno y/o festivos. Estas intervenciones se notificarán con la antelación suficiente. Se estima un total de **100 horas de intervenciones extraordinarias al año** incluidas en el importe total de la oferta.

6.4 Cualificación Técnica

En el transcurso de la ejecución del contrato podrán surgir nuevas tecnologías, de necesaria adaptación por parte de los recursos asignados a los servicios. La transición de éstas se llevará a cabo con la coordinación del Responsable o Responsables de EJIE.

Se deberá garantizar la actualización de los conocimientos en los componentes de los servicios. Esta actualización de conocimientos deberá ser evaluable por EJIE, semestralmente, siendo responsabilidad del adjudicatario la adaptación de los recursos. En el caso de que no se llegue a las adaptaciones requeridas podrá conllevar la rescisión del contrato.

6.5 Plan de Transición

En la oferta se deberá presentar claramente tanto el plan de transición de entrada de servicio como de salida al finalizar el contrato.

Al finalizar el periodo del presente contrato o su prórroga, el adjudicatario estará obligado, por un periodo anterior o posterior a la finalización a prestar apoyo, y realizar la transferencia del conocimiento, documentación, etc. al siguiente adjudicatario del contrato en caso de que éste sea distinto al adjudicatario del presente pliego.

El plazo máximo para cada uno de los planes de transición es de **un mes**.

7 Criterios de adjudicación

Se valorará cada servicio independientemente de manera que una vez sumadas las puntuaciones se obtenga la oferta más adecuada a las prestaciones solicitadas tanto económica como técnicamente.

La valoración se va a realizar de manera ponderada y deben tenerse en cuenta las siguientes consideraciones:

- De 100 puntos máximos de valoración, la distribución es de 51 % para la oferta económica y un 49 % para la oferta técnica.
- Será necesario superar el 60% de la valoración técnica para tenerse en cuenta la oferta económica. Determinar en apartado umbral técnico
    - Será necesario obtener el 50% de la valoración de cada apartado de la propuesta técnica para considerarse que se ha superado la valoración técnica. Es decir, en caso de que alguno de los componentes diseño del servicio, dimensión del servicio o plan de trabajo no haya obtenido un valor igual o superior al 50% no se considerará la oferta técnica.

Para la valoración de las diferentes ofertas, se tendrán en cuenta los siguientes pesos en la construcción de la valoración final:

Oferta Económica	**51%**
Calidad de la solución propuesta y plan de trabajo	**25%**
Grupo de trabajo propuesto y organización.	**20%**
Plan de transición de entrada/salida del servicio	**4%**

7.1 Normas de aplicación de los criterios de valoración

7.1.1 Oferta Económica (51%)

La valoración de la oferta presentada se realizará en función de los precios propuestos por el proveedor, siendo valorado negativamente un coste inadecuado, tanto por exceso como por defecto.

La proposición económica se valorará bajo la siguiente fórmula que se describe a continuación.

El número total de puntos asignables es de 51, aplicándose una fórmula progresiva de 3 fases con las siguientes especificaciones:

Primera fase – hasta 30 puntos
– Se asignarán 3 puntos por cada 1% de descuento que sobre el presupuesto de licitación tenga la oferta presentada, hasta un máximo de 30 puntos.

Segunda fase – hasta 45 puntos (30 de la primera fase)
– Las ofertas que en la primera fase no hayan conseguido 30 puntos, en esta fase tendrán 0 puntos.
– Para el resto de ofertas, se asignarán 2 puntos por cada 1% de descuento adicional sobre el presupuesto de licitación, hasta un máximo de 15 puntos.

Tercera fase – hasta 51 puntos (45 de la primera y segundas fases)

– Las ofertas que en la segunda fase no hayan conseguido 45 puntos, en esta fase tendrán 0 puntos.

– Para las ofertas, la forma de calcular los 6 puntos restantes es proporcional utilizando la fórmula:

> Puntuación obtenida por la Oferta a valorar = 6 x (oferta económica más competitiva / oferta a valorar)

7.1.2 Oferta Técnica (49%)

Las propuestas que no obtengan al menos un sesenta por ciento de valoración en el global de apartados de la oferta técnica, quedarán excluidas y no se procederá a la apertura de sus ofertas económicas.

