Departamento de Seguridad del Gobierno Vasco

Ampliación de NAS y renovación de cabinas SAN

Pliego de Bases Técnicas

1 INTRODUCCIÓN

El despliegue de nuevas aplicaciones, así como la previsión de implantar nuevos procedimientos y herramientas en el ámbito de la seguridad ciudadana hace prever a corto y medio plazo una importante explosión de ficheros (fundamentalmente vídeos) que, por su naturaleza no estructurada requiere de necesidades específicas para su óptima salvaguarda.

Como respuesta al incremento en la demanda de almacenamiento para datos no estructurados, soportados en sistemas de tipo “NAS” (Network Attached Storage) se hace necesario ampliar la capacidad de los clústeres Isilon existentes en el DSGV con el objetivo de ampliar y consolidar nuevos entornos. Es conveniente, además, actualizar la arquitectura de las matrices de discos que soportan la solución para, incorporando discos no rotacionales, mejorar las latencias en el acceso a los datos.

Estos sistemas Isilon actuales se encuentran en un nivel de ocupación alto. Se pretende ampliar dichos clústeres scale-out para permitir dar respuesta a estos nuevos requisitos con nodos de tipo capacidad extendiendo así la dimensión de la solución actual. Adicionalmente se incorporarán nodos con tecnología Flash que, actuando como caché, permitirán una mejora importante en los tiempos de acceso a los ficheros almacenados.

Para el almacenamiento de datos estructurados, máquinas virtuales y otros elementos de la arquitectura de sistemas se utiliza almacenamiento de bloque conectado a la red SAN de la que dispone el Departamento de Seguridad.

Las cabinas IBM StorWize 5020 que proporcionan el almacenamiento de este tipo están próximas a su fin de vida útil. Además, están formadas en su mayor parte por discos de tecnología SATA con unas latencias y capacidad de ejecución de operaciones de entrada salida (IOPS) lejos de lo necesario para algunos sistemas como Euskarri o SAP.

Mediante el presente pliego se pretende adecuar los sistemas de almacenamiento de datos redimensionanado su capacidad de modo de cobertura tanto, a las necesidades actuales como a nuevos requisitos provenientes de la propia evolución de los sistemas.

2 OBJETO

El objeto del presente Pliego es definir las condiciones técnicas que debe cumplir las ofertas de los licitadores para el suministro, instalación, configuración y garantía in-situ de elementos hardware y software que permitan:

- Aumentar la capacidad de almacenamiento NAS (Network Attached Storage) hasta alcanzar, por lo menos el volumen indicado en el apartado 3. Implementar nodos caché para optimizar la respuesta de la plataforma.
- Proporcionar dos cabinas de disco All-Flash para conectar a la SAN (Storage Area Network) instalada en los CPDs del Departamento de Seguridad.
- El licitador tendrá que incluir todo el material auxiliar: cableado, SFPs, tornillería, etc., las licencias y los servicios necesarios para el correcto funcionamiento de la solución que plantee de forma que se aseguren unas condiciones de disponibilidad de al menos el 99.99% en el periodo de garantía y soporte indicado.

2.1 División por lotes del expediente

Para facilitar la concurrencia de ofertas y optimizar los costes asociados a este expediente se considera adecuado su fraccionamiento en lotes en base a la tecnología de los elementos a proporcionar en cada uno de ellos. Las empresas licitadoras podrán presentar ofertas por uno o más lotes.

2.1.1 Lote 1 – Ampliación almacenamiento NAS

Ampliación de los equipos NAS ISILON de los que ya dispone el DSGV para alcanzar las capacidades de almacenamiento, IOPS, etc requeridos.

2.1.2 Lote 2 – Renovación cabinas SAN

Cabinas de disco All-Flash NVME que servirán para reemplazar los equipos actuales de almacenamiento tipo bloque una vez conectadas a la red SAN.

3 LOTE 1 – AMPLIACIÓN ALMACENAMIENTO NAS.

3.1 Situación actual

El almacenamiento NAS se basa en dos clústeres Isilon de EMC repartidos entre los dos centros de datos departamentales, siendo uno activo y el otro pasivo y replicando la información mediante tareas "SyncIQ".

Cada clúster está formado por 6 nodos A2000.

