PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE SEGURIDAD DE LOS SISTEMAS MICROINFORMÁTICOS DE BIDEGI

CLAVE: 2025JKIR0042

Fecha: Noviembre 2025

Índice

0. OBJETO DEL CONTRATO 1
1. ANTECEDENTES Y OBJETO DEL DOCUMENTO 2
2. INVENTARIO SISTEMAS MICROINFORMÁTICOS 3
3. ALCANCE DEL SERVICIO 4
3.1. SERVICIO DE CONECTIVIDAD A INTERNET 4
3.2. SERVICIO DE ALMACENAMIENTO EN LA NUBE 4
3.3. RENOVACIÓN LICENCIAS MANTENIMIENTO DE FIREWALL 5
3.4. LICENCIAS XDR 5
3.5. SERVICIO DE VIGILANCIA DE EVENTOS 6
3.6. SERVICIO DE SOPORTE TÉCNICO 7
3.7. AUDITORÍA DE SEGURIDAD 7
3.8. OTRAS NECESIDADES 8
4. METODOLOGÍA DE GESTIÓN DEL SERVICIO 9
4.1. FASE DE TRANSICIÓN 9
4.2. FASE DE EJECUCIÓN DEL SERVICIO 9
4.3. FASE DE DEVOLUCIÓN DEL SERVICIO 10
5. PLAZO DE EJECUCIÓN 11
6. PRESUPUESTO Y CERTIFICACIÓN 12

0. OBJETO DEL CONTRATO

El objeto del presente expediente es la contratación de un servicio de seguridad para los sistemas microinformáticos que dan servicio a las oficinas de BIDEGI situadas en Zarautz, así como los servicios para garantizar la continuidad de negocio ante incidentes.

Este servicio de seguridad será complementario al servicio de mantenimiento de los sistemas microinformáticos, regulados a la fecha de redacción del presente documento por el expediente SERVICIO DE MANTENIMIENTO SISTEMAS MICROINFORMATICO DE BIDEGI 2021JKIR0015.

De esta forma el expediente asociado al mantenimiento microinformático tendrá como fin el mantenimiento del día a día de la microinformática de BIDEGI, asistiendo a las necesidades operativas que surjan de acuerdo a lo regulado en el tercer expediente. Por su parte el presente expediente de seguridad de los sistemas microinformáticos velará por garantizar las conexiones seguras y garantizar la continuidad de negocio de acuerdo a como se regula en el presente pliego de prescripciones técnicas.

Igualmente sería complementario al servicio de telecomunicaciones, igualmente vigente en un tercer expediente.

1. ANTECEDENTES Y OBJETO DEL DOCUMENTO

Los sistemas asociados a la tecnología de la información están asumiendo cada vez más relevancia en las organizaciones, convirtiéndose en un elemento crítico para el desarrollo de las actividades ordinarias.

BIDEGI Gipuzkoako Azpiegituren Agentzia / Agencia Guipuzcoana de Infraestructuras S.A., empresa pública creada en el año 2003 por la DIPUTACIÓN FORAL DE GIPUZKOA no es ajena a esta realidad, viéndose progresivamente acrecentadas sus necesidades de soporte microinformático, tanto en lo que a material se refiere como de soporte o asistencia.

En lo referente a la seguridad de la información y continuidad de negocio, hasta la fecha se ha venido realizando por la empresa que realizaba el mantenimiento de los sistemas microinformáticos de BIDEGI, como parte de los trabajos de mantenimiento que realizaban. Sin embargo debido a la mayor sofisticación de la infraestructura, la mayor dependencia de los sistemas IT, y por la ocurrencia de ciertos incidentes en 2024 se determinó la necesidad de un servicio más específico, reforzando las medidas de seguridad, así como las vinculadas a la continuidad de negocio asociadas con las comunicaciones.

En este escenario en 2024 se contrató como medida de choque inicial un expediente de SERVICIOS DE SEGURIDAD DE LA RED INFORMÁTICA DE BIDEGI S.A. clave 2024JKZU0025, que consistió en la migración del Firewall obsoleto previamente existente a dos Firewall redundados Fortinet FG-70, la instalación de una segunda línea de conexión a internet con fibra y con redundancia 4G, un servicio de backup en la nube ante posibles problemas (p.ej. fuego) en el CPD de BIDEGI y la instalación de un SOC sencillo para la monitorización del Firewall.