Ajuste proporcional de la valoración

Con el fin de ajustar al máximo la valoración técnica se aplicará una regla de tres directa de manera que, la propuesta con mayor puntuación técnica obtenga el máximo de la puntuación (49 puntos) y el resto de las propuestas recibirán una asignación proporcional directa.

Puntuación técnica definitiva = (49 x Puntuación evaluada) / Puntuación técnica más alta entre las presentadas

VALORACIÓN TÉCNICA

					FACTORES DE PONDERACIÓN			
			Puntos	Puntos max.	Óptimo	Mejorado	Básico	Deficiente
Calidad de la solución propuesta y plan de trabajo		**25%**	**25**		**1**	**0,75**	**0,5**	**0,25**
Enfoque	**20%**			5	5	3,75	2,5	1,25
Planteamiento individual por función (70%)								
Soporte técnico	**24%**			6	6	4,5	3	1,5
Mejora continua y gobierno de las tecnologías	**23%**			5,75	5,75	4,3125	2,875	1,4375
Auditoría de seguridad y concienciación	**23%**			5,75	5,75			
Acciones de mejora	**5%**			1,25	1,25	0,9375	0,625	0,3125
Procedimientos de gestión, control y calidad del servicio	**5%**			1,25	1,25	0,9375	0,625	0,3125
Grupo de trabajo y organización		**20%**	**20**					
Detalle de los perfiles profesionales	**50%**			10	10	7,5	5	2,5
Adecuación del tamaño y estructura del equipo	**50%**			10	10	7,5	5	2,5
Plan de transición de entrada y salida		**4%**	**4**					
Recursos y tiempo empleados		20%		0,8	0,8	0,6	0,4	0,2
Estrategia empleada		80%		3,2	3,2	2,4	1,6	0,8

TOTAL PUNTOS	**49**	**32,4375**	**21,625**	**10,8125**

- Calidad de la solución propuesta y plan de trabajo
  - **Enfoque:** se valorará el enfoque global de los servicios ofertados, la estrategia general propuesta.

Óptimo	Se considerará cuando el servicio global propuesto cumple las características definidas en el pliego, desarrolla total, exhaustiva y adecuadamente todos los apartados y ofrece una visión coherente, con un modelo más eficaz y eficiente y una estrategia óptima.
Mejorado	Se considerará cuando el servicio global propuesto cumple las características definidas en el pliego, desarrolla adecuadamente todos los apartados y ofrece una visión coherente.
Básico	Se considerará cuando el servicio global cumple las características definidas en el pliego y desarrolla todos los apartados.
Deficiente	Se considerará cuando el servicio global propuesto no cumple las características definidas en el pliego

  - **Planteamiento individual por función:** se valorará el planteamiento presentado para cada proporcionar cada uno de los servicios indicados.
    - Soporte técnico
    - Mejora continua y gobierno de las tecnologías
    - Auditoría de seguridad y concienciación

Óptimo	El servicio ofertado asociado a la función concreta objeto de valoración se ha descrito coherentemente en base a lo solicitado y con un planteamiento óptimo. Se realizan propuestas que permitirán la adopción de un modelo más eficaz, y competitivo, en definitiva más eficiente.
Mejorado	El servicio ofertado asociado a la función concreta objeto de valoración se ajusta a lo solicitado ofreciendo valor añadido adicional a las especificaciones del pliego, con un buen planteamiento.
Básico	El servicio ofertado asociado a la función concreta objeto de valoración se ajusta a lo solicitado sin ofrecer valor añadido adicional a las especificaciones del pliego.
Deficiente	El servicio ofertado asociado a la función concreta objeto de valoración no se ajusta a lo solicitado.

