Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

EXPEDIENTE Nº: EJIE-029-2024

Servicios de asistencia técnica de ciberseguridad para el Departamento de Seguridad del Gobierno Vasco (DSGV).

Especificaciones de compra / Pliego de condiciones técnicas

Febrero 2024

Versión	Fecha	Resumen de cambios	Elaborado por:	Aprobado por:
1.0	23/02/2024	Versión Inicial	Javier González Tavera	Josu Bagazgoitia

Índice

1 Introducción

1.1 Perfil de la Compañía

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 de los Departamentos y Organismos Autónomos del Gobierno, 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 https://www.ejie.eus.

2 Objeto del contrato

2.1 Introducción

La Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos, en adelante DGTSI, adscrita a la Viceconsejería de Administración y Servicios, es la encargada de prestar servicios informáticos y de comunicaciones al Departamento de Seguridad del Gobierno Vasco (en adelante DSGV).

Para llevar a cabo estas funciones es necesario disponer de un equipo humano que sea capaz de prestar servicios de asistencia técnica y soporte a los técnicos propios del Área de Sistemas de forma que se pueda asegurar el nivel de servicio requerido por los aplicativos y plataformas de ciberseguridad utilizados en DSGV.

2.2 Objeto de la Contratación

El objeto de este expediente es la contratación de los servicios necesarios para la **Asistencia Técnica de Ciberseguridad**. Dicho servicio se estructurará de forma que pueda cubrir las necesidades del área de Ciberseguridad proporcionando para ello los recursos necesarios para la gestión y la optimización de los medios disponibles en cada momento, obteniendo el máximo aprovechamiento de las posibilidades de los sistemas informáticos del Departamento de Seguridad y garantizando el correcto funcionamiento de los sistemas de DSGV.

Los objetivos perseguidos con esta contratación, entre otros, son:

- Garantizar un servicio de calidad.
- Optimizar la disponibilidad y utilización de los recursos.
- Evitar deficiencias de servicio.
- Flexibilidad para asumir nuevas competencias y tecnologías.

La prestación de los servicios solicitados requiere, la asignación de recursos humanos con un alto nivel de capacitación técnica para resolver los problemas que se planteen de forma satisfactoria. Además, las empresas licitantes deberán ser capaces de proporcionar refuerzo y soporte a los técnicos asignados al contrato cuando la situación lo demande.

Se debe contemplar durante el periodo de vigencia del contrato, la posibilidad de realizar ajustes por cambios en la infraestructura tecnológica actualmente operativa, cambio fundamentado por la propia evolución de la arquitectura tecnológica de la organización, cuyo alcance exacto es imposible prever en estos momentos. El dimensionamiento del servicio ofrecido deberá prever esta circunstancia.

3 Alcance del contrato

En este apartado se describe el alcance de los servicios solicitados a través de este expediente.

3.1 Entorno tecnológico

El entorno tecnológico sobre el que se prestarán los servicios de asistencia técnica aquí descritos se indica en el Anexo reservado *Entorno tecnológico de Ciberseguridad* del Pliego de Condiciones Técnicas, en adelante PCT.

Asimismo, dado que este entorno tiene un carácter de renovación y evolución continua, los servicios de asistencia técnica estarán alineados con dicha evolución.

3.2 Cobertura horaria

El desarrollo de las funciones con carácter presencial se realizará dentro del horario normal:

- Lunes a jueves: 8h a 18h
- Viernes y jornada intensiva: 8h a 15h

Durante el horario denominado normal se debe garantizar el nivel de servicio presencial, sin discontinuidades.

En situaciones de crisis o de intervenciones planificadas DSGV podrá solicitar la extensión de la disponibilidad del servicio como se describe en el apartado 5.5 Horario del servicio.

.

4 Requisitos del Servicio

4.1 Requisitos técnicos del Servicio

El servicio de Asistencia Técnica de Ciberseguridad será el encargado de la "monitorización y respuesta de la seguridad" de DSGV.

En esa línea, se encargará de la administración completa de las herramientas específicas dedicadas a la monitorización y respuesta de la seguridad de las que disponga DSGV (consultar Anexo reservado *Entorno tecnológico de Ciberseguridad* del PCT).

Dentro del alcance de este expediente se incluyen servicios de mantenimiento correctivo y preventivo que solo son de aplicación para el entorno marcado objeto de administración completa que se especifica en el citado Anexo reservado.

Adicionalmente será el responsable de incorporar a dicha monitorización y respuesta los diferentes elementos que se consideren relevantes, detallándose a continuación requisitos relacionados con dicha "monitorización y respuesta de la seguridad":

4.1.1 Soporte Técnico

Esta función la realizará el servicio en el ámbito de las infraestructuras de las que es responsable y administra completamente:

4.1.1.1 Gestión de Incidencias

El Objetivo del proceso de Gestión de Incidencias es conseguir la restauración del servicio a la normalidad cuanto antes y minimizar el impacto adverso sobre las operaciones de negocio ante cualquier incidencia. Se debe garantizar que se mantengan los niveles de servicio de alta calidad y que la disponibilidad del servicio se corresponda con los requisitos exigidos.

4.1.1.2 Gestión de Peticiones

Con la Gestión de Peticiones se asegura que aquellas peticiones expresas para el presente servicio en materia de Seguridad son recogidas, clasificadas y ejecutadas.

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

- Definición de políticas de seguridad y catálogo de peticiones en este ámbito.
- Aprobación de peticiones relacionadas con seguridad en base a políticas establecidas.
- Proporcionar a los responsables del servicio toda la información necesaria según las políticas y reglas establecidas.

4.1.1.3 Gestión del Conocimiento

Es el proceso responsable de recoger, analizar, almacenar y compartir conocimiento e información dentro de la organización. Cuando una nueva tecnología le es encomendada, el servicio tiene la responsabilidad

de la aceptación y posterior mantenimiento y evolución de la documentación técnica necesaria para el desarrollo de sus actividades relacionadas con la monitorización, definición de políticas, etc.

4.1.2 Gestión de Incidentes de Seguridad

Dentro del proceso de Gestión de Incidencias el servicio asumirá el rol de "Gestor de Incidentes de Seguridad", con las siguientes responsabilidades:

- Colaborar en la revisión/definición de los procedimientos de respuesta a incidentes de seguridad.
- Coordinar y gestionar los incidentes de seguridad.
- Elaboración de procedimientos de respuesta para el nivel 1 (operación) para los diferentes tipos de incidentes de seguridad, priorizando los más habituales.
- Efectuar el seguimiento del proceso en el segundo nivel: Monitorizar la eficacia de la Gestión de Incidentes de seguridad, asegurando que se resuelven dentro de los niveles objetivos definidos.
- Realizar recomendaciones de mejora y elevarlas al responsable del proceso de Gestión de Incidencias.
- 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.
- Realizar informes periódicos con el detalle y acciones realizadas en relación a los incidentes de seguridad.

