GOBIERNO DEL
PRINCIPADO DE

PLIEGO DE PRESCRIPCIONES TECNICAS DE

una plataforma de backup/restore en el CPD Principal y Secundario del Principado de Asturias.

(Expediente 9 /2017)

Dirección: C/ Coronel Aranda, 2, 5ª planta, sector derecho, 33005 Oviedo. Tfno: 985 10 53 20. Fax: 985 10 59 45

Índice

1 ALCANCE Y OBJETIVO DEL CONTRATO ..... ¡ERROR! MARCADOR NO DEFINIDO.

1.1 INTRODUCCIÓN ..... **¡ERROR! MARCADOR NO DEFINIDO.**
1.2 ARQUITECTURA ACTUAL 5
1.3 OBJETO 6
1.3.1 Suministro ..... **¡Error! Marcador no definido.**
1.3.2 Servicios ..... **¡Error! Marcador no definido.**

2 REQUISITOS TÉCNICOS **9**

2.1 REQUISITOS DE SUMINISTRO 9
2.1.1 Características de la solución 9

3 REQUISITOS DE IMPLANTACIÓN **14**

3.1 FASES DEL PROYECTO 14
3.1.1 Fase I - Análisis de la situación actual y diseño de la nueva Infraestructura 14
3.1.2 Fase II - Suministro, implantación y migración a la nueva infraestructura. 15
3.1.3 Fase III - Formación de la solución 17
3.1.4 Fase IV - Soporte y Mantenimiento de la solución 17
3.2 ACUERDOS DE NIVEL DE SERVICIO 19
3.2.1 Aspectos generales 19
3.2.2 Acuerdos de Nivel de Servicio 20

1 Introducción

La Dirección General de Tecnologías Informáticas y de las Comunicaciones, dependiente de la Consejería de Empleo, Industria y Turismo del Principado de Asturias dispone de una plataforma de backup corporativo formada por varios servidores de backup, una cabina de discos y un robot de cintas. Los servidores realizan dos copias diarias de la información a proteger, la primera copia en la cabina de discos DD4500 o el robot de cintas SL3000, según el entorno que estemos copiando y la segunda copia en el robot de cintas SL3000. Sobre esta plataforma se realizan las copias de los datos de los entornos de APA, Justicia y parte del entorno sanitario. En la nueva plataforma se pretende además integrar a los Hospitales y Centros de Salud, que actualmente no están incluidos en la plataforma corporativa.

Esta plataforma de backup está ubicada en el CPD Principal y tanto las versiones del software de backup (Tivoli Storage Manager) como los servidores donde está instalado ya no están soportados por los fabricantes, lo que hace imprescindible una renovación de la plataforma.

La renovación consiste en la adquisición de una nueva plataforma de backup formada por appliances o servidores, una cabina de discos y un robot de cintas en el CPD Principal y appliances o servidores y una cabina de discos en el CPD Secundario. Los appliances son servidores de propósito específico, optimizados para el único software que se instala y ejecuta en ellos, en este caso el software de backup, de tal manera que la administración y actualización de todos los componentes es única. Las copias que se realicen en el CPD Primario estarán replicadas en el CPD Secundario y viceversa.

Esta renovación de la plataforma permite la actualización tecnológica y la implementación de nuevas funcionalidades que mejoran nuestras infraestructuras en cuanto a rendimiento, capacidad, disponibilidad y escalabilidad.

Dada la integración de la infraestructura con gran parte de los servidores ubicados en los CPDs, se ha tenido en cuenta no solo el suministro e instalación de la plataforma, sino también el análisis y diseño de la integración de esta con los servidores de datos a los cuales debe dar servicio de backup.

Arquitectura Actual

Se indica en este apartado la arquitectura de la plataforma de backup actualmente implantada en el Principado de Asturias y se detallan los componentes que son objeto de la migración a la nueva plataforma especificada y requerida en este pliego.

- Se dispone de 9 servidores de backup para al ámbito de Consejerías/Justicia y 4 servidores de backup para el ámbito Sanitario, todos ellos en arquitectura x86_64, con SO Linux SLES y en distintas versiones de software de IBM TSM (desde versión 5.5 hasta 6.3). Todos los servidores están conectados a la red de almacenamiento del Principado de Asturias. Estos servidores se conectan vía SAN (Red de Almacenamiento) contra las cabinas de almacenamiento y el robot de cintas.

- Se están gestionando actualmente más de 1500 nodos de backup en infraestructura física y virtual (sobre plataforma VMWare), teniendo en cuenta que un 30% de los nodos son máquinas físicas, un 65% son máquinas virtuales sin almacenamiento RDM (Raw Decice Mapping) asignado y un 5% son máquinas virtuales con almacenamiento RDM asignado. Actualmente se está realizando backup/restore de plataformas Linux, Novell Open Enterprise Server, Windows, Solaris y DartOS (mediante protocolo NDMP) y se están utilizando agentes de TSM para realizar backup en caliente de forma consistente de entornos Oracle, SAP, Exchange, SQL Server.

- Las copias de seguridad diarias del ámbito de Consejerías/Justicia se están realizando contra la cabina EMC Data Domain 4500 y los archivados de alta retención se realizan contra el robot de cintas SL3000. Adicionalmente se realiza doble copia tanto de las copias diarias como de los archivados en el robot de cintas SL3000.

- Las copias de seguridad diarias del ámbito Sanitario se realizan contra la cabina EMC Data Domain 4500 y el robot de cintas SL3000 y los archivados de alta retención se realizan contra el robot de cintas SL3000. Adicionalmente se realiza doble copia tanto de las copias diarias como de los archivados en el robot de cintas SL3000.

- Todas las copias de seguridad de los sistemas ubicados en el CPD Principal y en el CPD Secundario se realizan vía LAN contra los servidores de TSM con líneas de backup dedicadas a 1 GB. Las copias de seguridad de los sistemas ubicados en oficinas remotas del Principado se realizan vía WAN.

- Se dispone de una cabina EMC Data Domain DD4500 para el ámbito Consejerías/Justicia y Sanitario.

- Se dispone de un robot de cintas SL3000 con 24 drivers LTO4 y 1419 slots, compartida por los dos ámbitos.

- Los sistemas operativos de los servidores a proteger son:

  Entorno UNIX

  Solaris

  Entorno LINUX

  SUSE LINUX
  Red Hat Linux
  CentOS
  Novell Open Enterprise Server

  Entorno WINDOWS

  Microsoft Windows

2 Alcance y Objetivo del Contrato

2.1 Arquitectura Actual

Se indica en este apartado la arquitectura de la plataforma de backup actualmente implantada en el Principado de Asturias y se detallan los componentes que son objeto de la migración a la nueva plataforma especificada y requerida en este pliego.