  - **Acciones de mejora:** se valorará el planteamiento realizado en la propuesta de gestión de las mejoras del servicio

Óptimo	El planteamiento de la gestión de la mejora se considera muy adecuado a nivel global, bien diseñado y desarrollado con suficiente nivel de detalle. Se considera que aportará

	valor significativo al servicio global.
Mejorado	El planteamiento de la gestión de la mejora se considera adecuado a nivel general. Se considera que aportará cierto valor al servicio global.
Básico	Se oferta lo solicitado sin aportar mayor detalle ni valor.
Deficiente	Planteamiento de acciones de mejora es deficiente.

- Procedimientos de gestión, control y calidad del servicio:

Óptimo	Los procedimientos de gestión, control y calidad del servicio tienen alcance global y buena orientación estratégica, se han desarrollado con gran nivel de detalle y se considera que aportarán valor al servicio. El cuadro de mando se ha desarrollado con buen nivel de detalle.
Mejorado	Los procedimientos de gestión, control y calidad del servicio tienen alcance global, se han desarrollado suficientemente y se considera que aportarán valor al servicio.
Básico	Los procedimientos de gestión, control y calidad del servicio cumplen básicamente con lo solicitado.
Deficiente	Los procedimientos de gestión, control y calidad del servicio se consideran insuficientes o no se han descrito suficientemente.

- Grupo de trabajo y organización: se valorará la composición y organización del equipo de trabajo, identificando características de los perfiles y la asignación de recursos y funciones
  - Detalle de los perfiles profesionales: se deben identificar los roles y perfiles asociados a todos y cada uno de los servicios solicitados.

Óptimo	La propuesta de perfiles profesionales se considera adecuada para cubrir los servicios. En todos ellos el perfil se considera muy adecuado.
Mejorado	La propuesta de perfiles profesionales se considera adecuada para cubrir los servicios. En algunos de ellos el perfil se considera muy adecuado.
Básico	La propuesta de perfiles profesionales se considera básicamente adecuada para cubrir los servicios.
Deficiente	La propuesta de perfiles profesionales se considera inadecuada.

  - Adecuación del tamaño y estructura del equipo: se valorará la composición, organización del equipo de trabajo y la asignación de recursos

Óptimo	La propuesta de tamaño y estructura del equipo se considera óptimamente adecuada para cumplir lo solicitado en el pliego.
Mejorado	La propuesta de tamaño y estructura del equipo se considera adecuada para cumplir lo solicitado en el pliego.
Básico	La propuesta de tamaño y estructura del equipo se considera parcialmente adecuada para cumplir lo solicitado en el pliego.
Deficiente	La propuesta de tamaño y estructura del equipo se considera insuficiente.

- Plan de transición de entrada y salida
  - Recursos y tiempo empleados: se valora cómo se plantea la aceptación y devolución del servicio en lo correspondiente a recursos y tiempo empleado

Óptimo	Se considera que los recursos y/o tiempos ofertados son suficientes y especialmente adecuados para realizar planes de transición con buenas garantías de éxito, y con los controles de calidad suficientes y visión general del servicio desde las fases iniciales.
Mejorado	Se considera que los recursos y/o tiempos ofertados son suficientes y especialmente adecuados para realizar planes de transición con buenas garantías de éxito.
Básico	Se considera que los recursos y/o tiempos son suficientes para ejecutar ambos planes de transición.
Deficiente	Se considera que los recursos y/o tiempos son insuficientes.

  - Estrategia empleada: se valorará el planteamiento de la transición de entrada y salida, fases, condicionantes, organización, etc.

Óptimo	La estrategia planteada para los planes se ha descrito con suficiente detalle, el planteamiento se considera excelente y especialmente adecuado.
Mejorado	La estrategia planteada se considera adecuada para realizar ambos planes, con un buen planteamiento y suficiente detalle.
Básico	La estrategia planteada se considera de alguno de los dos planes se considera suficiente, pero no la de ambos.
Deficiente	La estrategia planteada se considera insuficiente.