4.1.3 Mejora continua y Gobierno de las Tecnologías en materia de Seguridad

La DGTSI 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 en el ámbito de la seguridad, formando equipos de trabajo cuya misión se expone en los siguientes apartados.

El objetivo por conseguir es el de vigilancia y propuestas de optimización de las configuraciones de las tecnologías de su competencia para que los niveles de seguridad de los Sistemas de Información sean los adecuados.

Asimismo, como parte de sus labores, se identificarán acciones proactivas de mejora en la seguridad de los sistemas de su competencia que den lugar a un incremento en la calidad del servicio suministrado por la DGTSI a sus usuarios. Estas mejoras serán entregadas en los informes de seguimiento mensual para su valoración.

4.1.3.1 Configuración de seguridad los sistemas

Será objetivo de esta función auditar y colaborar en la configuración de los distintos sistemas en el ámbito de la seguridad, especialmente las infraestructuras de seguridad. Para ello se dotarán de las herramientas necesarias para tal fin que pondrá DSGV a su disposición:

- Revisión de las infraestructuras de seguridad existentes en la actualidad y propuesta de evolución.
- Integración de las herramientas de manera automatizada como fuente autoritativa de configuración para implementar respuestas a nivel de seguridad.
- Colaboración en el desarrollo de pilotos y en la implantación de nuevos productos e infraestructuras de seguridad.
- Definición y supervisión de políticas de actualización de los diferentes sistemas de la organización, como parte del proceso de gestión de vulnerabilidades y de obsolescencia. Especial énfasis en el equipamiento de seguridad y el equipamiento expuesto en Internet.
  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.
- Monitorización, gestión y coordinación de la Seguridad IT en el día a día con herramientas propias de Seguridad y revisando otras.

- Hardening: Colaboración en la definición e implementación de guías de bastionado de los diferentes ámbitos IT, especialmente en los elementos de seguridad. Investigación y recomendaciones.
- Gestión y supervisión de la administración de la Seguridad en los diferentes elementos.
- Colaboración en el tratamiento de Obsolescencia Programada.

4.1.3.2 Operativa de Seguridad

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

- Monitorización de la seguridad:
    - Diseño y análisis de diferentes herramientas de correlación de eventos de seguridad
    - Implantación de la solución identificada e integración con el resto de las herramientas de seguridad presentes en la DGTSI
    - Seguimiento diario de alarmas e informes generados por las distintas herramientas de monitorización de la seguridad (SIEM, DLP,)
    - Ingeniería asociada a la correlación de eventos de seguridad y generación de alarmas
    - Seguimiento mensual de indicadores
    - Planteamiento de actividad anual
- Colaboración en la operación de las infraestructuras de seguridad.
- Gestión de vulnerabilidades:
    - Propuesta de plan anual de tareas de hacking ético y test de penetración como parte del servicio.
    - Ejecución y gestión de escaneos regulares y bajo demanda
    - Gestión de auditorías de seguridad: Análisis y gestión de las vulnerabilidades detectadas.
- Optimización de reglas de cortafuegos, tanto de perímetro como de CPD.
- Vigilancia alerta temprana: investiga y monitoriza proactivamente 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.
- Colaboración en la gestión de identidades de acceso.

4.1.3.3 Estrategia de Seguridad

Dentro de las tareas a realizar se destacan las siguientes:

- Participación en la definición y ejecución de la estrategia de seguridad.
- Mejora continua y Cuadros de mando de seguridad.
- Evaluación semestral sobre productos de seguridad:
    - Riesgos.
    - Actuaciones/Alternativas.
- Gestión de licencias en el ámbito de la seguridad.
- Elaboración de los planes de Obsolescencia Tecnológica.
- Desarrollo del Plan de Continuidad de Negocio TI y de los Planes de Contingencias derivados.

4.1.3.4 Análisis y gestión de vulnerabilidades

El servicio debe liderar la gestión del ciclo de vida completo de las vulnerabilidades de sus infraestructuras.

- Propuesta y ejecución de un plan anual de tareas de hacking ético y test de penetración como parte del servicio.
- Ejecución y gestión de escaneos regulares y bajo demanda
- Gestión de auditorías de seguridad: Análisis y gestión de las vulnerabilidades detectadas, persiguiendo el parcheo o corrección de las vulnerabilidades o errores detectados, completando el ciclo de la gestión de vulnerabilidades.

4.1.4 Asesoramiento y Cumplimiento de Normativas de seguridad

En este ámbito, el servicio realizará las siguientes tareas:

- Acompañamiento y asesoramiento al responsable de sistemas en materia de Seguridad de manera transversal (normativa y técnica).
- Supervisión, dirección y apoyo en materia de Seguridad a los grupos operacionales.
- Seguimiento y mantenimiento de la seguridad acorde a la legislación aplicable y/o buenas prácticas.
- Colaboración en la definición de políticas de Seguridad y seguimiento de la aplicación de las mismas.
- Concienciación: Elaboración, ejecución y seguimiento de un plan de concienciación a los usuarios del Departamento.
- Identificación de nuevas necesidades en materia de Seguridad IT.
- Labores de vigilancia y pilotaje de nuevas herramientas y/o servicios.
- Ejecución de auditorías internas según normativas ISO 27001, ENS, GDPR.

4.1.5 Otras tareas a demanda

Bajo demanda, DSGV podrá solicitar los servicios de un perito acreditado para realizar 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.”), tareas relacionadas con pentesting (hacking ético y penetración), Red Team, respuesta ante incidentes, etc.

El licitador deberá indicar el precio por jornada para la realización de estos tipos de tareas en el modelo económico (Anexo I del PCP).

4.1.6 Bolsa de horas

Se solicita una bolsa de horas para asistencia adicional que cubra intervenciones planificadas, así como casos de emergencia o necesidades imprevistas relacionadas con incidentes o problemas como ataques de seguridad, brechas de datos, problemas de red críticos, incidentes de malware o virus, problemas de acceso no autorizado, etc. El adjudicatario deberá disponer de medios para recibir las peticiones de este tipo de actuaciones ya que el horario es 24x7.