- Se dispone de 9 servidores de backup para al ámbito de Consejerías/Justicia y 4 servidores de backup para el ámbito Sanitario, todos ellos en arquitectura x86_64, con SO Linux SLES y en distintas versiones de software de IBM TSM (desde versión 5.5 hasta 6.3).Todos los servidores están conectados a la red de almacenamiento del Principado de Asturias. Estos servidores se conectan vía SAN (Red de Almacenamiento) contra las cabinas de almacenamiento y el robot de cintas.

- Se están gestionando actualmente más de 1500 nodos de backup en infraestructura física y virtual (sobre plataforma VMWare), teniendo en cuenta que un 30% de los nodos son máquinas físicas, un 65% son máquinas virtuales sin almacenamiento RDM (RawDeciceMapping) asignado y un 5% son máquinas virtuales con almacenamiento RDM asignado. Actualmente se está realizando backup/restore de plataformas Linux, Novell Open Enterprise Server, Windows, Solaris y DartOS (mediante protocolo NDMP) y se están utilizando agentes de TSM para realizar backup en caliente de forma consistente de entornos Oracle, SAP, Exchange, SQL Server.

- Las copias de seguridad diarias del ámbito de Consejerías/Justicia se están realizando contra la cabina EMC Data Domain 4500 y los archivados de alta retención se realizan contra el robot de cintas SL3000. Adicionalmente se realiza doble copia tanto de las copias diarias como de los archivados en el robot de cintas SL3000.

- Las copias de seguridad diarias del ámbito Sanitario se realizan contra la cabina EMC Data Domain 4500y el robot de cintas SL3000 y los archivados de alta retención se realizan contra el robot de cintas SL3000. Adicionalmente se realiza doble copia tanto de las copias diarias como de los archivados en el robot de cintas SL3000.

- Todas las copias de seguridad de los sistemas ubicados en el CPD Principal y en el CPD Secundario se realizan vía LAN contra los servidores de TSM con líneas de backup dedicadas a 1 GB. Las copias de seguridad de los sistemas ubicados en oficinas remotas del Principado se realizan vía WAN.

- Se dispone de una cabina EMC Data Domain DD4500 para el ámbito Consejerías/Justicia y Sanitario.

- Se dispone de un robot de cintas SL3000 con 24 drivers LTO4 y 1419 slots, compartida por los dos ámbitos.

- Los sistemas operativos de los servidores a proteger son:

  Entorno UNIX

  Solaris

  Entorno LINUX

  SUSE LINUX
  Red Hat Linux

CentOS
Novell Open Enterprise Server

Entorno WINDOWS

Microsoft Windows

2.2 Objeto

El objeto consiste en la contratación de una plataforma de backup/restore en el CPD Principal y Secundario del Principado de Asturias.

Asi mismo comprende el servicio de backup/restore de todos los sistemas actualmente gestionados por el software de backup IBM Tivoli Storage Manager (TSM) y de todos los Centros de Salud y Hospitales dependientes de la Consejería de Sanidad del Principado de Asturias, que no están integrados en la plataforma de backup actual. La relación de estos sistemas se entregarán bajo acuerdo de confidencialidad.

El objeto del contrato contempla una parte de suministro y otra de servicios.

Suministro

- En el CPD Principal se requieren los appliances o servidores de backup necesarios para proporcionar el servicio de backup/restore en alta disponibilidad requerido y especificado en este pliego, un repositorio de almacenamiento (único e independiente) de los backups, con una capacidad para gestionar 300 TB de frontal distribuidos y replicados entre ambos CPDs y de al menos 1500 TB de backup brutos (TB sin deduplicación) y un robot de cintas con, al menos, 4 drives LTO6, 100 slots y 200 cartuchos de cinta LTO6. Esta infraestructura se suministrará junto a todo el software y licencias permanentes necesarias para el cumplimiento de los requisitos solicitados.

- En el CPD Secundario se requieren los appliances o servidores de backup necesarios para proporcionar el servicio de backup/restore especificado y requerido en este pliego con un repositorio de almacenamiento (único e independiente) de los backups con la capacidad suficiente para almacenar 300 TB de frontal distribuidos y replicados entre ambos CPDs y de al menos 1500 TB de backup brutos (TB sin deduplicación). Esta infraestructura se suministrará junto a todo el software y licencias permanentes necesarias para el cumplimiento de los requisitos solicitados.

En el CPD Principal se deberá suministrar un repositorio de backup que deberá estar dimensionado conforme a los requerimientos técnicos que se describen en el pliego de prescripciones técnicas de este concurso.

En el CPD Secundario se deberá suministrar un repositorio de backup que deberá estar dimensionado conforme a los requerimientos de este pliego, o bien se podrá utilizar la cabina EMC DataDomain 4500 actualmente disponible y en funcionamiento en el CPD Principal y que cuenta con una capacidad de 240 TB netos en Active Tier y 42,5 TB netos en Extended Retention Tier, con un 80% de ocupación a fecha de febrero de 2017. Esta cabina está en soporte hasta mayo de 2018. Si se optara por utilizar esta cabina, se

deberá ajustar la capacidad y el mantenimiento de la misma para cumplir los requerimientos de este pliego, así como su traslado al CPD Secundario.

En todo caso, las cabinas deberán cumplir los requerimientos técnicos de replicación técnicos que se describen en el pliego de prescripciones técnicas de este contrato..

Servicios

- Análisis de la situación actual y diseño de la nueva infraestructura que incluye:
    - Análisis de la arquitectura actualmente implantada en el Principado de Asturias.
    - Diseño de la nueva infraestructura
    - Documentación de diseño de la nueva infraestructura (Documentos de Diseño de la arquitectura de MESISPA)
    - Definición y diseño de la migración de la infraestructura anterior a la nueva infraestructura.
    - Planificación de implantación de la nueva infraestructura.
    - Planificación de la migración a la nueva infraestructura incluyendo la migración de datos.

- Implantación del equipamiento adquirido que incluye:
    - Servicios de instalación, configuración, optimización y puesta en marcha de la solución de backup/restore en ambos CPDs.
    - Servicios de implantación de la solución de backup en los sistemas de información de los Centros de Salud y Hospitales.
    - Documentación de toda la plataforma instalada y del proyecto siguiendo las metodologías del Principado de Asturias (MESISPA).
- Migración a la nueva infraestructura de los servicios y datos de la infraestructura actual
    - Servicios de migración de todos los **sistemas de información**,o servidores, actualmente cuyas copias de seguridad son gestionadas por el software de backup IBM Tivoli Storage Manager (TSM) a la nueva solución.
    - Servicios de migración de los **datos de backup** almacenados en los sistemas de backup/restore actualmente gestionados por el software de backup de IBM Tivoli Storage Manager (TSM) y que tengan una retención mayor a 30 días.