7.1 Condiciones de Seguridad/Generales

EJIE S.A. proporcionará acceso a sus sistemas informáticos y entregará la información, software y documentación necesaria para poder llevar a cabo los Servicios especificados, debiendo la empresa adjudicataria comprometerse a no utilizar para otros fines que los recogidos en el presente Pliego de Condiciones Técnicas, así como a no extraerla, cederla, publicarla o venderla total o parcialmente, ni en soporte informático ni en papel, debiendo proceder a la devolución de los soportes de la información facilitados por EJIE, S.A., así como a la descarga de la misma de los equipos informáticos (si existieran), una vez se dé por concluido el trabajo. Queda terminantemente prohibido:

- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.
- Los equipos y/o aplicaciones que no estén especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de EJIE o bajo supervisión de EJIE. Todos los ordenadores personales que se conecten a la red corporativa serán de las marcas y modelos homologados. El proveedor pondrá a disposición de EJIE dichos equipos para que se les instale el software necesario. Todos los ordenadores personales a los que EJIE les haya instalado software se llevarán a EJIE para que se formatee el disco duro a la finalización del servicio a EJIE.
- El proveedor se compromete a informar periódicamente a EJIE de los activos de información con los que proporciona el servicio.

Serán también de obligado cumplimiento las “Políticas de Seguridad para empresas proveedoras” (Anexo Seguridad del presente PCT, publicadas también en www.ejie.eus, apartado “Perfil de contratante”, “información”).

8 Contenido de las Ofertas

8.1 Contenido

EJIE requiere la presentación de las ofertas al menos en castellano. Si así lo desean, se permite a los suministradores que proporcionen información adicional, como descripciones de productos e información de referencia a modo de anexos.

Todos los documentos que formen parte de la respuesta al Pliego de Condiciones tendrán que estar identificados al menos por un título, un número de documento y su fecha de publicación. Dentro de cada documento, todas las páginas deben mostrar el título del documento y el número de página.

Las ofertas que se presenten en función de lo establecido en el presente pliego y Anexos y el Pliego de Condiciones Particulares, deben incluir:

Documento de Propuesta Técnica-

Se requiere que la respuesta al presente pliego por parte de los licitantes sea lo más detallada posible, incluyendo apartados específicos para todos y cada uno de los criterios y subcriterios de adjudicación.

Documento de Propuesta/Oferta Económica

1. Importe Total de la oferta Económica: sin I.V.A

   *Coste Transición será por cuenta de la empresa adjudicataria.

2. La realización de los servicios por necesidades de proyectos, se ajustan a la programación propia del proyecto. Por necesidades no previstas inicialmente en el desarrollo del servicio, se determinará un precio hora de presencia física (precio por asistencia y presencia física en EJIE- €/ hora-) para el caso de que sean necesarias más de 100 horas/año de intervenciones en horario extraordinario.

8.2 Consideraciones

8.2.1 Equipo de trabajo

8.2.2 Constitución inicial del equipo de trabajo

El equipo humano a incorporar tras la formalización del contrato ***para la ejecución de los trabajos deberá estar formado por componentes relacionados en la oferta adjudicataria y consecuentemente valorados***.

Si tras la adjudicación se observara que el equipo de proyecto no se corresponde con el Documento de Propuesta Técnica objeto de la misma y:

3. Caso que el adjudicatario presente justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio, se procederá a:
   - ✓ La presentación por el adjudicatario de sustituto o sustitutos con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir,
   - ✓ Aceptación de los sustitutos por parte de la Dirección del Proyecto de E.J.I.E.
4. ***Caso de que E.J.I.E. estime que el cambio no se corresponde con causa justificada***, de fuerza mayor y no imputable al adjudicatario, ***E.J.I.E. se reserva el derecho*** no solo a la aprobación ***de*** la persona o personas sustitutivas, sino incluso a la revisión de la adjudicación y en su caso ***la rescisión del pedido/contrato***, si este hecho fuera elemento determinante en la mencionada adjudicación.

8.2.3 Modificaciones en la composición del equipo de trabajo

La valoración final de la calidad del servicio la realizará EJIE y podrá solicitar el cambio de cualquiera de los componentes del equipo de trabajo, con un preaviso de quince días, por otro de igual categoría, titulación, perfil lingüístico y experiencia, si existen razones justificadas que lo aconsejen.