En este sentido, el licitador deberá indicar su propuesta de un mínimo de 48 y un máximo de 72 horas en el modelo económico (Anexo I del PCP), que podrán ejecutarse a lo largo de la duración del contrato para cubrir las tareas descritas.

Al tratarse de un dato de carácter objetivo (evaluable mediante fórmulas) de los establecidos en el archivo electrónico de fórmulas, no podrá incluirse dentro de la oferta técnica (archivo electrónico de criterios de juicio de valor) porque la oferta sería excluida.

4.2 Requisitos metodológicos del servicio

El desarrollo del Servicio y su calidad deberá gobernarse de acuerdo a unos Acuerdos de Nivel de Servicio (ANS) que sirvan para medir el grado de calidad del mismo, un Plan de Calidad que desarrolle las estrategias

y procedimientos implantados para la consecución de los ANS y unas reuniones periódicas que permitan evaluar la marcha del Plan de Calidad, el grado de cumplimiento de los ANS y permitir la toma de decisiones necesarias para mitigar desviaciones y mejorar continuamente la calidad del servicio.

Los niveles de servicio ofertados deberán cumplir, como mínimo, los indicados en este pliego. Adicionalmente el licitador podrá ofrecer otros ANS que complementen a los anteriores. Estos ANS, junto con sus penalizaciones asociadas, serán revisados por la adjudicataria y DSGV. En cualquier caso, si a criterio de DSGV fuera necesario para mejorar el servicio que presta a sus clientes, durante estas revisiones los ANS podrán ser actualizados, añadidos o retirados. El incumplimiento de dichos niveles será penalizado según lo dictado en el pliego de condiciones particulares.

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

La adjudicataria deberá asistir a reuniones de seguimiento periódicas según lo establecido en el presente contrato. Sin perjuicio de lo anterior, podrán establecerse más reuniones específicas debidamente justificadas promovidas/requeridas tanto por DSGV como por la adjudicataria. En lo posible, estas reuniones adicionales deberán planificarse con la antelación suficiente e indicar las personas convocadas y el orden del día a tratar.

4.2.1 Niveles de servicio

4.2.1.1 Mantenimiento preventivo

El licitador propondrá en su oferta un plan de mantenimiento preventivo que incluya las tareas necesarias orientadas a evitar la aparición de problemas y/o incidencias en las plataformas objeto del servicio dentro de un plan de mantenimiento preventivo orientado por el fabricante de cada equipo y completado por aquellas otras tareas propuestas por el licitador.

Dentro del plan de mantenimiento preventivo se incluirán las tareas de instalación de los parches de los diferentes elementos de software gestionados por el servicio. Estas instalaciones se realizarán de acuerdo con las directivas dictadas por el Área de Sistemas de la DGTSI.

Los informes de gestión del servicio deberán incluir el porcentaje de plataformas pendientes de instalación de actualizaciones y con errores en las mismas. En los informes se tomará como referencia el día 30 de cada mes y no deberán superar el 20% de elementos sin actualizar.

En caso de sistemas con errores de instalación se propondrán medidas correctoras que deberán ser aprobadas por el Área de Sistemas.

4.2.1.2 Mantenimiento correctivo

4.2.1.2.1 Sistema de recepción de avisos de incidencia

La empresa adjudicataria deberá disponer de un medio de atención de incidencias, destinado a recibir, procesar y coordinar la prestación de su servicio de mantenimiento.

En consonancia con el “Periodo de Atención” solicitado, el contratista dispondrá de un sistema de recepción de avisos de incidencias durante las 24 horas del día, con respuesta personal como mínimo durante la jornada laboral y con localizaciones individuales y personalizadas para el personal “in situ”, admitiéndose respuestas mecanizadas (reencaminamiento automático del aviso al equipo de mantenimiento) fuera de la jornada laboral.

4.2.1.2.2 Tiempos de respuesta y acción

La capacidad y celeridad del contratista a la hora de responder a los avisos y de ejecutar las tareas objeto de este contrato se miden mediante el establecimiento de los denominados “Tiempos de respuesta y acción”.

Se definen los siguientes conceptos de tiempo orientados a establecer sistemas de medición de los niveles de servicio:

- Tiempo de respuesta al aviso
- Tiempo de inicio de actividades “in situ”
- Tiempo de reparación

Se recoge a continuación la definición de cada uno de estos tiempos y los límites fijados:

- **Tiempo de respuesta al aviso**

  En caso de producirse un aviso de incidencia, se define el tiempo de respuesta al aviso como el tiempo contado a partir de la notificación del aviso al Adjudicatario, a través del sistema de recepción de avisos establecido en el contrato, hasta que el servicio técnico del Adjudicatario se pone en contacto con DSGV para conocer la naturaleza del aviso, analizar su naturaleza e iniciar si procede las actuaciones.

  Este tiempo no debe sobrepasar el “Tiempo máximo de respuesta al aviso” fijado y que se especifica en la tabla de tiempos de referencia.

- **Tiempo de inicio de actividades “in situ”**

  En caso de que se requiera la realización de actividades “in situ” sobre los elementos del alcance, se define el tiempo de inicio de actividades como el tiempo, contado a partir de notificar por parte del DSGV la necesidad de dicha actuación al Adjudicatario, hasta el inicio de las reparaciones o tareas “in situ”.

  Inicialmente será un tiempo de referencia, controlado, y con posible incorporación posterior a los ANS exigibles.

  Este tiempo no debe sobrepasar el “Tiempo máximo de inicio de actividades” fijado y que se especifica en la tabla de tiempos de referencia.

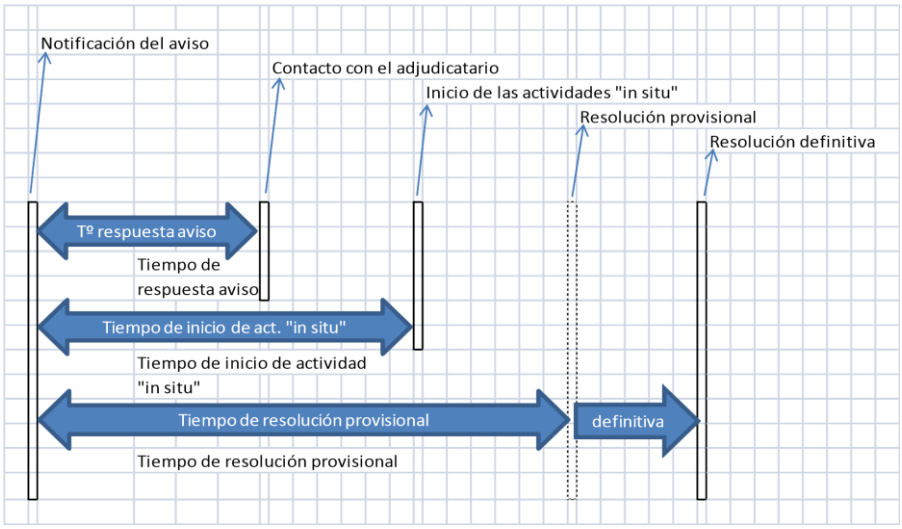
- **Tiempo de resolución**

  Se define el “Tiempo de resolución” como el tiempo contado a partir de la notificación de la necesidad de una actuación al Adjudicatario, hasta la solución, ya sea Total o Parcial, del problema reportado. (abarca a todos los definidos anteriormente)