- Mantenimiento de la infraestructura IBM Tivoli Storage Manager (TSM) a sustituir, desde la firma del contrato hasta la finalización de la migración.
- Formación de los técnicos del Principado de Asturias de acuerdo con lo especificado en el apartado 3.1.3 del pliego de prescripciones técnicas de este contrato.

- Soporte y mantenimiento de la solución ofertada de acuerdo con los requisitos indicados en el apartado 3.1.4 del pliego de prescripciones técnicas de este contrato.

3 Requisitos Técnicos

3.1 Requisitos de Suministro

3.1.1 Características de la solución

Se describen a continuación las características requeridas de la solución de backup y de los sistemas a suministrar tanto para el CPD Principal como para el CPD Secundario.

3.1.1.1 Funcionalidades

1) Se requiere en el CPD Principal una solución de backup de tipo PBBA (Purpose-Built Backup Appliance), entendiendo PBBA como una solución hardware y software integrada, cuyo propósito específico es la realización de copias de seguridad y restauración de datos.

2) Los appliances o servidores del CPD Principal deberán permitir realizar copias de seguridad de los sistemas que se encuentren operativos en el CPD Principal, oficinas remotas, centros de salud y hospitales y deberán permitir mantener una segunda copia, mediante un sistema de replicación contrala infraestructura del CPD Secundario. La réplica debe incluir no solo los datos protegidos mediante las copias de seguridad sino también los metadatos y todos los componentes lógicos necesarios para poder continuar con el servicio de backup en caso de contingencia. Se deberá disponer de al menos un appliance o servidor para el ámbito Consejerías/Justicia y al menos un appliance o servidor para el ámbito Sanitario.

3) Los appliances o servidores del CPD Principal deberán estar configurados en alta disponibilidad y deberán permitir una configuración que permita distribuir la gestión de las copias de seguridad por ámbito (Consejerías/Justicia y Sanidad), permitiendo en caso de caída de uno de ellos el failover a un segundo appliance o servidor, bien del mismo ámbito si existiera, bien del otro ámbito, manteniendo y soportando la gestión del backup/restore en el CPD Principal. En el caso de caída de todos los appliances o servidores de un ámbito, la gestión de las copias de seguridad deberá ser asumida por los appliances o servidores del otro ámbito en el CPD Principal. Solo en caso de caída de todos los appliances o servidores del CPD Principal se deberá realizar la contingencia del servicio de backup al CPD Secundario para realizar toda la gestión de las copias de seguridad con el/los appliance/s o servidor/es del CPD Secundario.

4) Se requiere en el CPD Principal un repositorio de almacenamiento de los backups único e independiente basado en disco, que permita una deduplicación global de todos los datos protegidos y compartido por todos los appliances o servidores.

5) Se requiere en el CPD Principal un robot de cintas para hacer backup de algunos servicios concretos donde el ratio de deduplicación que se obtiene así lo aconseje. De estos servicios se hará doble copia en el robot. Además se utilizará para hacer una tercera copia de algunos entornos específicos cuyo backup está en el repositorio de disco.

6) Se requiere en el CPD Secundario una solución de backup de tipo PBBA (Purpose-Built Backup Appliance) formada por uno o más appliances o servidores, que permita dar continuidad al servicio en caso de contingencia del servicio de backup del CPD Principal.

7) El/los appliance/s o servidor/es del CPD Secundario deberán permitir realizar copias de seguridad de los sistemas que se encuentren operativos en el CPD Secundario y deberán permitir mantener una segunda copia, mediante un sistema de replicación contra la infraestructura del CPD Principal. En el

CPD Secundario se permite compartir en el/los mismo/s appliances/s o servidor/es la gestión de la copias de seguridad de los dos ámbitos (Consejerías/Justicia y Sanidad).

8) Se requiere en el CPD Secundario un repositorio de almacenamiento de los backups único e independiente basado en disco, que permita una deduplicación global de todos los datos protegidos y compartido por todos los appliances o servidores que permita dar continuidad al servicio en caso de contingencia del servicio de backup del CPD Principal.

9) La solución de backup debe permitir la replicación de los datos de backup de manera automatizada, deduplicada y bidireccional entre los dos CPDs.

10) La réplica de datos de backup entre los dos repositorios debe realizarse por IP, con los datos deduplicados y cifrados, utilizando la funcionalidad concreta del repositorio, aunque mantendrá la consistencia (catálogo único) con el mismo, teniendo en todo momento el software de backup corporativo control y constancia de dónde se encuentra la información primaria y de respaldo.

11) En caso de una contingencia parcial en el CPD Principal, es decir, solo uno o varios servicios de negocio entran en una contingencia y se levantan en el CPD Secundario, el backup o restore de estos servicios se deberá gestionar desde el/los appliance/s o servidor/es y el repositorio del CPD Secundario y en este caso se deberá realizar su doble copia en el CPD Principal. En caso de una contingencia total de los servicios de negocio del CPD Principal, todos los backups y/o restores se deberán realizar en el CPD Secundario.

12) Una vez resuelta la contingencia del servicio y una vez este levantado de nuevo en el CPD Principal, el backup o restore de este servicio se deberá gestionar de nuevo desde el/los appliace/s o servidor/es y el repositorio del CPD Principal y su doble copia se deberá realizar de nuevo contra el CPD Secundario. De igual forma, una vez resuelta una posible contingencia total de los servicios de negocio, todos los backups y/o restores se deberán realizar de nuevo desde el CPD Principal.

13) En caso de una contingencia en el repositorio de almacenamiento de los backups del CPD Principal, los appliances o servidores del CPD Principal deberán continuar con la gestión de las copias de seguridad y restauración, atacando al repositorio de almacenamiento del CPD Secundario. Una vez recuperado el repositorio del CPD Principal se deberán sincronizar los datos de backup y se restablecerán las copias contra este repositorio.

14) En caso de una contingencia en el repositorio de almacenamiento de los backups del CPD Secundario, el/los appliance/eso servidor/es del CPD Secundario deberán continuar con la gestión de las copias de seguridad y restauración, atacando al repositorio de almacenamiento del CPD Principal. Una vez recuperado el repositorio del CPD Secundario se deberán sincronizar los datos de backup y se restablecerán las copias contra este repositorio.

15) La solución de backup debe permitir aplicar las políticas de backup vigentes en el Principado de Asturias en cuanto a la periodicidad de los backups, archivados y retenciones de los mismos.

16) La solución debe poder proteger la información de forma deduplicada en origen utilizando deduplicación global en línea (no post-proceso).