Si el adjudicatario propusiera el cambio de una de las personas del equipo de trabajo, se deberá solicitar por escrito con quince días de antelación, y requerirá de las siguientes condiciones:

1. Justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio,
2. Presentación de sustituto o sustitutos con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir,
3. Aceptación de la Dirección del Proyecto de E.J.I.E.

Los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto debidos a las sustituciones de personal, deberán subsanarse mediante periodos de solapamiento sin coste adicional, durante el tiempo necesario. Si a criterio de la Dirección del Proyecto de E.J.I.E., esto no fuera posible, las tres primeras semanas (periodo de adaptación) de trabajo del sustituto no serán facturables corriendo a cargo del adjudicatario. Igualmente correrán a cargo del adjudicatario las actividades/costes de formación necesarias para la realización efectiva de las actividades del servicio.

8.2.4 Transferencia tecnológica

Durante la ejecución de los trabajos objeto del contrato el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por la Dirección del proyecto de E.J.I.E., y a tales efectos, la información y documentación que ésta solicite para disponer de un pleno conocimiento de los trabajos desarrollados, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizados para resolverlos.

Todos los trabajos realizados para el buen fin del presente contrato tendrán carácter confidencial, no pudiendo la empresa adjudicataria utilizar para sí ni proporcionar a terceros, datos o información alguna de los trabajos contratados sin autorización escrita de EJIE, estando, por tanto, obligado a poner todos los

medios a su alcance para conservar el carácter confidencial y reservado tanto de la información y documentación recibida de EJIE, como de los resultados obtenidos del trabajo realizado.

La empresa adjudicataria será responsable de daños y perjuicios que se deriven del incumplimiento de esta obligación.

Todos los derechos de propiedad intelectual y de 'Copyright' que se puedan derivar de dichos trabajos serán propiedad exclusiva de EJIE, obligándose las partes a otorgar el documento oportuno cuando éste sea necesario, para la debida constancia pública de este hecho ante cualquier Organismo o Registro, tanto de la Comunidad Autónoma como de la Administración Central del Estado Español.

La empresa adjudicataria será responsable de daños y perjuicios que se deriven del incumplimiento de esta obligación.

8.2.5 Licencias y productos

En caso de que el proveedor plantee la utilización de productos adicionales a los ya existentes en la organización, EJIE analizará la necesidad e idoneidad de los mismos y procederá a su aceptación o denegación.

9 Anexo 1 - Entorno tecnológico

En este anexo se describe el entorno tecnológico actual:

Sistemas Estratégicos

1	Sistemas de detección y prevención de intrusión
2	SIEM
3	Cortafuegos de perímetro y datacenter
4	Protección del correo electrónico
5	Sistemas Radius/TACACS

Volumen:

Apartado	EQUIPOS	CANTIDAD
1	Sondas serie I (Mcafee)	1
1	Sondas serie M (Mcafee)	4
2	SIEM: • disponemos de una plataforma propia en base a la pila tecnológica ELK de Elasticsearch. • VMware vRealize Log Insight	2
3	Cluster Firewall perímetro (Actualmente Stonegate-Forcepoint)	8
3	Cluster Firewall de datacenter (Cisco FWSM)	3
4	Sistemas Antispam (Mcafee)	2
5	Sistemas ACS (Cisco). **Un equipo dedicado a recolección de logs.**	3
-	Cluster Sistemas IPAM (Efficient IP) **Se utilizará como fuente de información. No se requiere gestión.**	1
-	Consola EPO Antivirus (Mcafee-Intel) **Se requiere conocimiento profundo de la plataforma y proponer estrategia y directrices de seguridad al grupo que lo gestiona.**	7.500

Herramientas gestión de la configuración y administración:

- Plataforma de gestión de IPS: Network Security Manager (Mcafee)

- Plataforma de gestión de firewall: SCM (Stonegate Center Management)
- Consola de gestión de antivirus EPO (Mcafee)
- Consola de gestión Antispam: Mcafee EMAIL Security Appliance
- Plataforma de Gestión de Red: HP Open View (Network Node Manager y Network Automation)

Soporte especializado de tercer nivel:

Mantenedor más fabricante.