  La solución adoptada por el contratista en cada caso puede ser de dos tipos:

  - Solución Total: cuando el servicio ha sido repuesto y no queda pendiente acción alguna.
  - Solución Parcial: cuando el servicio ha sido repuesto, pero de forma provisional y/o quedan pendiente acciones tales como reparación del equipo averiado y reposición a su ubicación original o al stock de repuestos.

Gráfico explicativo de tiempos:



Dada la naturaleza diversa de los trabajos solicitados resulta difícil establecer un “Tiempo máximo de resolución “concreto para la resolución de cualquier tipo de incidencia.

En cualquier caso, el tiempo de resolución de la incidencia no podrá alargarse más allá de lo estrictamente necesario y en ningún caso se admitirán demoras debidas a falta de materiales de uso común o falta de capacidad humana o técnica.

Este tiempo no debe sobrepasar el “Tiempo máximo de resolución” fijado y que se especifica en la siguiente tabla de tiempos de referencia:

Criticidad (*)	Cobertura exigida	Tº Respuesta		Tº inicio “in situ”		Tº Resolución provisional (h. reales continuas)	Tº Resolución definitiva
		Horario Normal	Fuera Horario Normal	Horario Normal	Fuera Horario Normal		
Crítica	Horario normal y 24x7 (Bolsa de horas)	5’	20’	1 h.	1 h.	2 h.	30 días
Alta	Horario normal	5’	n/a	1 h.	n/a	4 h.	30 días
Media-Baja	Horario Normal	30’	n/a	2 h.	n/a	8 h.	30 días

(*) La criticidad del incidente identifica la situación de riesgo (crítica, alta, media-baja) para la seguridad de los servicios y negocio prestados por DSGV.

4.2.1.3 Nivel de servicio

La prestación de los servicios objeto del pliego conllevará el cumplimiento de una serie de niveles de servicio, y la aplicación de penalizaciones en caso de incumplimientos.

Los niveles de servicio aquí relacionados tienen el carácter de mínimos. Los licitadores pueden proponer Niveles de servicio superiores a los aquí indicados y/o prestaciones diferentes a las requeridas para mejorar la calidad del servicio prestado.

INDICADOR DE SERVICIO	DESCRIPCIÓN	VALOR OBJETIVO
Tiempo máximo de notificación incidente para su resolución	Tiempo que transcurre desde que una alerta se origina en el sistema, ésta es procesada (verificación de incidente categorizado) y se notifica a DSGV para su tratamiento.	*a definir por licitador
Tiempo máximo de notificación incidente categorizado como CRITICO para su resolución –	Tiempo que transcurre desde que una alerta se origina en el sistema, ésta es procesada, se confirma como CRITICA y se notifica a DSGV para su tratamiento.	*a definir por licitador
Eficacia en el diagnóstico de incidentes	% de incidentes correctamente categorizados	>95%
Eficacia en la notificación	% de falsos positivos	<5%
Tiempo máximo de respuesta para la aplicación correcta de medidas correctivas o recomendaciones de ajuste	Tiempo que transcurre desde que se valida por parte de DSGV la introducción de un cambio o ajuste sobre el servicio y se inician los trabajos asociados a ese cambio.	*a definir por licitador
Desviación máxima sobre los tiempos de entrega de informes de seguimiento periódicos	Desviación máxima permitida sobre los plazos de entrega acordados para los informes periódicos de seguimiento de servicio	<2d

INDICADOR DE SERVICIO (Mantenimiento correctivo)	VALOR OBJETIVO	
	Horario Normal	Horario Disponible
Tiempo de respuesta al aviso de Incidencias	98%	95%
Tiempo de inicio de actividad “in situ” (a modo de referencia, inicialmente no exigible)	98%	95%
Tiempo de resolución de Incidencias provisional	98%	95%
Tiempo de resolución de Incidencias definitivo	98%	95%

4.2.2 Plan de Calidad

El licitador deberá proponer un plan de calidad que garantice la correcta ejecución del servicio prestado y seguimiento del mismo.

Este plan debe 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 debidamente formalizado en el Plan de Transformación.

4.2.2.1 Plan de Seguimiento del servicio

Durante la ejecución del contrato se definirán conjuntamente una serie de **informes** con periodicidad acordada, que servirán para el seguimiento de la calidad del servicio ofrecido y para el conocimiento de las tareas desarrolladas.

Por parte del licitador se propondrá un conjunto de informes de partida que permitan cumplir esa función, así como el uso de herramientas que permitan una constante monitorización de la actividad desarrollada a través de **cuadros de mando**, con el objetivo de tener una imagen lo más real y actualizada posible, en cada momento, del estado del nivel de servicio y su evolución de forma que sirvan de ayuda en la toma de decisiones.

4.2.2.1.1 Comité de Seguimiento Técnico

- **ENTREGABLES POR PARTE DE LOS SERVICIOS.**
  - Informe mensual de seguimiento de servicio.
  - Seguimiento Incidencias y problemas.
  - Informes periódicos con el detalle y acciones realizadas en relación a los incidentes de seguridad.
  - informes periódicos sobre el estado de la ciberseguridad.
  - Informes a demanda sobre situaciones específicas de riesgo.
  - Actas de reuniones.

4.2.2.1.2 Comité de Gestión (Mensual)

- **ENTREGABLES POR PARTE DE LOS SERVICIOS.**

  Los entregables asociados al seguimiento del plan de calidad serán acordados y definidos en función de la propia evolución del servicio y el licitador deberá presentar un modelo de entregables propuesto. No obstante, podemos considerar inicialmente los siguientes:

  1. **Informe Mensual de seguimiento** deberá contener al menos:
     - Seguimiento de ANS indicando causas de incumplimientos si los hubiera.
     - Seguimiento incidencias graves y acciones tomadas.
     - Seguimiento de los proyectos en los que se participa.
     - Seguimiento de horas de bolsa: información de aviso, descripción de la asistencia, horas consumidas, horas restantes.
     - Acciones proactivas del servicio.
     - Planes de formación.