17) La solución de backup deberá poder realizar las copias de seguridad en el repositorio de almacenamiento de los backups o en el robot físico de cintas.

18) La solución debe proporcionar una deduplicación global para todo el entorno protegido, a excepción de los backups realizados sobre el robot físico de cintas, independientemente del tipo de datos, sistema operativo, naturaleza física o virtual o ámbito de los sistemas protegidos.

19) Toda la información protegida, independientemente de la política de backup y de donde este realizada (repositorio de disco o robot de cintas), deberá permanecer en el sistema de propósito específico para Backup (PBBA).

20) La solución de backup debe permitir la realización de copias full con alta retención a partir de los datos ya almacenados en la solución de backup y de forma deduplicada.

21) La solución de backup debe permitir realizar una copia de tipo full diariamente, deduplicando la información en origen y trasmitiendo únicamente los bloques modificados.

22) La recuperación de la información será en un solo paso, sin tener la necesidad de implementar políticas de restore de un backupFull más incremental o diferencial.

23) La solución debe permitir realizar backup/restore de las plataformas Windows, Linux, Solaris a nivel de fichero plano tanto en plataforma física como virtual. La relación de Sistemas Operativos está especificada en el apartado1.2 de este pliego.

24) La solución debe permitir realizar backup en caliente garantizando la consistencia de las copias de seguridad y la integración con las distintas herramientas para copia online de las siguientes plataformas: BBDD Oracle, SAP, SQL Server, Microsoft Exchange y Microsoft Sharepoint.

25) La solución debe proteger sistemas NAS, mediante protocolo NDMP que deberá poder realizarse como full backup diario, permitiendo realizar el restore en un sólo paso.

26) La solución debe proteger los entornos virtuales tanto a nivel de imagen (sin instalar agente en la máquina virtual) como mediante la instalación de agente en la máquina virtual permitiendo:

- Integración con vStorage APIs for Data Protection (VADP).
- Uso de la funcionalidad Change Block Tracking (CBT) para la transmisión únicamente de los bloques modificados en el backup.
- Restauración granular a nivel de ficheros individuales o discos virtuales de backups realizados a nivel de imagen (.vmdk) para máquinas Windows y Linux.
- El arranque de la máquina virtual directamente desde el backup, permitiendo la restauración en la máquina original, en otra máquina ya existente o en una nueva.
- Capacidad de integración con tecnología de thinprovisioning, en backup y recuperación.
- Posibilidad de gestionar restores desde vSphere Web Client.
- Debe permitir la eliminación del paging file o swap de las imágenes del backup.
- Debe permitir la eliminación del espacio no ocupado de las imágenes del backup.

27) La solución debe garantizar la integridad de todos los datos protegidos, mediante mecanismos de seguridad y redundancia automáticos (no procesos manuales) que garanticen la integridad de todas las copias de seguridad almacenadas.

28) La solución debe permitir la realización de backup/restore de infraestructuras remotas no consolidadas a través de comunicaciones WAN, deduplicando la información en origen de forma global sin necesidad de instalación de dispositivos físicos en las sedes remotas.

29) La solución debe permitir la posibilidad de delegar la restauración granular de ficheros a determinados usuarios que no dispongan de permisos de administración sobre los servidores protegidos ni sobre los sistemas de backup.

30) La solución debe tener la capacidad de cifrado en tiempo real tanto en la transmisión de la información como en el destino de la misma.

31) La solución debe disponer de una consola única para la gestión, administración y operación de la misma, incluyendo todas las licencias necesarias y que permita:

- Administrar y configurar la solución de backup tanto en modo gráfico como en modo línea de comandos.
- Monitorizar la solución de backup y generar eventos/alertas de fallos o de cualquier problema de rendimiento de la solución y generar informes para realizar análisis de los eventos ocurridos. La herramienta debe guardar históricos de los eventos/alertas durante al menos un año y deben estar disponibles para su explotación.
- Generar informes de capacidad y consumo de la solución de backup.
- Generar informes diarios con los resultados de las copias de seguridad.

3.1.1.2 Disponibilidad y fiabilidad

32) La solución de backup no debe tener ningún componente lógico como punto único de fallo y todos deben estar replicados para garantizar la continuidad del servicio de backup.

33) Los repositorios de almacenamiento deben disponer de sistemas de protección ante fallos de componentes físicos. Adicionalmente los repositorios deberán disponer de un sistema de consistencia de los datos ante cortes de suministro eléctrico no programados y apagado ordenado de los mismos.

34) El repositorio del CPD Principal deberá disponer de redundancia de controladoras.

3.1.1.3 Capacidad

35) La solución de backup debe estar dimensionada para permitir la gestión de backup/restore de **300 TB** de frontal (volumen de información a proteger) y **1500 TB** de backup a proteger (volumen de copia tras la aplicación de las políticas de backup y sin tener en cuenta ningún tipo de deduplicación) en cada CPD, teniendo en cuenta que el 25% de los datos son estructurados y el 75% de los datos son no estructurados.

Del volumen total de los TB de frontal el 30% pertenece al ámbito Consejerías/Justicia y 70% al ámbito Sanitario, aunque estos porcentajes pueden variar a lo largo del contrato.

36) La solución de backup debe estar dimensionada para gestionar el backup de **1500 nodos** de backup teniendo en cuenta que el 30% de ellos son servidores físicos, el 65% son servidores virtuales sin almacenamiento asignado en modo RawDeviceMapping (RDM) y el 5% restante son servidores virtuales con almacenamiento asignado en modo RawDeviceMapping (RDM).

37) El repositorio de almacenamiento unificado tanto del CPD Principal como del CPD Secundario, deberá disponer de una capacidad mínima en el momento de la instalación de 300 TB netos, sin contar la deduplicación.

38) El robot físico deberá disponer de al menos 4 drives LTO6 y100 slots. Se deberán proporcionar 200 cintas LTO6.

39) El adjudicatario deberá proveer de los interfaces físicos necesarios en todos los componentes de la solución de backup (conexiones a 1Gb, a 10Gb y FC), para garantizar el cumplimiento de todos los requisitos en cuanto a rendimiento, capacidad, disponibilidad y escalabilidad que se requieren en

este pliego, teniendo en cuenta que actualmente, las redes de backup del Principado de Asturias son dos redes independientes y dedicadas a 1 Gb, una para ámbito Consejerías/Justicia y otra para el ámbito Sanitario. Adicionalmente, la solución de backup deberá disponer de los interfaces físicos necesarios en todos los componentes de la solución para redes de backup a 10 Gb.