La configuración de los nodos es: A200-4U-Single-16GB-1x1GE-2x10GE SFP+-120TB-400GB SSD-SED).

Cada nodo dispone de 2 puertos ethernet a 10 Gbps para el acceso de los clientes, un puerto ethernet a 1 Gbps para el acceso administrativo, un disco SSD de 400GB brutos para la cache L3 y un almacenamiento de 120TB brutos proporcionado por discos SAS mecánicos a 7200 rpm hasta un total de 720TB brutos en cada clúster.

La paridad del clúster es "+2d:1n" soportando el fallo de dos discos o un nodo.

El licenciamiento actual incluye los siguientes productos:

Software	Licensed for	Status	Expiration date
OneFS	6 nodes	Licensed	N/A
CloudPools	0 nodes	Unlicensed	N/A
Security hardening	0 nodes	Unlicensed	N/A
HDFS	0 nodes	Unlicensed	N/A
SmartConnect Advanced	6 nodes	Licensed	N/A
SmartDedupe	6 nodes	Licensed	N/A
SmartQuotas	6 nodes	Licensed	N/A
SnapshotIQ	6 nodes	Licensed	N/A
SyncIQ	6 nodes	Licensed	N/A

3.2 Situación objetivo

3.2.1 Suministros hardware solicitados

Se ofertarán los siguientes equipos hardware:

- 4 nodos Isilon A2000, con 20 discos de 12TB Self Encrypted Drives cada nodo en cada uno de los dos CPDs.
- 3 nodos Isilon/PowerScale F200, con 4 discos de 7,68 TB Self Encrypted Drive cada nodo en cada uno de los dos CPDs

Tras esta ampliación, se dispondrán de 2026 TiB RAW/ 1.675 TiB netos de capacidad NAS Scale Out en cada uno de los dos CPD del Departamento de Seguridad del Gobierno Vasco.

3.2.2 Licencias

Se requieren las siguientes licencias en cada uno de los nodos Isilon/PowerScale suministrados:

- SmartQuotas
- SmartConnect
- SnapShots
- InsightIQ
- SyncIQ
- SmartDedupe
- SmartPools
- Software de monitorización y gestión

Con el objetivo de integrar los nuevos equipos en el cluster existente, se requiere el suministro de la siguiente licencia en cada uno de los nodos Isilon A200 existentes con su período de mantenimiento a cotérmino el mantenimiento de cada equipo A200:

- SmartPools

3.2.3 Servicios adicionales

La oferta incluirá, como servicios adicionales:

- Transporte, enrackado, instalación y puesta en marcha de los elementos hardware.
- Retirada y reciclaje de los embalajes. Los residuos de embalaje generados en las tareas de instalación (básicamente cartón y plástico) se recogerán separadamente y se depositarán en los contenedores de recogida selectiva que le indique la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos.
- Configuración inicial y conexión con el resto de la infraestructura del Departamento de Seguridad.
- Ejecución de las pruebas necesarias para validar la solución y para optimizar su funcionamiento.
- Registro de cada elemento en la plataforma de gestión.
- Definición de los procedimientos de monitorización. Implantación de los mismos en la plataforma del DSGV.
- Formación al personal designado por el Departamento de Seguridad en las herramientas de administración y monitorización. Se deberá prever la formación a, por lo menos, 4 personas.
- Formación al personal designado por el Departamento de Seguridad en las tecnologías de almacenamiento desplegadas. Se deberá prever la formación a, por lo menos, 4 personas.
- Mantenimiento de los elementos hardware instalados. Dada la criticidad de estos, el servicio se prestará en formato 24*7 con tiempos de respuesta no superiores a 1 hora y tiempo de resolución de las incidencias no superior a 24 horas.
- La garantía de los servicios de instalación deberá prestarse durante al menos tres años después del final de proceso de puesta en marcha.

- En el caso del software, deberá incluirse la entrega de nuevas versiones o parches durante el período de garantía.
- Se incluirán todos los elementos de mantenimientos preventivos especificados por el fabricante y la reparación, con la eventual sustitución de piezas deterioradas, de cualquier avería que pudiera producirse. La garantía de los productos incluirá piezas y mano de obra, debiendo efectuarse las intervenciones en el centro donde estén ubicados los equipos.
- Se presentará documentación sobre gestión de la garantía y el mantenimiento, de forma que se detalle los tiempos de respuesta y procedimientos de actuación para cada una de las posibles incidencias, los teléfonos de contacto del integrador o fabricante que de soporte y cualquier código necesario para proceder a la apertura de solicitudes de servicio.