  2. **Actas de reuniones**

  3. **Informe Trimestral de estado de la infraestructura,** capacidad, disponibilidad, seguridad, riesgos asociados.

4.2.2.2 Plan de Transformación

El objetivo de este entregable es detallar las líneas maestras que van a gobernar la Evolución y Mejora Continua del Servicio y de las Infraestructuras e incluir indicadores objetivos que permitan evaluar su grado de cumplimiento.

Como parte de la oferta presentada, el licitador deberá presentar una propuesta de Plan de Transformación inicial que, al menos, deberá contener:

- Definición de factores críticos sobre los que se desarrollará el plan.
- Indicadores objetivos de seguimiento de la evolución y grado de cumplimiento del plan.

El plan definitivo, junto con los objetivos de cumplimiento se consensuarán con DSGV a partir de la propuesta final presentada por la adjudicataria.

4.2.3 Reuniones de seguimiento

La adjudicataria deberá asistir a las reuniones de seguimiento periódicas amén de las adicionales que se puedan establecer de forma discrecional.

Se establecen dos Comités:

4.2.3.1 Comité de Seguimiento Técnico

OBJETIVO	Revisión del día a día del servicio, incidencias, interrupciones de servicios, riesgos, seguimiento de los proyectos. En principio, se realizarán reuniones mensuales de seguimiento del servicio, que serán más frecuentes si las condiciones de realización del servicio lo requirieran
PARTICIPANTES DGSTI	Responsable del Servicio

4.2.3.2 Comité de Gestión (Mensual)

OBJETIVO	Seguimiento de la consecución de los objetivos del servicio
PARTICIPANTES DGSTI	■ Dirección de la DGTSI. ■ Jefes de Área. ■ Responsable del Servicio.

4.2.4 Metodología aplicable y Entorno tecnológico

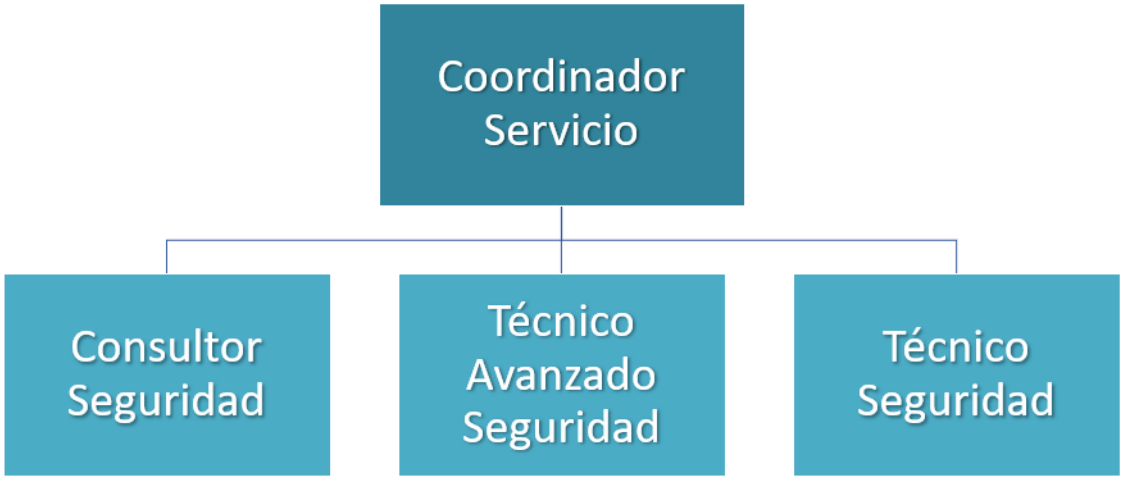
La empresa adjudicataria deberá presentar el conjunto de técnicas, herramientas y procedimientos para llevar a cabo todas las actividades planteadas en este expediente y cumplir los objetivos marcados por DSGV.

En la propuesta de metodología se deberá tener en cuenta el contexto en el que se desarrollarán los trabajos (Sector Público) y plantear qué datos prevé extraer y contrastar a partir de dicho contexto para conseguir la máxima adaptación a las necesidades de DSGV.

5 Planificación y Organización del Servicio

5.1 Organigrama del Servicio

El equipo de trabajo encargado de construir el entorno objeto de este contrato deberá respetar el siguiente organigrama:



Para llevar a cabo la organización del equipo, así como establecer, mantener, y ejecutar los procedimientos, con el objetivo de obtener un máximo rendimiento y calidad del servicio, la empresa adjudicataria deberá designar un **Coordinador del servicio**.

A nivel técnico se designarán un **Consultor** de seguridad, un **Técnico avanzado** de seguridad y un **Técnico** de seguridad.

Más adelante se describen los roles y dedicaciones.

5.1.1 Modelo de relación

El licitador presentará un marco de actuación durante la prestación del servicio en cuanto a niveles de interlocución y relaciones entre la DGTSI y los responsables del servicio, identificando cuáles serán los Órganos de Control del servicio y las funciones de cada uno de ellos.

5.2 Equipo de trabajo

5.2.1 Roles y ámbito de responsabilidad

- **Coordinador del servicio**

El Coordinador del servicio deberá disponer de un perfil adecuado al nivel de exigencia técnica exigido en las condiciones del pliego y se encargará de la relación profesional entre el proveedor y la DGTSI.

Tendrá las siguientes funciones:

- Controlar los Procesos de Gestión ITIL y establecer los indicadores de control de gestión y los informes de gestión.
- Mantener y actualizar con la DGTSI los Acuerdos de Niveles de Servicio (ANS).
- Auditar el Sistema de Calidad y los Procesos de Gestión, estableciendo los planes de mejora necesarios.
- Iniciar el periodo de transición del Servicio coordinándose con el adjudicatario actual, supervisando en colaboración con la DGTSI, la transferencia de información, datos y experiencia del servicio actualmente en operación.
- Coordinar las funciones del servicio y la correcta ejecución de los procesos de gestión.
- Dicha figura se encargará de comunicar al personal que vaya a prestar servicios en la DGTSI, las Normas generales de Seguridad y Salud para contratas y subcontratas, así como de certificar que dicho personal ha recibido y conoce dicho documento y que se compromete a cumplir y a hacer cumplir a su personal la normativa de seguridad y salud vigente durante el tiempo de ejecución del contrato. En caso de incumplimiento de cualquiera de estas obligaciones la DGTSI se reserva el derecho de resolver los contratos que tenga vigentes con la empresa contratada.