40) A nivel de conectividad la solución deberá disponer de puertos necesarios para que en caso de caída de alguno de ellos se disponga de interfaces suficientes para que el servicio no se vea afectado.

41) A nivel de conectividad se deberá tener en cuenta que actualmente en el Principado de Asturias existen dos redes backup a 1 Gb, físicamente independientes, una para ámbito Consejerías/Justicia y otra para el ámbito Sanitario, por lo que todos los componentes físicos que conforman la solución de backup tanto del CPD Principal como en el CPD Secundario, deberán disponer de los interfaces físicos necesarios para realizar la conexión a las dos redes de forma independiente.

3.1.1.4 Rendimiento

42) Se requiere una capacidad de ingestión mínima de 18 TB/h con un mínimo de 140 streams concurrentes de escritura.

3.1.1.5 Escalabilidad

43) Los appliances o servidores del CPD Principal y el CPD Secundario deberán tener una capacidad de crecimiento de hasta un 50% en la capacidad de proceso, en el número de nodos a gestionar y en los TB que puede proteger.

44) Los repositorios del CPD Principal y el CPD Secundario deberán tener una capacidad de crecimiento de hasta un 25% sobre la capacidad neta utilizada en el momento de la finalización de la migración, en un único pool de deduplicación global.

45) Cualquier incremento de capacidad adicional que sea requerida en la solución de backup deberá ser añadida sin migración de los datos previamente almacenados y sin parada de servicio en el CPD Principal.

46) El licenciamiento debe permitir la ampliación posterior del mismo con una unidad mínima de compra de 1TB

3.1.1.6 Licencias

47) Se suministrarán todas las licencias necesarias para el cumplimiento de los requisitos especificados en este pliego. Estas licencias deberán ser permanentes, es decir, seguir siendo válidas de forma indefinida tras la finalización del contrato. Las licencias estarán sujetas a los requisitos de soporte y mantenimiento de este pliego.

3.1.1.7 Integración

48) Integración SNMP con la solución de monitorización global del CPD (alertas gestión).

4 Requisitos de Implantación

4.1 Fases del proyecto

La ejecución del proyecto de implantación se realizará en tres fases:

- **Fase I - Análisis de la situación actual y diseño de la nueva Infraestructura.** Se realizará un análisis de la arquitectura de backup actualmente implantada en el Principado de Asturias y todos los servicios conectados a la misma, diseño y documentación de la nueva infraestructura, definición de la estrategia de migración de los distintos servicios y de los datos residentes en la infraestructura actual a la nueva solución de backup y documentación de las intervenciones a acometer y planificación de las mismas. Esta fase ira desde la firma del contrato y tendrá una duración máxima de 60 días naturales.

- **Fase II – Suministro, implantación y migración a la nueva infraestructura**. Se realizará el suministro, instalación, configuración, documentación y puesta en marcha de la solución de backup suministrada así como la migración de los datos a la nueva solución de backup y la migración de todos los elementos conectados a los servidores de backup actuales a la nueva solución de backup. La duración máxima de esta fase es de 210 días desde la firma del contrato. Esta fase se divide en dos subfases:

    - Suministro e implantación. Estas subfases podrán superponerse a la Fase I.
    - Migración a la nueva infraestructura. No podrá comenzar hasta que se haya acabado la Fase I y la subfase de suministro e implantación.

- **Fase III - Formación de la solución.** Consistirá en la formación del equipo identificado por la APA. Esta fase irá desde la implantación de la nueva infraestructura hasta un año después de la primera formación. Se divide en dos subfases:

    - La primera formación deberá impartirse en un plazo máximo de dos meses después de la implantación de la nueva infraestructura.
    - Formación siguiendo el programa oficial de certificación de los fabricantes del equipamiento suministrado en un plazo máximo de un año después de la primera formación.

- **Fase IV. Soporte y Mantenimiento de la infraestructura. Constará de dos subfases:**

    - Soporte de la Actual Infraestructura. Deberá mantenerse desde la firma del contrato hasta que se finalice la migración de los datos y se apague esta infraestructura.
    - El soporte de la nueva infraestructura irá desde la finalización de la Fase II y durará hasta el final del contrato.

A continuación se detallan los requisitos de cada una de estas fases.

4.1.1 Fase I - Análisis de la situación actual y diseño de la nueva Infraestructura

49) El plazo máximo de finalización para la Fase I es de 60 días naturales a contar desde la formalización del contrato.

50) Se deberá realizar un análisis de la situación actual de la infraestructura de backup y de los servicios TIC que se están protegiendo. Este análisis determinará el diseño y la arquitectura de la nueva solución de backup a implantar. Como resultado de este requerimiento y para su aceptación, el adjudicatario deberá entregar un documento con la arquitectura y diseño de la solución de backup.

51) Se deberá definir la estrategia de migración de los distintos sistemas y de los datos almacenados en los servidores actuales a la nueva solución de backup, así como las distintas intervenciones a realizar, una estimación de la duración de cada tarea y una planificación para acometer esas intervenciones. Como resultado de este requerimiento y para su aceptación el adjudicatario deberá entregar un documento con la estrategia de la migración.

52) Se deberá realizar una planificación completa del proyecto incluyendo todas las tareas necesarias para acometer todas las fases del mismo (implantación, migración, documentación y formación), en el que se deberán detallar todas las tareas a realizar, el tiempo requerido para cada una de ellas y la planificación de las mismas. Como resultado de este requerimiento y para su aceptación el adjudicatario deberá entregar un documento con la planificación de todas las tareas a acometer durante las distintas fases del proyecto.

53) El adjudicatario deberá desarrollar un informe en el que identifiquen y analicen los riesgos y factores críticos que puedan surgir durante la ejecución del proyecto de migración, así como la probabilidad de que ocurran y el impacto derivado de su materialización. Deberá elaborar también el plan de acción necesario para la gestión de estos riesgos y factores críticos. Como resultado de este requerimiento y para su aceptación el adjudicatario deberá entregar un informe de riesgos y un plan de acción para mitigarlos.

4.1.2 Fase II - Suministro, implantación y migración a la nueva infraestructura.

54) El plazo máximo de finalización para la Fase II es de 210 días naturales a contar desde la formalización del contrato. Esta fase del proyecto podrá solaparse con la Fase I durante las tareas de implantación, aunque no con las tareas de migración a la nueva infraestructura.