4 LOTE 2 – RENOVACIÓN CABINAS SAN

4.1 Situación actual

El almacenamiento SAN departamental está estructurado en dos capas: presentación y cabinas de disco.

La capa de presentación es un stretch-cluster formado por cuatro controladores de la familia IBM Spectrum Virtualize (MTM: 2147-SV1) distribuídos entre los dos CPDs departamentales. Cada nodo dispone de dos tarjetas con 4 puertos FC a 16 Gbps. Sus funciones son:

- Virtualizar la capa de almacenamiento gestionando el acceso a los datos desde los distintos sistemas departamentales
- Replicar los datos entre ambos centros de datos proporcionando alta disponibilidad
- Facilitar la migración de datos entre distintos sistemas de almacenamiento y/o centros de datos
- Mejorar el acceso a los datos mediante una caché global y la identificación de datos calientes (autotiering)
- Optimizar los recursos mediante la deduplicación y compresión de los datos

El almacenamiento es proporcinado por dos cabinas IBM Storwize v5020 (MTM:2078-224) formadas por 1 enclosure de control y 7 de expasión repartidas entre los dos centros de datos departamentales siendo ambas activas.

Cada cabina dispone de dos controladoras con dos puertos ethernet a 1Gbps para el acceso administrativo, una tarjeta FC de 4 puertos a 16 Gbps y un almacenamiento de 322.31TiB brutos proporcionado por tres tipos de discos diferentes repartidos según la tabla:

Capa	Discos/Tamaño	mDisks	Paridad
Flash (24)	SSD/744.71GiB	2	RAID level: RAID 5 Redundancy: 1 Spare drives: 1
Enterprise (120)	HDD/10k rpm/1.09TiB	2	RAID level: Distributed RAID 5 Redundancy: 1 Rebuild Areas Total: 2
Nearline (24)	HDD/7200 rpm/7.28TiB	1	RAID level: Distributed RAID 6 Redundancy: 2 Rebuild Areas Total: 1

4.2 Situación objetivo con la renovación

El objetivo de la renovación de las cabinas SAN es mejorar las latencias observadas en el acceso a disco con la arquitectura actual y duplicar la capacidad disponible para su uso por los sistemas corporativos.

4.2.1 Dimensionamiento

- Se requieren dos cabinas de disco All-Flash NVMe, una por cada CPD.
- Cada cabina propuesta deberá incluir un mínimo de 15 discos NVMe con capacidad mínima cada disco de 7 TB.
- Cada cabina deberá incluir al menos 160 TiB usables en discos NVMe con una ratio de data reduction al menos de un 4:1, aportando un mínimo de 642TiB efectivos en cada uno de los dos CPDs. En caso de que, por la tipología de datos almacenados por el Departamento de Seguridad del Gobierno Vasco, esta ratio no se alcanzara y, por lo tanto, el volumen efectivo de datos susceptibles de ser almacenados fuera inferior a 642 TiB, se suministrarán, instalarán y configurarán, sin coste adicional para el Gobierno Vasco, los discos necesarios para alcanzar ese volumen de datos utilizando la misma tecnología que los provistos inicialmente.