- **Consultor de seguridad**

Perfil altamente cualificado en materia de seguridad global, con un conocimiento transversal de la seguridad, y altamente especializado en ciertas tecnologías que le permite participar en la operativa y en la mejora continua de los Servicios de Seguridad.

- **Técnico avanzado de seguridad**

Perfil especializado de Seguridad con la experiencia descrita en el PCP, conocimientos globales y transversales de seguridad que le permita ejercer, aparte de las tareas operativas más avanzadas, tareas más específicas de operaciones de seguridad y mejora continua de los Servicios de Seguridad.

- **Técnico de seguridad**

Perfil de Seguridad con una orientación principalmente a la operación y mejora continua de los Servicios de Seguridad, pero sin perjuicio de participar ocasionalmente, con la tutela del técnico avanzado, en labores propias de éste.

5.2.2 Dimensionamiento y dedicación

Los recursos con los que se dimensione el servicio dependerán de las ofertas presentadas, pero se considera, y por tanto es un requisito mínimo, que para cubrir los roles planteados al menos es necesario que el equipo tenga la capacidad establecida en la siguiente tabla para cada uno de los roles, cumpliendo para ello con la dedicación indicada durante la ejecución del contrato:

	% Dedicación	**Año 1**	**Año 2**	**Total contrato**
Coordinador	**5%**	85 horas	85 horas	**170 horas**
Consultor	**50%**	850 horas	850 horas	**1.700 horas**
Técnico Avanzado Seguridad	**100%**	1.700 horas	1.700 horas	**3.400 horas**
Técnico Seguridad	**100%**	1.700 horas	1.700 horas	**3.400 horas**

Con la intención de fomentar la estabilidad del grupo de trabajo y el mantenimiento de la calidad global del servicio, a lo largo de la vigencia del contrato, podrán imponerse penalizaciones por excesiva rotación de los componentes presentados en la oferta técnica, reservándose DSGV, en último término, el derecho a su rescisión por incumplimiento reiterado. En este mismo sentido, y consensuado con DSGV, se fomentará la promoción interna en caso de bajas laborales de recursos adscritos al servicio.

5.2.3 Lugar de trabajo

En este contrato específicamente se prestará en la sede que el DSGV tiene en Erandio (Bizkaia):

Larrauri-Mendotxe Bidea, 18

48950 Erandio

Bizkaia

5.3 Carga de trabajo

Dentro de la oferta, basándose en los requerimientos expuestos en el pliego y de su enfoque del servicio, deberá hacer una propuesta base, que en el transcurso de la prestación del servicio podrá modificarse dependiendo de las necesidades.

En caso de producirse alguna variación, la DGTSI comunicará al menos con 1 mes de antelación las características de la misma.

5.4 Actualización tecnológica

Se debe garantizar la actualización de los conocimientos en los componentes del servicio. Esta actualización de conocimientos debe ser evaluable por la DGTSI.

Tal y como se establece en el PCP, el equipo técnico debería estar certificado por los fabricantes o bien demostrar experiencia de al menos dos años en proyectos de los entornos más significativos definidos en el Anexo reservado *Entorno tecnológico de Ciberseguridad*. Asimismo, en caso de evolución del escenario de ciberseguridad del DSGV, si en el transcurso del contrato se estableciera un nuevo entorno tecnológico estratégico, deberá aportarse el plan para cumplir con las condiciones solicitadas.

La DGTSI se reserva la facultad de solicitar, en cualquier momento, antes o después de la adjudicación y durante el curso de los trabajos, cualquier otro documento complementario, en orden a la comprobación de cuantos datos haya ofrecido la empresa licitadora, tanto respecto a sí misma como con respecto al personal propuesto.

5.4.1 Plan de Formación y actualización tecnológica

Es responsabilidad del adjudicatario garantizar la formación adecuada del personal del mismo asignado al equipo de trabajo.

El Adjudicatario deberá garantizar y mantener un equipo que asegure el soporte y el correcto funcionamiento para cumplir con el nivel de servicio acordado y planteará un plan de formación para el equipo de trabajo formado. Este plan será valorado por la DGTSI.

5.5 Horario del servicio

El desarrollo de las funciones con carácter presencial se realizará dentro del horario habitual:

- Lunes a jueves: 8h a 18h
- Viernes y jornada intensiva: 8h a 15h

Durante el horario denominado normal o habitual se debe garantizar el nivel de servicio presencial, sin discontinuidades.

En situaciones de crisis o de intervenciones planificadas DSGV podrá solicitar la extensión de la disponibilidad del servicio a un horario 24x7 dentro del marco de este contrato, tal y como se describe en el apartado 4.1.6 Bolsa de horas.

Dado que la extensión de la jornada puede exceder de las horas/jornadas que cada individuo deba cumplir de acuerdo con sus condiciones laborales, se elaborará un plan que deberá ser aprobado por la DGTSI para cubrir el horario habitual en toda su extensión con unos mínimos presenciales durante el periodo dedicado para la comida, de forma que siempre esté disponible alguien capacitado para prestar el servicio solicitado.

El adjudicatario tomará las medidas que fueran precisas para asegurar que tiene suficiente personal localizable y puede atender cualquier incidencia dentro del periodo de atención y con el tiempo de respuesta requerido en el contrato.

5.5.1 Requerimientos en horario habitual

El adjudicatario deberá proporcionar un teléfono de contacto único que permita contactar con los técnicos asociados al servicio.

El adjudicatario deberá asegurar que ese teléfono será atendido en todo momento por alguno de los técnicos asociados al servicio durante el horario habitual.

5.5.2 Requerimientos fuera del horario habitual

Fuera del horario habitual el tipo de atención podrá ser:

- Soporte de atención telefónica.
- Acceso remoto vía RAS/VPN.
- Presencia in situ.

Las operaciones y asistencias que requieran los servicios objeto del contrato descritos en el apartado 4.1.6 Bolsa de horas, podrán solicitarse fuera del horario habitual en horario nocturno y/o festivo.

Entre dichas asistencias, las intervenciones planificadas se planificarán de acuerdo con el personal técnico de DSGV en un horario convenido y que menos afecte al funcionamiento de los servicios.

El adjudicatario deberá disponer de los medios necesarios para asegurar las solicitudes serán atendidas en todo momento por alguno de los técnicos asociados al servicio fuera del horario habitual.

5.6 Planes de Transición

En la oferta debe presentar claramente tanto el Plan de Transición de entrada de servicio como la devolución del servicio al finalizar el contrato.