Estando próximo el vencimiento del anterior servicio, y constatando la solvencia de la solución, mediante el presente expediente se desea renovar el servicio, ajustando el mismo con la experiencia adquirida en estos meses de servicio, de tal forma que se garantice la máxima seguridad de la información y máxima continuidad de negocio en el servicio microinformático de BIDEG

2. INVENTARIO SISTEMAS MICROINFORMÁTICOS

Los sistemas microinformáticos de BIDEGI objeto del presente expediente son unos usuales de una oficina, de acuerdo a lo que se describe en las siguientes líneas.

No son objeto de los sistemas microinformáticos objeto del presente expediente ni la web de BIDEGI, ni el resto de infraestructura IT industrial de las carreteras gestionadas por BIDEGI, siendo estos objeto de terceros expedientes. Únicamente es del objeto del presente expediente los sistemas microinformáticos de la oficina de BIDEGI, cuyo alcance en la actualidad es el siguiente:

- Servidores:
  - 2 Servidores Hpe proliant DL360 gen10 que dan servicio a 8 servidores virtuales.
  - 1 Cabina de disco HPE MSA1060-ENCL-SFF.
- Equipamiento de red:
  - 2 Firewall Fortinet FG-70G.
  - 2 switches D-link DGS-1510-52XMP.
  - 2 Bases wifi Aruba IAP215RW.
  - 1 NAS SynologyRS1221+.
  - 1 NAS NetGear ReadyNAS 2120 v2
- Equipos ofimáticos:
  - 15 portátiles.
  - 24 pc’s de sobre mesa.
  - 2 Pantallas multitáctil.
  - 6 impresoras de red.
  - 6 scanner y otros dispositivos multiservicio.

Nótese que los equipos indicados son aproximados, pudiendo reducirse o ampliarse a lo largo de la vida del contrato.

Entre otros tampoco están incluidos:

- Centralita telefónica siendo esta virtual y externalizada.
- Servicio de correos externalizado con office 365.
- Servicio web externalizado en un hosting de IZFE.
- Dominios en Arsys

3. ALCANCE DEL SERVICIO

Es objeto del alcance del servicio:

- Servicio de conectividad a internet.
- Servicio de almacenamiento para backup.
- Renovación licencia de mantenimiento Firewall.
- Licencias de XDR.
- Servicio de vigilancia de eventos (SOC).
- Servicio de soporte técnico.
- Auditoría interna y externa bienal.
- Otros alcances en función de necesidades.

En las líneas siguientes se detalla el alcance esperado de estos servicios.

3.1. SERVICIO DE CONECTIVIDAD A INTERNET

Los servicios de telecomunicaciones son provistos por Euskaltel, dentro del contrato marco que tiene vigente la DIPUTACIÓN FORAL DE GIPUZKOA y al que BIDEGI está adherido.

Sin embargo y con el fin de garantizar la continuidad de negocio y como línea segura para la configuración de Firewall se deberá proveer de una conexión a internet mediante fibra óptica segura, con un ancho mínimo de 300Mb simétricos.

Esta conexión deberá disponer de una conexión de respaldo en 4G.

Deberá incluir 2 IP’s públicas fijas con servicio antiddos.

Con objeto de garantizar la redundancia, esta línea deberá ser de un operador DIFERENTE al que actualmente se tienen contratado dentro del servicio de Telecomunicaciones del previamente citado acuerdo marco.

3.2. SERVICIO DE ALMACENAMIENTO EN LA NUBE

Adicionalmente a las copias de seguridad que se realizan de manera local, se requiere disponerse de un sistema de almacenamiento en la nube, que acepte copias de seguridad mediante Veeam Backup del conjunto de máquinas virtuales.

Todas las transferencias de datos entre el origen y destino del backup se realizará mediante conexiones cifradas de extremo a extremo, AES de 256 bits, y el backup se guardará encriptado.

ENS a nivel medio o alto y la infraestructura deberá albergarse en el Estado español.

Deberá disponerse de una capacidad de almacenamiento de 24TB ampliables a lo largo del expediente si el almacenamiento creciera con el tiempo.

3.3. RENOVACIÓN LICENCIAS MANTENIMIENTO DE FIREWALL

En la actualidad los dos Firewall instalados a principios de 2025 cuenta con soporte de fabricante, el cual vence en marzo de 2026. Es objeto de este servicio la renovación de estas licencias de mantenimiento de los dos Firewall FG-70G del servicio Unified Threat Protection (UTP) o similar que incluya IP, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service an Forticare Plus.

Este servicio deberá estar expresamente contratado con el fabricante del Firewall.

Incluirá las 10 licencias de VPN con doble factor de autentificación instaladas.