4.2.2 Característica de la Arquitectura

- Arquitectura de almacenamiento debe ser diseñada para aprovechar la tecnología de memoria de estado sólido (All-Flash) con múltiples controladoras Activas/Activas, no se admitirán los diseños basados en arquitecturas Activas/Pasivas y/o Activas/Standby.
- Debe admitir el protocolo NVMe en el acceso a sus discos y no debe incorporar discos rotacionales.
- Debe poder soportar cargas de trabajo de bloques en el mismo hardware sin necesidad de hardware externo para las cargas de ficheros.
- Cada cabina de almacenamiento debe tener un mínimo de 768 GB de Memoria caché y capacidad de procesamiento equivalente, al menos, a 48 cores Intel x86.
- Debe ser capaz de soportar crecimiento multi-dimensional, tanto ScaleUp (añadiendo capacidad) como ScaleOut (añadiendo controladoras). Los crecimientos en capacidad deberán poder ser realizados de manera no disruptiva.
- Las cabinas de almacenamiento deben disponer de puertos de FrontEnd FC que puedan negociar a velocidades de, por lo menos, 32 o 16Gbps. Los puertos FC a 32 Gbps aportarán un acceso End-to-End NVMe desde ellos hasta los discos, aportando un FrontEnd NVMe over Fibre Channel.
- Las controladoras de las cabinas deberán poder actulizarse a nuevas gamas dentro de la misma familia de hardware.
- El diseño aportado debe garantizar una disponibilidad para el negocio de 99,9999%. El licitador aportará los datos utilizados para el cálculo de esta cantidad.
- El diseño propuesto debe carecer de puntos únicos de fallo y tener todo el hardware redundado. Las cabinas deben ser resilientes al fallo de una fuente de alimentación, controladora, disco o cable. Todo lo anterior debe poderse cambiar en caliente (arquitectura hot-swappable)
- Todas las actualizaciones de software o hardware deberán poder hacerse de forma no disruptiva (sin interrupción de servicio)
- Los datos se replicarán entre las dos cabinas ofertadas asegurando la continuidad del negocio en caso de perdida de servicio de uno de los CPDs.

- Debe soportar compresión in-line y deduplicacion in-line para maximizar la eficiencia en capacidad. La solución deberá aportar hardware para hacer estas funciones y garantizar que el rendimiento no se vea afectado.
- No se admitirán métodos de eficiencia post proceso que dependan de ciclos libres de CPU para aplicar características de eficiencia.
- El fabricante aportará números de rendimiento IOPS /MBs/rt con la reducción de datos activada y toda la capacidad de la cabina direccionada.
- Las características de reducción de datos aplicaran a todos los discos de la solución y para todas las estructuras de datos.
- Se incluirán licencias de deduplicación, replicación y cifraLa licencia de DRR estará incluida para todo el espacio direccionable de la cabina.
- La cabina incluirá capacidades de thin provisioning / virtual provisioning. La licencia de thin provisioning será incluida para todo el espacio direccionable de la cabina.

4.2.3 Integración con SVC

La solución propuesta debe poder presentarse a los clientes utilizando los equipos SVC IBM-2147 de los que dispone el DSGV.

Adicionalmente se admitirán ofertas que, además de las propias cabinas, incluyan una alternativa a la propia solución SVC, siempre que mantenga o mejore los niveles de alta disponibilidad actuales. Es decir, el sistema alternativo ofertado debe ser capaz de virtualizar tanto las cabinas objeto de suministro como las cabinas actuales propiedad del Departamento de Seguridad, siempre garantizando un tiempo de recuperación ante desastres (RTO) –bien en una de las cabinas, bien en un CPD completo–, igual a cero.

4.2.4 Replicación

- Las cabinas debe soportar al menos replica asíncrona bidireccional sobre IP con opción de configurar “1:1”, “1:n” , “n:1”
- La replicación deb permitir crear un clúster activo/activo con granularidad de LUN.
- La solución deberá soportar snapshots, si existiera algún tipo de overhead (CPU, espacio SSD), el fabricante tendrá en consideración ese overhead y proveerá de suficientes recursos para usar al menos 500TiB de Snapshots de datos creados en la cabina.

4.2.5 Administración

- La solución debe proveer un mecanismo simple de administración cuyo entorno gráfico debe formar parte del software instalado en la cabina.
- La solución debe proveer entorno grafico GUI, línea de comando CLI. Se valorará que dispona de una API Rest que permita administrar el 100% de las funcionalidades y monitorizar la cabina.
- Se valorará la capacidad de administración con Ansible siempre y cuando el fabricante aporte la documentación y ejemplos de tal uso.
- Se debe permitir la monitorización el rendimiento (latencia, IOPS, lectura/escritura, ancho de banda, tamaño de IO, longitud de la cola), la capacidad (total, ahorro -

compresión, deduplicación, thin, snapshots) y la configuración con la capacidad de redirigir alertas a una dirección de correo electrónico.