5.6.1 Plan de Transición de entrada al Servicio

El adjudicatario debe especificar los recursos de gestión específicos que aportará en las Fases de Transición y Devolución, así como los que tiene que aportar la DGTSI.

Esta fase pondrá un especial énfasis en la gestión del cambio de todos los aspectos implicados, con especial foco en la información a los usuarios internos y finales de los cambios en las formas de funcionamiento de los servicios, y formación de los proveedores y usuarios en los aspectos que corresponda.

Asociados a la realización de esta fase se producirán documentaciones y actuaciones de formación dirigidas a los nuevos adjudicatarios de los servicios contratados.

El proceso de transición para asumir el control del servicio será por cuenta del adjudicatario.

5.6.2 Plan de Transición de salida del Servicio

El adjudicatario estará obligado, durante el periodo anterior o posterior a la finalización del contrato, 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.

5.7 Garantía de la disponibilidad del Servicio

En todo caso y circunstancia, la adjudicataria debe obligarse a garantizar la disponibilidad del servicio. Para ello debe reflejar la estrategia, políticas o mecanismos de actuación habilitados frente a contingencias materiales provocadas por desastres, emergencias, falta de respuesta en el plazo, etc. y de recursos humanos que puedan poner en riesgo la prestación óptima del servicio a fin último de garantizar su prestación y calidad en cualquier circunstancia.

5.7.1 Plan de Continuidad de Negocio y Plan de Contingencia

A continuación, se enumeran los requisitos que los proveedores han de cumplir para asegurar la prestación del servicio. Se dividirán en requisitos obligatorios y requisitos opcionales:

- Requisitos obligatorios:
  - El proveedor deberá disponer de un plan de continuidad de negocio que asegure la provisión del servicio en modo contingencia, ante cualquier caso que imposibilite la ejecución normal (o preestablecida) del servicio. Este plan deberá tener identificadas a todas las personas y roles necesarios para su correcta ejecución.
  - El proveedor deberá contar con un plan de pruebas (simulacros) exhaustivo que cubra todos los aspectos de continuidad vinculados a la provisión del servicio. Estas pruebas estarán programadas y su ejecución estará acompañada de la generación de evidencias necesaria para poder aportarlo ante una puntual solicitud de DSGV o para su revisión en las auditorías a proveedores.
  - El proveedor deberá contar, si procede, con planes de mejora derivados de las pruebas realizadas.
  - Se deberá disponer de un canal de comunicación especial en el que el proveedor informará a DSGV de manera urgente de cualquier incidente que active el plan de continuidad del servicio e informará periódicamente mientras se encuentre en situación de contingencia. Así mismo, se comunicará a DSGV el final de la situación de contingencia y cuando el servicio se encuentre, de nuevo, en funcionamiento normal.

- Requisitos opcionales:
  - Disponer de una política de continuidad del proveedor que esté alineada con el servicio prestado a DSGV.
  - Disponer de un análisis de impacto en el negocio (BIA) que sirva como base para el plan de continuidad del servicio. Este BIA debería contemplar el grado de afección que, sobre el servicio a DSGV, tendría un incidente disruptivo a nivel de la empresa proveedora.

Teniendo lo anterior en cuenta, como parte de la oferta el licitador deberá presentar un plan de contingencia que, al menos, y sin implicar que sean las únicas situaciones de contingencia que se puedan dar, deberá contener su propuesta sobre:

- Indisponibilidad, planificada o no, de la utilización de los emplazamientos físicos habitualmente utilizados para la entrega del servicio (oficinas, etc.).
- Indisponibilidad, planificada o no, de elementos tecnológicos habitualmente utilizados para la entrega del servicio (redes de comunicaciones, hardware, software, licencias, etc.).
- Indisponibilidad por brechas de seguridad (malware, campañas de phishing, etc.).
- Indisponibilidad, planificada o no, de elementos auxiliares habitualmente utilizados para la entrega del servicio (vehículos, maquinaria, herramientas, etc.).
- Bajas médicas no planificadas de personal asociado al servicio por un período superior a una semana.
- Bajas médicas no planificadas de personal asociado al servicio, de carácter indefinido o permanente.
- Bajas laborales no planificadas, bien de carácter temporal o permanente.
- Bajas laborales planificadas, bien de carácter temporal o permanente.
- Ausencias planificadas por periodos vacacionales.

También se deberá indicar la forma de garantizar, en todo momento, la disponibilidad de un equipo mínimo adecuado para la prestación óptima del servicio y el método propuesto para la asunción automática de responsabilidades de los roles clave del servicio (Coordinador del Servicio, Consultor y Técnicos de seguridad) ante indisposiciones, bajas médicas o laborales, vacaciones…etc.

5.8 Ejecución del contrato

El adjudicatario será responsable del correcto desarrollo de los trabajos y proyectos relacionados, de acuerdo a los requerimientos del presente pliego.

5.8.1 Supervisión del contrato

La actuación del contratista será supervisada por el técnico responsable del contrato por parte de la DGTSI. A su vez el contratista designará un responsable de la empresa.

El técnico responsable de la DGTSI tiene las más amplias atribuciones, y sus órdenes e instrucciones serán inmediatamente ejecutivas.

El responsable de la empresa adjudicataria y el técnico de la DGTSI mantendrán reuniones periódicas para revisar la situación y desarrollo de los servicios.

El adjudicatario deberá proporcionar la información requerida por la DGTSI para conocer la situación y desarrollo de las actividades solicitadas. Las discrepancias sobre el desarrollo de los servicios serán resueltas al nivel más elevado de representación.

El incumplimiento por parte del adjudicatario de lo establecido en el presente pliego de Bases Técnicas y cuando dicho incumplimiento sea reiterativo o se refiera a órdenes que le hayan sido impartidas por escrito y advirtiéndole que son esenciales para el buen fin del contrato, se considerará causa de resolución del mismo.

5.8.2 Inicio del servicio

Como primera actividad asociada al contrato se establecerá una reunión de “lanzamiento del servicio” entre el Adjudicatario y DSGV, en el cual se identificarán los interlocutores de ambas partes.

En esta reunión además se definirán el resto de las condiciones que afectan a la ejecución del servicio, si existiesen, y se establecerán los procedimientos de trabajo a ejecutar, en base a la propuesta presentada, que deberá ser aprobado por DSGV.

5.8.3 Registro y control de actividades

Los técnicos asignados por el adjudicatario al contrato actuarán bajo la supervisión de los representantes del DSGV que les sean asignados.