3.4. LICENCIAS XDR

La plataforma de XDR a suministrar deberá proveer de servicios de detección y respuesta ampliada, diseñada para recopilar, correlacionar y analizar telemetría de múltiples vectores de seguridad: endpoints, servidores, Firewall, correo electrónico, nube y red. Su objetivo es ofrecer una visión unificada del entorno de amenazas, lo que permite detectar ataques sofisticados y multietapa.

Gracias a esto, el sistema de monitorización deberá poder identificar e incidentes permitiendo optimizar la respuesta y simplificar la gestión.

El sistema XDR deberá incluir capacidades de respuesta automatizada, permitiendo la contención inmediata de incidentes mediante acciones como aislamiento de endpoints, bloqueo de procesos, revocación de credenciales o segmentación temporal.

Asimismo, las licencias XDR deberán incluir acceso a inteligencia de amenazas actualizada proveniente de fuentes globales y del fabricante, garantizando la identificación temprana de campañas activas, indicadores de compromiso (IoC) y tácticas, técnicas y procedimientos (TTP).

La solución deberá cumplir con estándares de privacidad y normativas vigentes, garantizando la protección de datos almacenados y procesados. La plataforma deberá permitir escalabilidad acorde al crecimiento de la organización, manteniendo un rendimiento óptimo en la ingestión, análisis y almacenamiento de eventos.

La instalación de las licencias en los terminales y servidores locales en BIDEGI sí será realizado por el servicio de mantenimiento de microinformática pero sí será objeto de este contrato 1) proveer de las licencias necesarias, 2) la configuración de la solución incluyendo la plataforma

central (y hardware si fuera necesario) 3) realizar una guía de instalación 4) el mantenimiento y evolución de la solución.

Dentro del marco del presente contrato se deberán proveer de 40 licencias para equipos PC's y 10 licencias para servidores.

Este número de licencias podrá ser ampliado dentro del marco del presente contrato.

3.5. SERVICIO DE VIGILANCIA DE EVENTOS

Se deberá proveer de un Servicio de Operación del Centro de Seguridad (SOC) en modalidad 24x7x365, encargado de la monitorización continua de todos los activos protegidos mediante soluciones XDR y del Firewall perimetral. Este servicio deberá incluir la vigilancia constante de alertas, análisis de eventos de seguridad, identificación temprana de amenazas y correlación multivector, garantizando la revisión proactiva de comportamientos anómalos tanto en endpoints como en la infraestructura de red. El SOC deberá disponer de herramientas SIEM o equivalentes que permitan correlacionar la telemetría recibida de los sistemas XDR y del Firewall.

El servicio deberá contemplar gestión completa de incidentes, abarcando la clasificación, priorización, investigación y contención de posibles amenazas. Se exigirá que el SOC aplique procedimientos normalizados basados en buenas prácticas internacionales (como MITRE ATT&CK o NIST), y que realice acciones de respuesta remota autorizadas, tales como aislamiento de máquinas comprometidas, bloqueo de direcciones IP, reglas temporales en el Firewall, análisis forense inicial y recomendaciones de remediación. Asimismo, se requerirá que se generen informes detallados de cada incidente, incluyendo línea temporal, impacto potencial, análisis de causa raíz y medidas de mitigación aplicadas.

El Adjudicatario deberá ofrecer mantenimientos preventivos y revisiones periódicas, incluyendo el análisis del estado de las políticas XDR, la revisión del rendimiento de los agentes instalados en endpoints y servidores, así como auditorías de la configuración del Firewall para asegurar su alineación con las políticas de seguridad de la organización.

Finalmente, se solicitará la entrega de informes periódicos de ciberseguridad, con frecuencia bimensual, que incluyan métricas clave (KPI), estado de riesgos, tendencias de amenazas, cumplimiento de SLA y recomendaciones de mejora continua.

3.6. SERVICIO DE SOPORTE TÉCNICO

La empresa adjudicataria, además de implantar la solución requerida, deberá asistir en todo lo relativo a los incidentes detectados en función de lo establecido en los acuerdos de nivel de servicio del presente pliego de prescripciones técnicas.

En especial deberá atenderse a peticiones de cambio en la reglas de Firewall, habilitar o deshabilitar VPN, y en general cualquier otra actuación sobre el Firewall dentro de la misma jornada laboral.

Igualmente incluirá soporte de mantenimiento del equipamiento instalado así como asistencia técnica para la configuración o dudas de funcionamiento de cualquiera de los servicios.

La empresa adjudicataria deberá especificar un teléfono de contacto con el equipo técnico asignado al servicio.

3.7. AUDITORÍA DE SEGURIDAD

De forma bienal, una dentro del primer año de ejercicio del contrato y otra en el tercer año antes de la finalización del mismo se deberá realizar una auditoría de seguridad.