4.2.6 Seguridad

- El hardware ofertado debe soportar cifrado de datos sin degradación del rendimiento cumpliendo con la certificación "FIPS-140-2".
- Se incluirán las licencias de cifrado para la capacidad total de las cabinas.

4.2.7 Migración de datos

- Los servicios ofertados para este Lote 2 incluirán el plan de migración de los datos actuales detallando plazos, metodología, procedimientos y tareas.

4.2.8 Servicios adicionales

La oferta incluirá como servicios adicionales:

- Transporte, enrackado, instalación y puesta en marcha de los elementos hardware.
- Retirada y reciclaje de los embalajes. Los residuos de embalaje generados en las tareas de instalación (básicamente cartón y plástico) se recogerán separadamente y se depositarán en los contenedores de recogida selectiva que le indique la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos.
- Configuración inicial y conexión con el resto de la infraestructura del Departamento de Seguridad.
- Ejecución de las pruebas necesarias para validar la solución y para optimizar su funcionamiento.
- Registro de cada elemento en la plataforma de gestión.
- Definición de los procedimientos de monitorización. Implantación de los mismos en la plataforma del DSGV.
- Formación al personal designado por el Departamento de Seguridad en las herramientas de administración y monitorización. Se deberá prever la formación a, por lo menos, 4 personas.
- Formación al personal designado por el Departamento de Seguridad en las tecnologías de almacenamiento desplegadas. Se deberá prever la formación a, por lo menos, 4 personas.
- Mantenimiento de los elementos hardware instalados. Dada la criticidad de estos, el servicio se prestará en formato 24*7 con tiempos de respuesta no superiores a 1 hora y tiempo de resolución de las incidencias no superior a 24 horas.
- La garantía de los servicios de instalación deberá prestarse durante al menos tres años después del final de proceso de puesta en marcha.
- En el caso del software, deberá incluirse la entrega de nuevas versiones o parches durante el período de garantía.
- Se incluirán todos los elementos de mantenimientos preventivos especificados por el fabricante y la reparación, con la eventual sustitución de piezas deterioradas, de cualquier avería que pudiera producirse. La garantía de los productos incluirá piezas y

mano de obra, debiendo efectuarse las intervenciones en el centro donde estén ubicados los equipos.

- Se presentará documentación sobre gestión de la garantía y el mantenimiento, de forma que se detalle los tiempos de respuesta y procedimientos de actuación para cada una de las posibles incidencias, los teléfonos de contacto del integrador o fabricante que de soporte y cualquier código necesario para proceder a la apertura de solicitudes de servicio.

5 ASPECTOS GENERALES COMUNES A TODOS LOS LOTES

5.1 Soporte y mantenimiento

Las propuestas recogerán para la totalidad del plazo de ejecución (60 meses) un mantenimiento proactivo y correctivo de los elementos objeto de suministro en formato 24 * 7.

En la propuesta se deberán indicar claramente los mecanismos de cumplimiento de los tiempos de respuesta y SLAs aplicables ante incidencias según las siguientes definiciones de gravedad:

Gravedad	Tipificación de la incidencia	SLA
Crítica	Un sistema en producción u otro(s) sistemas de misión crítica están caídos y no hay una solución disponible inmediatamente. • Todos o una fracción sustancial de los datos de misión crítica están en riesgo significativo de pérdida o corrupción. • Se ha producido una pérdida sustancial de servicio • Las operaciones del negocia se han visto gravemente interrumpidas	Tiempo de respuesta: 30 minutos Cobertura horaria: 7x24
Mayor	La funcionalidad principal está dañada gravemente • Las operaciones pueden continuar de forma limitada, aunque la productividad a medio plazo puede verse afectada adversamente. • Hay una solución temporal disponible	Tiempo de respuesta: 2 horas Cobertura horaria: 7x24
Menor	Pérdida de funcionalidad parcial y no crítica de la funcionalidad del software • El funcionamiento de algunos componentes está afectado pero el software se puede continuar utilizando	Tiempo de respuesta: 3 horas Cobertura horaria: Horario laborable local
Consultas	Preguntas generales sobre utilización de los productos. Errores en la documentación.	Tiempo de respuesta: 8 horas Cobertura horaria: Horario laborable local

Para los casos en los que para la resolución de una incidencia se precise el reemplazo de componentes hardware la instalación dichos repuestos y la retirada y devolución del elemento defectuoso quedará dentro del alcance de este servicio. Si el elemento a sustituir se tratara de un disco este quedaría a disposición del Departamento de Seguridad para su destrucción de acuerdo con los procedimientos definidos en la Política de Seguridad.