55) La implantación ha de incluir todos los elementos y actuaciones necesarias para el correcto funcionamiento de todos los requisitos solicitados. Entre estas actuaciones se encuentran:

- Suministro, desembalaje, ensamblado de todos los componentes hardware solicitados y anclaje en los armarios provistos por el adjudicatario
- Instalación física, conexionado y etiquetado de todos los elementos que conforman la solución de backup.
- Los elementos de conexión de la nueva infraestructura de backup serán suministrados por el licitador en número suficiente para cumplir con los requisitos de este pliego en cuanto al conexionado de todos los dispositivos.
- Instalación del software y configuración de la solución de backup, para cumplir con los objetivos de disponibilidad, fiabilidad, capacidad y rendimiento requeridos en este pliego.
- Instalación del software de gestión de la solución de backup y configuración de todas las funcionalidades requeridas en este pliego.
- Configuración de la monitorización de todos los dispositivos que conforman la solución de backup. Definición de alertas ante cualquier evento que pueda provocar problemas de rendimiento y/o del servicio de backup.
- Configuración de herramienta para aviso automático de fallos al equipo de soporte (adjudicatario y/o fabricante) de los elementos de este contrato.

56) La migración a la nueva infraestructura incluye la migración detodos los datos gestionados por la actual solución de backup, excluyendo los incrementales con retención 30 días que actualmente están en el DD 4500y las dobles copias del resto de datos, asegurando la correcta aplicación de

todos los requisitos solicitados. Desde el comienzo de esta migración debe garantizarse el correcto y completo funcionamiento de esta solución en 24x7.

Entre estas actuaciones se encuentran:

- Definición de un documento para cada una de las intervenciones a realizar identificadas en la fase de análisis y en el que se recoja el detalle de todas las tareas a realizar durante cada intervención y el resultado esperado, así como la estimación de tiempos de cada una de las tareas y el impacto en el servicio/s TIC que pueda/n verse afectado. Los documentos de intervención se realizarán conforme a la estrategia de migración definida en la fase I. Además en cada documento de intervención se deben recoger las pruebas a realizar tras la migración y el resultado esperado. También se debe incluir en cada documento un plan de contingencia para resolver los problemas identificados previamente como posibles riegos y su resolución.
- Ejecución por parte del adjudicatario de todas las tareas a realizar para acometer la migración de los datos a la nueva solución de backup.
- El adjudicatario deberá hacerse cargo de la provisión de todos los elementos hardware y software necesarios para la realización de la migración de los datos a la nueva solución de backup, así como de la provisión de las licencias requeridas para llevar a cabo la misma.
- Análisis de riesgos de cada una de las migraciones a realizar e impacto en el servicio de backup y plan de acción para su mitigación.

57) En caso de que para la realización de cualquiera de las tareas de esta fase sea necesaria una parada de algún servicio TIC del Principado de Asturias, ésta se realizará en ventana horaria de mínimo impacto (fuera de horario laboral, en horario nocturno, fines de semana y festivos).

58) El adjudicatario propondrá un plan de pruebas para el equipamiento suministrado. El plan de pruebas debe incluir, además de aquellos otros aspectos que proponga el licitador, los siguientes:

- Correcto encendido y apagado de los equipos.
- Verificación de backup/restore de los datos de los distintos entornos.
- Verificación de las funcionalidades requeridas y ofertadas adicionalmente.
- Correcta detección de los eventos de alerta en el sistema de monitorización.
- Realización de informe de rendimiento y funcionamiento en cuanto a capacidad, deduplicación, volumen de copia diario, etc para garantizar el correcto dimensionamiento de la solución de backup.
- Realización de las pruebas de contingencia necesarias para asegurar el correcto funcionamiento de las réplicas y funcionamiento en caso de contingencia según los escenarios planteados en este pliego.

59) Los planes de pruebas propuestos serán aprobados por la APA, quien podrá solicitar la realización de pruebas adicionales.

60) El adjudicatario utilizará equipamiento implantado y personal propio para la realización de los planes de pruebas acordados y se realizarán conjuntamente con personal de la APA en caso de que sea requerido.

61) Como resultado de esta fase y para su aceptación, el adjudicatario deberá entregar la siguiente documentación:

- Manuales de instalación y operación (MIOS) en los que se incluya toda la información relativa a la instalación, configuración y operación de todos los productos (software) instalados y configurados.
- Documento de servicio de la solución de backup, en el que se incluyan los diagramas lógicos y físicos de la solución de backup y una descripción de cada componente, así como sus dependencias con otros servicios TIC.
- Inventario de todos los componentes hardware y software instalados.
- Documentos de intervención.
- Documento de arquitectura y diseño final.

4.1.3 Fase III - Formación de la solución

62) El adjudicatario impartirá formación para un grupo de al menos 5 personas identificadas por la APA, que serán los encargados de la gestión, administración y operación de los diferentes componentes objeto del presente procedimiento de licitación. Esta formación se llevará a cabo en la sede de la APA en Asturias y la duración total será de, al menos, 25 horas. Los alumnos recibirán en formato electrónico toda la documentación asociada al curso. El contenido será validado por la APA e incluirá, entre otros que pudieran ser considerados de interés por el adjudicatario, apartados de operación, gestión, configuración y monitorización de la solución ofertada.

63) Durante el proyecto, el adjudicatario estará disponible para realizar traspaso de conocimientos en el puesto de trabajo a los administradores, utilizando directamente la solución implantada y los procedimientos y funcionalidades que se utilizarán para su administración cotidiana, con el objetivo principal de profundizar en las tareas referidas a la operación, administración, configuración, dimensionamiento y mejora de la solución.

64) Adicionalmente al punto 62, el adjudicatario deberá preparar un plan de formación para un grupo de 3 personas a identificar por la APA, siguiendo el programa oficial de certificación de los fabricantes del equipamiento suministrado. Todos los costes de la formación y certificación serán a cargo del licitador.

4.1.4 Fase IV - Soporte y Mantenimiento de la solución

4.1.4.1 Requisitos Generales

65) La contratación del suministro y prestaciones para la implantación de una solución de backup para la APA incluye el soporte y mantenimiento integral prestado por el adjudicatario que asegure que todas las infraestructuras, funcionalidades y elementos de dicha solución se encuentran disponibles y en condiciones óptimas para su utilización al menos, durante la vigencia de este contrato.

66) El ámbito de responsabilidad del soporte y mantenimiento del adjudicatario alcanza a todas aquellas infraestructuras, licencias, recursos y elementos suministrados, trabajos y cualquier otra prestación que el adjudicatario haya realizado como parte del contrato.

67) El soporte y mantenimiento de la solución comenzará una vez finalizado el plazo definido para la ejecución de la Fase II (210 días naturales) y dicha fase esté completamente finalizada. La duración de este será de veintinueve meses que podrán ser prorrogados otros veintinueve meses.