El responsable de la empresa adjudicataria y el técnico de DSGV mantendrán reuniones periódicas para revisar la situación y desarrollo de los servicios.

Los trabajos se realizarán con el alcance y objetivos que determine el personal de DSGV.

Como parte del contrato, el adjudicatario estará obligado a dar total cumplimiento a las condiciones que al efecto de seguimiento y control de actividades establezca DSGV u organismos por él designados.

Asimismo, el adjudicatario se compromete a cumplir convenientemente con los registros que a efectos de control de presencia disponga DSGV en sus instalaciones.

5.8.4 Asignación del Personal

La Administración se reserva la facultad de solicitar, en cualquier momento, antes o después de la adjudicación, y durante el curso de los trabajos, cualquier otro tipo de documento complementario, en orden a la comprobación de cuantos datos haya ofrecido la empresa adjudicataria, tanto con respecto a sí misma, como con respecto al personal que proponga para la prestación de los servicios.

No obstante, la designación de técnicos realizada por la empresa adjudicataria podrá ser modificada, a simple petición de la Administración, y en este caso, el adjudicatario se obliga a proponer otras personas, de idéntica categoría, y con circunstancias personales y profesionales, al menos, idénticas a las inicialmente propuestas.

La elección por la Administración de esas u otras personas no alterará en ningún caso el precio ofertado por la empresa adjudicataria.

La empresa adjudicataria se compromete a adoptar las medidas necesarias orientadas a prevenir la rotación y, en cualquier caso, a minimizar el impacto que pueda ocasionar en la Administración y en el propio servicio.

Cualquier cambio en los integrantes del equipo de trabajo deberá ser conocido y aprobados por la Administración.

6 ANEXO I – Normas de Seguridad relativas a los sistemas de información

6.1 Normas básicas

El adjudicatario se compromete a cumplir la política de Seguridad de la Información del Departamento de Seguridad del Gobierno Vasco y todas las normativas y procedimientos aplicables en el contexto del servicio.

El Departamento de Seguridad del Gobierno Vasco tendrá derecho a llevar a cabo auditorías de las actividades del equipo de trabajo del adjudicatario para asegurarse de que la prestación de los servicios se realiza de acuerdo a lo establecido en el presente pliego. Todo el material e información requerida para dichas inspecciones estará disponible sin restricciones.

La información facilitada para abordar los trabajos no se aplicará ni utilizará con una finalidad diferente a la que es objeto de este pliego ni el prestador de servicio la comunicará, ni siquiera a efectos de su conservación a terceros.

El adjudicatario y el personal a su cargo están obligados a guardar secreto y absoluta confidencialidad respecto de la información que les sea confiada en virtud del servicio prestado.

El prestador del servicio deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de la información y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

- No introducir software informático ajeno al Departamento de Seguridad.
- No difundir ni publicar los sistemas de seguridad existentes o previstos.
- No revelar la información obtenida de los sistemas de información del Departamento de Seguridad, ni la documentación que se le suministre o la que pudiera tener acceso en el desempeño de sus funciones, con independencia del soporte en que se encuentre contenida.
- Acceso exclusivo a la información necesaria para el desempeño de las funciones encomendadas.
- Utilizar exclusivamente la password-clave a él asignada y adquirir el compromiso de actuar de forma cuidadosa para que nadie conozca su palabra de paso.
- Utilizar adecuadamente y de forma cuidadosa los sistemas de seguridad implantados, de forma que se respeten y mantengan los niveles de seguridad.

Además, el adjudicatario adquirirá los siguientes compromisos, que a continuación se describen en cuanto a materia de seguridad se refiere:

- Los equipos conectados a la Intranet del Departamento de Seguridad no podrán conectarse a ningún sistema informático o de telecomunicaciones ajeno al Departamento.
- Los equipos o sistemas que por su actividad requieran conexión a servicios externos al Departamento deberán estar aislados, es decir, separados física y lógicamente de la red informática del Departamento de Seguridad.
- Esta expresamente prohibido la instalación de módems (o similar) en equipos (PCs, Servidores, etc.) conectados a la red del Departamento de Seguridad.

El personal del adjudicatario se comprometerá formalmente a conocer y cumplir todas las condiciones y obligaciones contempladas en la prestación del servicio. De forma específica, se comprometerá a guardar secreto y confidencialidad respecto a la información que le sea confiada incluso una vez finalizada su participación en el proyecto.

6.2 Acceso y protección de datos

El adjudicatario quedará expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en este Pliego de Prescripciones Técnicas, ni tampoco ceder a otros ni siquiera a efectos de conservación.

A estos efectos, deberán establecerse las máximas cautelas en el acceso a los datos. Cualquier infracción en este sentido será calificada como grave y será causa de resolución del contrato, sin perjuicio de las responsabilidades penales, o de otro tipo, en que se puedan incurrir.

El adjudicatario quedará obligado al cumplimiento de lo dispuesto en la Ley orgánica 15/1999 de 13 de diciembre sobre protección de datos de carácter personal, y en el correspondiente reglamento de desarrollo de la LOPD (aprobado por real Decreto 1720/2007, de 21 de diciembre, en vigor desde el 19 de abril de 2008); y especialmente en lo indicado en su artículo número 12, que a continuación se transcribe:

"Artículo 12.- Acceso a los datos por cuenta de terceros.

1.- (…)

2.- La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el Artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3.- Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruido o devueltos al responsable del tratamiento, al igual que cualquier otro soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4.- En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que se hubiera incurrido personalmente."

A tal fin, y conforme el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, el oferente incluirá en su oferta Memoria Descriptiva de las medidas de seguridad que adoptarán para asegurar la disponibilidad, confidencialidad e integridad de los datos manejados y de la documentación facilitada.

6.3 Propiedad intelectual

Los derechos de propiedad intelectual relacionados con el trabajo realizado pertenecerán a la Administración. Cualquier producto o subproducto derivado del mismo no podrá ser utilizado para otros fines fuera del ámbito que le corresponda, sin el permiso expreso por escrito de la Administración.

Asimismo, todos los entregables que deban facilitarse a los Departamentos y Organismos Autónomos del Gobierno Vasco (salvo las ofertas previas) únicamente deberán llevar como logotipo o señas de identidad el escudo del Gobierno Vasco o logotipos aceptados por el propio Departamento y Organismo Autónomo.

El Contratista se verá también obligado a guardar las normas vigentes sobre, Copyright, propiedad intelectual y documentación clasificada o de difusión restringida que, por necesidades del contrato, se vea obligado a manejar.