Con la modalidad de soporte ofertada la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos, o un tercero contratado por la misma y en quien esta delegue, tendrá además la capacidad de abrir casos de soporte directamente con el fabricante.

El contrato de soporte en vigor dará derecho al Departamento de Seguridad al uso de nuevos microcódigos o versiones de software publicados, así como a la instalación de los mismos por parte de personal directo del fabricante.

El fabricante deberá proveer de acceso 7x24 a las herramientas de soporte en línea, de manera que la Dirección de Gestión de Telecomunicaciones y Sistemas Informáticos tenga acceso a las nuevas versiones de software o firmware que se adquieran mediante este contrato por el periodo de mantenimiento ofertado.

La política de seguridad de la información en vigor en el Departamento de Seguridad del Gobierno Vasco no permite el acceso remoto a los Sistemas para operaciones de soporte o mantenimiento.

5.2 Documentación

Las ofertas técnicas deberán detallar la arquitectura ofertada en cuanto a elementos, software licenciado y funcionalidades disponibles con el mayor nivel de detalle posible, y aportando tablas de topología, interconexión y escenarios de funcionamiento de la tecnología ofertada.

Los licitadores deberán incluir en sus propuestas al menos la siguiente documentación:

- Solución Técnica:
  - Descripción global de la propuesta, haciendo referencia a detalles de la arquitectura y topología, así como a las condiciones de rendimiento, disponibilidad, seguridad y escalabilidad.
  - Relación detallada de los elementos ofertados, cuyas características deberán estar claramente descritas para su evaluación y deberán venir acompañadas de la justificación respecto a cómo cumplen los requisitos especificados en las bases de prescripciones técnicas.
  - Relación de licencias software, incluyendo número y tipo de suscripciones.
  - Información sobre acondicionamiento necesario para el funcionamiento de los equipos. Datos aproximados de consumo eléctrico y disipación térmica, así como una aproximación del peso de los equipos.
  - Procedimientos relacionados con la continuidad del servicio.
- Plan de implantación.
  - Descripción pormenorizada de las tareas a efectuar.
  - Cronograma de actividades previstas para la puesta en marcha.
  - Identificación de responsables para las diferentes fases y tareas.
- Garantía y soporte.
  - Plan de mantenimiento sobre el período de garantía.
  - Mecanismos para la prestación del soporte (web, correo, teléfonos de contacto, planes de trabajo, bolsas de horas, etc.).
- Plan de formación. Con detalles relativos a calendario, duración y contenido de esta.
- Mejoras. Prestaciones no solicitadas, y que de forma cuantitativa y/o cualitativa añadan valor a la oferta presentada. El DSGV se reserva el derecho a valorar si lo ofertado y no solicitado se considera mejora.

- Durante la implantación, se generará toda la documentación referente a la codificación de todos los elementos instalados: números de serie, ubicación física, esquemas de conexión, usuarios de acceso y administración.

5.3 Plazos

Una vez firmado el contrato el adjudicatario dispondrá de un plazo de dos meses para el suministro de los equipos y un mes adicional para la implantación.

6 CONDICIONES DE SEGURIDAD.

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.

En concreto conviene resaltar la imposibilidad de conectar equipos no autorizados a las redes del Departamento de Seguridad y la prohibición de realizar conexiones remotas para la ejecución de cualquier tipo de trabajos, monitorizaciones, etc.

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.

Al finalizar el contrato, y una vez haya sido transferida la información al Departamento de Seguridad del Gobierno Vasco, el adjudicatario se compromete a destruir toda la información, teniendo en cuenta los distintos soportes o documentos donde esta pueda constar: bases de datos en discos, ficheros temporales, copias de seguridad, soportes en papel, etc. A tal efecto, una vez realizada la operación descrita, entregará una declaración por escrito al Departamento de Seguridad donde conste que así se ha realizado.