68) La solución de backup se integra en dos CPDs en el que conviven e interactúan diversos sistemas que deben estar operativos con los mismos criterios de calidad para prestar un servicio homogéneo. El servicio de soporte y mantenimiento debe prestarse en colaboración con los distintos agentes que intervienen en el mantenimiento de la infraestructura tecnológica de la APA. Por tanto, en aquellos

casos en los que algún componente incluido en el presente procedimiento de licitación, esté conectado o interactúe con elementos cuya operación corresponda a empresas diferentes de la adjudicataria del presente procedimiento de licitación, el adjudicatario deberá responder del normal funcionamiento de sus componentes, debiendo demostrar los fallos que sean imputables a otros suministradores cuando considere que son la causa del mal funcionamiento del servicio.

69) Se requiere que el suministrador colabore en todos los supuestos de fallos con el resto de agentes que intervienen en el soporte y mantenimiento, para detectar y eliminar cualquier problema que esté afectando al servicio.

70) Este soporte y mantenimiento incluye, entre otros, los aspectos que se desarrollan en los apartados siguientes:

- Actualización de versiones de software y firmware de toda la infraestructura de backup, realizando adicionalmente un informe indicando las actualizaciones requeridas en los servidores donde están instalados los clientes de backup.
- Soporte técnico.
- Gestión y resolución de incidencias.
- Revisiones preventivas.
- Sustitución y reemplazo de componentes.

71) El soporte y mantenimiento incluirá todas las intervenciones que sean necesarias, tanto in-situ como en remoto, de forma que se resuelvan y/o ejecuten de forma óptima y con calidad todas las actividades, revisiones, procedimientos, etc.

72) En caso de que sea necesaria la sustitución de equipamiento, el adjudicatario deberá proceder a la sustitución in-situ del mismo por otro de características iguales o superiores.

73) El servicio de soporte y mantenimiento incluirá un máximo de cuatro instalaciones o actualizaciones de las nuevas versiones de software liberadas al mercado, para cada uno de elementos software suministrados.

74) La instalación o actualización del software se realizará por el adjudicatario en las ventanas de mantenimiento que establezca la APA, preferentemente en ventana horaria de mínimo impacto (fuera de horario laboral, fines de semana y festivos) y de manera aislada en los CPD Principal y Secundario. El adjudicatario realizará la carga de la versión in-situ cuando sea necesario, realizando las pruebas necesarias para verificar el correcto funcionamiento tras la actualización. Para realizar la instalación o actualización el adjudicatario deberá entregar un documento de intervención detallado con los pasos a realizar, las pruebas para verificar el correcto funcionamiento tras la intervención y un plan de marcha atrás.

75) El servicio de soporte y mantenimiento incluirá las actualizaciones de microcódigo u otros módulos tantas veces como sea necesario para el funcionamiento óptimo de los equipos y sistemas suministrados. Estas actualizaciones, al igual que las cargas de nuevas versiones de software, serán realizadas por el adjudicatario si la APA así lo solicitara.

76) El adjudicatario será responsable de realizar los ajustes necesarios en las configuraciones de los equipos implicados (appliances o servidores y cabinas) para adaptarlas a las nuevas versiones de software. Estos trabajos se realizarán bajo la coordinación de la APA.

77) La APA tendrá acceso directo a información de soporte de los elementos suministrados, para realizar consultas técnicas, abrir incidencias, acceder a documentación, así como obtener parches y actualizaciones o nuevas versiones del software suministrado y objeto del contrato.

78) El adjudicatario dispondrá de un centro de gestión de incidencias y soporte. Este centro estará accesible continuamente a través de una "Ventanilla única" de contacto durante las **24 horas del día, todos los días del año**, a través de teléfono, mediante una dirección de correo electrónico y/o un formulario web.

79) El soporte y mantenimiento se realizará in-situ siempre sea necesario y cuando la criticidad y el impacto de la intervención así lo requiera, quedando a criterio de la APA la decisión final.

80) El adjudicatario realizará todas las actuaciones necesarias para resolver una incidencia.

81) Se mantendrá informado a la APA o a quien éste determine en todo momento y de manera detallada de cualquier acción a tomar para la resolución de una incidencia.

82) Una incidencia se cerrará cuando la APA o quien éste determine haya aceptado dicho cierre, lo que normalmente se dará cuando el servicio se haya restablecido y estabilizado, y se haya informado a la APA o a quien éste designe.

83) Si después de cerrar una incidencia se vuelven a presentar los mismos fallos que se dieron por resueltos en un plazo de 1 mes, se reabrirá la misma incidencia anterior.

4.1.4.2 Priorización de incidencias

84) Las incidencias y consultas se clasifican en tres tipos, en función de su severidad. El nivel de severidad será asignado por la APA o quien éste determine en el momento de abrir una incidencia. En caso de que la incidencia se realice mediante apertura automática, la severidad será asignada por la propia herramienta. Se definen los siguientes niveles de severidad:

- Se considera incidencia de nivel alto a un problema severo que cause o pueda causar una degradación de la solución de backup, tanto a nivel de rendimiento como a nivel de disponibilidad.
- Se considera incidencia de nivel medio a un problema en la solución de backup que no causa degradación de rendimiento.
- Se considera incidencia de nivel bajo a una consulta o requerimiento de información sobre aspectos técnicos relacionados con la solución de backup objeto de este contrato.

4.2 Acuerdos de nivel de servicio

4.2.1 Aspectos generales

85) Los servicios estarán sometidos a un conjunto de acuerdos de nivel de servicio en base a los cuales se regirá el seguimiento del servicio, su proceso de mejora continua y la aplicación de las cláusulas de penalización.

86) La empresa adjudicataria se compromete a cumplir los Acuerdos de Nivel de Servicio en los términos establecidos en el presente informe.

87) El responsable del contrato, o en su defecto la persona (o personas) en la que puedan delegar esta actividad, supervisarán el cumplimiento de los Acuerdos de Nivel de Servicio (ANS).

88) El incumplimiento de los ANS dará lugar a la imposición de las penalidades establecidas o a la resolución del contrato.

89) Será siempre será potestad de la APA las determinaciones finales sobre el cumplimiento de los acuerdos de servicio globales.

90) En caso de que al aplicar la fórmula correspondiente a un ANS para determinar su penalidad resultase esta negativa no se compensará con el resto.

91) El incumplimiento de los niveles de servicio exigidos, indicados en este apartado, dará lugar a la imposición de las penalidades que se indican en cada uno de ellos.

4.2.2 Acuerdos de Nivel de Servicio

A) Soporte técnico global

La solución de backup objeto de este contrato debe estar en pleno funcionamiento. Por pleno funcionamiento se entiende que todos y cada uno de los componentes de la solución están operativos al menos el 99% del tiempo y no hay corte de servicio de backup/restore. En este 99% no se incluyen las incidencias que supongan caída del servicio. La disponibilidad se mide de forma anual.