Esta auditoría deberá evaluar tanto las vulnerabilidades internas, externas, como recomendaciones de carácter de gestión de la seguridad. También deberá incluir al menos una campaña de concienciación en materia de seguridad de la información.

De esta forma la auditoría abarcará la realización de un **análisis externo de vulnerabilidades**, dirigido a identificar debilidades explotables desde internet en los sistemas, servicios y direcciones IP públicas de la organización. Este análisis incluirá la enumeración de servicios expuestos, detección de configuraciones inseguras, versiones obsoletas, fallos de cifrado y posibles vectores de intrusión que puedan comprometer la superficie pública de ataque.

De forma complementaria, se llevará a cabo un **análisis interno de vulnerabilidades** sobre la infraestructura ubicada dentro de la red corporativa, incluyendo servidores, estaciones, dispositivos de red y servicios internos. El objetivo será identificar fallos de configuración, software sin actualizar, permisos inadecuados, aplicaciones vulnerables y cualquier elemento que pueda facilitar movimientos laterales o escaladas de privilegios por parte de un atacante.

La auditoría deberá combinar el uso de herramientas automáticas de escaneo combinadas con acciones manuales.

Por cada auditoría se generará un informe final que contendrá la descripción detallada de vulnerabilidades encontradas, evidencias técnicas, criticidad asociada y recomendaciones de remediación priorizadas según impacto y probabilidad. Este informe se acompañará de una

presentación ejecutiva con las conclusiones de la auditoría, así como propuestas de mejora para reforzar la postura de seguridad global de la organización, asegurando que las acciones recomendadas sean viables y alineadas con las buenas prácticas del sector.

El alcance de una campaña de concienciación en ciberseguridad comprenderá el diseño y ejecución de acciones formativas dirigidas a todo el personal de la organización, orientadas a mejorar sus hábitos y capacidades frente a amenazas digitales. La campaña incluirá contenidos sobre buenas prácticas, identificación de correos de phishing, gestión segura de contraseñas, uso adecuado de dispositivos y protección de la información, empleando formatos variados como sesiones formativas, materiales digitales y ejercicios prácticos. Asimismo, se contemplará la evaluación del nivel de sensibilización mediante pruebas o simulaciones, con el objetivo de medir la efectividad de la campaña y reforzar conductas seguras.

Estas auditorías las deberá realizar un agente independiente, de tal forma que se garantice la transparencia de las auditorías, tanto en lo que al presente servicio se refiere, al servicio de mantenimiento y/o al uso realizado de los recursos informáticos por los usuarios.

3.8. OTRAS NECESIDADES

Adicionalmente a los servicios expuestos en las líneas precedentes, es posible que en el transcurso del periodo de vigencia del presente contrato sea necesario ampliar algún servicio.

A modo meramente ilustrativo se incluyen las acciones que se consideran puedan ser necesarias:

- Ampliación de doble factor de autentificación Fortitoken Mobile
- Ampliación de espacio de almacenamiento en la nube
- Ampliación de licencias XDR

El abono de estas partidas se realizará en función de necesidad y previa autorización por el Director de Contrato de BIDEGI.

4. METODOLOGÍA DE GESTIÓN DEL SERVICIO

Dentro de la metodología del servicio se establecen tres fases claramente diferenciadas:

- Fase inicial de “transición y arranque del servicio”.
- Fase de “ejecución de servicio”
- Fase final de “devolución”

Si bien el Licitante para cada una de las fases deberá proponer su propia metodología de gestión del servicio, deberá cumplir con los requisitos mínimos que se establecen en este apartado.

4.1. FASE DE TRANSICIÓN

Esta fase se iniciará el primer día de la prestación de servicio y tendrá una duración máxima de un mes.

El objeto de esta fase será la asimilación por parte del Licitante de los interlocutores, necesidades y sistemas objeto del contrato así como la configuración del conjunto de servicios requeridos.

Durante esta fase se será laxo en la aplicación de los niveles de servicios definidos en la “fase de ejecución del servicio” pero sí será necesario que el Adjudicatario realice los trabajos definidos en el presente expediente.

Para garantizar este hecho el Licitante deberá detallar la forma de acometer la transición, desde la contratación del servicio hasta la puesta en fase de explotación del servicio una vez concluida la puesta en marcha. El Licitante deberá exponer expresamente como pretende acometer esta transición, apoyándose en casos de éxito realizados previamente.

4.2. FASE DE EJECUCIÓN DEL SERVICIO

En esta fase y a lo largo de los 3+1 años de desarrollo del expediente, se deberá acometer la prestación del servicio de acuerdo a lo definido en los pliegos que rigen el presente expediente. Tendrá una duración hasta el mes anterior a la finalización del expediente.