La solución de backup no debe sufrir más de 3 cortes de servicio de backup/restoreal año.

B) Tiempo de respuesta ante incidencias

b.1) Tiempo de respuesta ante incidencias de nivel alto

En caso de incidencias de nivel alto la empresa adjudicataria dará respuesta en 30 minutos desde que recepciona la comunicación de la misma.

b.2) Tiempo de respuesta ante incidencias de nivel medio

En caso de incidencias de nivel medio la empresa adjudicataria dará respuesta en 3 horas desde que recepciona la comunicación de la misma.

b.3) Tiempo de respuesta ante incidencias de nivel bajo

En caso de incidencias de nivel bajo la empresa adjudicataria dará respuesta en 8 horas desde que recepciona la comunicación de la misma.

C) Tiempo de resolución ante incidencias

c.1) Tiempo de resolución ante incidencias de nivel alto

En caso de incidencias de nivel alto, la empresa adjudicataria dispondrá de 12 horas para su resolución, entendiendo el tiempo de resolución como el comprendido entre la apertura de la incidencia y el cierre del caso.

c.2) Tiempo de resolución ante incidencias de nivel medio

En caso de incidencias de nivel medio, la empresa adjudicataria dispondrá de 24 horas para su resolución, entendiendo el tiempo de resolución como el comprendido entre la apertura de la incidencia y el cierre del caso.

D) El contratista está obligado a entregar los informes que a continuación se describen.

d.1) Informes inmediatos

Deben ser entregados en las 24 horas posteriores al cierre de la incidencia de nivel alto, en soporte magnético compatible con las aplicaciones software instaladas en la Administración del Principado de Asturias.

• **Informes de Incidencias de nivel alto.**

Se entregarán informe de la incidencia de nivel alto abierta, adjuntando toda la información relativa a la resolución de la misma, especificando las causas, los análisis realizados, las conclusiones obtenidas y los trabajos ejecutados para la resolución

d.2) Informes bimestrales

Estos informes que se deberán entregar en la primera quincena del mes posterior a los meses correspondientes, en soporte magnético compatible con las aplicaciones software instaladas en la Administración del Principado de Asturias.

• **Informe de Monitorización de la infraestructura objeto del contrato**

Se trata de un informe de estado de la infraestructura objeto del contrato, con información suficiente para el conocimiento del estado del mismo siendo datos imprescindibles los siguientes: alarmas producidas con identificación clara del origen de la misma, nivel de ocupación de cabina, nivel de uso de los medios de transmisión de información.

• **Informes de Incidencias.**

Se entregarán informes de las incidencias abiertas sobre la infraestructura objeto del contrato durante el periodo correspondiente, adjuntando toda la información relativa a la resolución de las mismas o el estado en que se encuentran caso de no estar cerradas.

d.3) Informes semestrales

Estos informes que se deberán entregar en el primer mes posterior al semestre correspondiente, en soporte magnético compatible con las aplicaciones software instaladas en la Administración del Principado de Asturias.

- **Informe de Rendimiento de la infraestructura objeto del contrato.**

El adjudicatario deberá realizar un informe de rendimiento detallado de cada uno de los componentes incluidos en este contrato, durante la duración del mismo, con una periodicidad semestral, con un apartado de riesgos y un plan de acción con propuestas para mejorar el rendimiento o mitigar los riesgos identificados. Posteriormente y tras autorización y planificación de la APA el adjudicatario realizará las acciones de mejora y/o correctivas que correspondan. También debe incluir una relación de piezas sustituidas en el que se indique la pieza (Código y partnumber o referencia del producto del fabricante), número de serie y ubicación que se cambia e idénticos datos para la nueva pieza.

E) El soporte para reportar problemas del software o el hardware y dar un nivel de severidad de la incidencia debe realizarse por teléfono o vía web en castellano y/o en inglés en un horario 24 horas 7 días a la semana.

F) La empresa adjudicataria proveerá los elementos que sean necesarios remplazar y será la empresa adjudicataria la responsable de la instalación de la pieza y en su caso de la devolución de la pieza sustituida.

G) Cualquier versión del software cubierta por este contrato debe estar disponible en formato electrónico para que la Administración del Principado de Asturias pueda hacer uso de la misma. El acceso a este software puede ser vía WEB y/o soporte magnético y/o soporte USB Siendo requisito mínimo darlo en uno de los soportes.

H) El software de entorno operativo del equipamiento, (software que permite a las cabinas de almacenamiento arrancar y funcionar de manera correcta), debe ser instalado por la empresa adjudicataria de este contrato.

I) La empresa adjudicataria debe disponer de herramientas de monitorización remota de los equipamientos objeto de este contrato que permitan la detección de cualquier error en la infraestructura gestionada.

J) El personal de la Administración del Principado dispondrá de acceso a la base de conocimiento del adjudicatario vía web para al menos un usuario.

K) La retirada de cualquier componente hardware de la infraestructura objeto de este contrato que haya sido sustituido debe ser realizada por la empresa adjudicataria y deberá ser realizada durante los tres meses siguientes a la sustitución.

L) El adjudicatario se obliga a:

Asegurar la estabilidad del equipo de trabajo para asegurar la permanencia del conocimiento adquirido por el mismo. No obstante, si causas no previstas forzaran la sustitución de algún miembro del equipo, o si el responsable del contrato o el Director del Proyecto de la DGTIC así lo solicitara, se mantendrá un período mínimo de 15 días de concurrencia entre los recursos entrante y saliente para asegurar la transferencia de conocimiento que minimice el impacto en el servicio.

El o los recursos entrantes a los que se refiere el párrafo anterior, deberán acreditar los mismos requisitos exigidos de solvencia que para los medios que en su caso, se hayan adscritos a la ejecución del contrato. La solicitud de cambio de un recurso en el equipo de trabajo deberá realizarse por parte del adjudicatario con un preaviso mínimo de 15 días.

RAMIRO CONCEPCIÓN SUÁREZ - 11049840L

Firmado digitalmente por RAMIRO CONCEPCIÓN SUÁREZ - 11049840L
Nombre de reconocimiento (DN): 2.5.4.13=Qualified Certificate: AAPP-FP-M-HW-KPSC, ou=certificado electrónico de empleado público, ou=CONSEJERÍAS - S3333001J, o=PRINCIPADO DE ASTURIAS, serialNumber=11049840L, sn=CONCEPCIÓN SUÁREZ, givenName=RAMIRO, cn=RAMIRO CONCEPCIÓN SUÁREZ - 11049840L, c=ES
Fecha: 2017.03.22 08:53:56 +01'00'

El Jefe del Servicio de Infraestructuras TIC