Continuando con lo definido en la fase de transición, y concluida esta, en la fase de ejecución será necesario prestar el servicio de acuerdo a unos niveles de calidad que permitan a BIDEGI y sus trabajadores desarrollar sus tareas ordinarias con mínima afección.

4.3. FASE DE DEVOLUCIÓN DEL SERVICIO

Un mes antes de la conclusión del plazo de prestación del servicio, el Licitante deberá favorecer la transición al potencial nuevo adjudicatario del servicio, procediendo a la "devolución del servicio" a BIDEGI.

En esta fase, adicionalmente a la prestación del servicio ordinario de acuerdo a lo establecido en la fase de ejecución del servicio, deberá realizar la entrega de la configuración, claves de acceso y demás información necesaria para facilitar la transición al siguiente proveedor del servicio.

5. PLAZO DE EJECUCIÓN

Se trata de la prestación de un servicio de tres años de duración, con fecha de inicio prevista para el 1 de marzo de 2026 y por tanto fecha de fin 28 de febrero de 2029, con posibilidad de prórroga por plazos mensuales hasta un plazo máximo de hasta 12 meses adicionales, por mutuo acuerdo entre las partes.

En Licitante deberá explicar es su metodología la forma de acometer las fases de puesta en marcha, transición e implantación debiendo cumplir que:

- Desde el inicio del servicio deberá prestar soporte de seguridad, si bien durante los primeros 15 días se será laxo en la aplicación de los niveles de servicio.
- En el plazo no superior a 15 días el Licitante deberá garantizar tener un amplio conocimiento de los sistemas que le habilite para la gestión del servicio de seguridad en su totalidad.
- En el plazo máximo de 30 días el Licitante deberá tener el servicio plenamente operativo, de tal forma que se puedan prestar los servicios de forma normal tal y como se requiere en el presente pliego de prescripciones técnicas.

El incumplimiento de cualquiera de los plazos aquí expuestos se considerará una infracción muy grave, pudiendo BIDEGI proceder a la resolución del contrato y a la aplicación de las penalidades expuestas en el presente documento.

6. PRESUPUESTO Y CERTIFICACIÓN

Según lo descrito, tanto el presupuesto como su certificación asociada está compuesta por tres partes:

- Un importe mensual fijo por los servicios de mantenimiento de seguridad.
- Un importe bienal cuando se realicen las auditorías.
- Un importe variable, en función de las necesidades.

De acuerdo a lo anterior se realizará una única certificación mensual que incluirá la parte fija del servicio así como la parte del importe variable que corresponda con los servicios adicionales prestados en el mes vencido. Esto incluye la auditoría una vez esta esté completa incluyendo el material y sesiones formativas.

De cara a la confección del presupuesto, y su puntuación correspondiente de acuerdo a lo establecido en el pliego administrativo, se establecen las siguientes estimaciones de precios de licitación y cantidades:

SERVICIO BASICO			
	Importe Mes	Unidades	Importe Total
Servicio de Conectividad a Internet	128,00 €	36	4.608,00 €
Servicio de 24Tb almacenamiento Nube	700,00 €	36	25.200,00 €
Licencias Mantenimiento Firewall (para dos firewall's)	93,00 €	36	3.348,00 €
Licencia XDR equipos PC (para 40 equipos)	348,00 €	36	12.528,00 €
Licencia XDR equipos Servidores (para 10 servidores)	137,50 €	36	4.950,00 €
Servicio de SOC y vigilancia	900,00 €	36	32.400,00 €
Servicio de soporte técnico y mantenimiento	288,00 €	36	10.368,00 €
Auditorias de seguridad	7.500,00 €	2	15.000,00 €
TOTAL SERVICIO BASICO			**108.402,00 €**
AMPLIACIÓN SERVICIO BASICO			
Licencia adicional XDR para PC	9	240	2.160,00 €
Licencia adicional XDR para Servidor	14	48	672,00 €
TB adicional de almacenamiento	26,5	300	7.950,00 €
Bloque de 15 licencias VPN doble factor		1	1.478,62 €
TOTAL AMPLIACIÓN SERVICIO BASICO			**12.260,62 €**
TOTAL IMPORTE LICITACIÓN			**120.662,62 €**

Gipuzkoako Azpiegituren Agentzia
AIÑIGO ARIAS RODRIGUEZ-ANTIGUEDAD
2025/11/24 IFK: A-20783023
Asti auzoa, 631 - A- 20800 Zarautz

https://munigex.net/r/0/200/AAAABC78M.76HT