Junta General
del Principado de Asturias

Servicio de Tecnologías e Infraestructuras

Pliego de Prescripciones Técnicas que han de regir en el Concurso, por procedimiento abierto, para la renovación del centro de proceso de datos de la Junta General del Principado de Asturias

ÍNDICE

1 Introducción y consideraciones previas

La Junta General del Principado de Asturias cuenta con un centro de proceso de datos (en adelante CPD) ubicado en las propias instalaciones de la institución.

Dicho CPD aloja la infraestructura de almacenamiento, servidores y licencias asociadas que permiten el funcionamiento de los sistemas de información de la Institución. Esta infraestructura informática necesita una renovación y adecuación a los nuevos requisitos con los que cuenta la Junta General, provenientes en primer lugar de la propia evolución tecnológica de los sistemas y soluciones usados en la Junta y en segundo lugar por la necesidad de implementar la capacidad de teletrabajo en la organización.

El actual CPD lleva en funcionamiento desde el año 2014. Dicha infraestructura es claramente insuficiente para las necesidades actuales y está funcionando al 100% de su capacidad, impidiendo de facto el crecimiento orgánico esperado de la institución en la parte del CPD (este crecimiento viene provocado por nuevos proyectos y por el propio crecimiento vegetativo de los sistemas de información, cada vez más complejos y con más necesidad de recursos). Aparte de consideraciones en lo que respecta a la capacidad del CPD, alguno de los elementos que lo componen están fuera de soporte y son obsoletos. Se estima necesaria una renovación completa de dicho CPD para poder garantizar el funcionamiento de los sistemas de información para los próximos años, dotando a la Junta de nuevas capacidades y mejorando la integridad y seguridad de los sistemas existentes.

Es conocido que el impacto de la pandemia global de COVID-19 en la sociedad ha promovido la adopción de nuevas formas de trabajo que, estando ya presentes en los usos y costumbres de algunas organizaciones, ha terminado por extenderse de forma generalizada en empresas, organismos y administraciones públicas. Así, la Junta General, que no es ajena a estos requisitos, necesita adaptar su infraestructura tecnológica para dotarse de la infraestructura que es condición previa a la implantación del teletrabajo con todas las garantías de seguridad, integridad y disponibilidad.

Teniendo en cuenta ambos requisitos primarios, en primer lugar, renovar una infraestructura obsoleta y en segundo dotarse de recursos que son condición necesaria para el teletrabajo, la Junta General del Principado de Asturias implementará una solución de CPD con el concepto activo/activo y se dotará del hardware y software necesario para cumplir con ambos requisitos.

2 Situación actual del centro de proceso de datos de la Junta General

La Junta General cuenta con un centro de datos con dos ubicaciones físicas, una en el edificio administrativo de la Calle Cabo Noval (CPD1) y otra en el Palacio de la Junta General en la calle Fruela (CPD2).

Ambos edificios están enlazados con una línea de comunicaciones redundada de 1Gbps sobre tecnología Metrolan (o similar) con terminación en interface Gigabit Ethernet.

El CPD1, que denominaremos principal, aloja la infraestructura de virtualización que en la actualidad soporta todos los servicios informáticos de la institución. Se compone de

- Dos servidores (host) de virtualización sobre tecnología VMWare vSphere
- Un sistema de almacenamiento IBM v3700
- Un autocargador LTO 5 sobre tecnología de conexión SAS
- Una cabina de almacenamiento QNAP
- Diferentes servidores físicos (no virtualizados) que alojan software específico
- Licencias Windows Server 2012 (incluyendo servidores, CAL y RDS)
- Sistema de publicación de aplicaciones RemoteApp sobre tecnología Windows 2012 RDS
- Sistema de cortafuegos redundando (HA) sobre tecnología Sonicwall
- Antivirus EPP sobre tecnología Kaspersky
- Dos switches de distribución para las conexiones del equipamiento de CPD (28 puertos Gigabit)

El CPD2, que denominaremos secundario, aloja una infraestructura de virtualización que en la actualidad sirve de réplica de datos de la infraestructura principal y adicionalmente, aloja servidores secundarios.

- Un servidor (host) de virtualización sobre tecnología VMWare vSphere
- Una cabina de almacenamiento QNAP
- Licencias Windows Server

Mediante la tecnología de VMWare Data Protection se realiza una réplica diaria de los volúmenes de las máquinas virtuales en producción de un edificio al otro.

La copia de seguridad se realiza con el software Veritas BackupExec y se hace sobre cinta y disco.

La infraestructura de red de la Junta General está dividida en diferentes VLAN que contienen el tráfico de red corporativo (usuarios, servidores, Internet, gestión, etc.). Estas VLAN están

extendidas entre los edificios, conformando a efecto de comunicaciones locales una única infraestructura. La red local consta de diferentes equipos de comunicaciones con enlaces redundantes que permiten la operación de la misma en caso de fallo de alguno de los equipos.

La publicación de servicios en Internet se realiza mediante el cortafuegos, que gestiona las IP públicas asignadas a la Junta y que realiza los correspondientes procesos de redirección/NAT a efecto de conceder/denegar el acceso a los servidores o Internet.

Ambas ubicaciones cuentan con sistema de alimentación ininterrumpida y, en el caso del edificio del Palacio, grupo electrógeno.

3 Situación futura del centro de proceso de datos de la Junta General

El futuro centro de datos objeto de esta contratación pretende, entre otras cosas, renovar el actual hardware/software, actualizando diferentes elementos que se encuentran al final de su vida útil –bien sea por capacidad o por obsolescencia- y mejorar la disponibilidad de los servicios que se ofrecen.

Habida cuenta de la multitud de soluciones, productos, proveedores y elementos que pueden combinarse para dar solución a un determinado requisito técnico, se establecen en este punto un conjunto de principios generales de diseño que deberán ser tenidos en cuenta por los licitadores que presenten oferta técnica al lote 1 (el lote 2 y el lote 3 se corresponden fundamentalmente con suministro de licencias o SaaS).

Estos principios de diseño deberán servir como principios rectores de las ofertas a presentar y, por tanto, aquellas propuestas técnicas que se aparten de manera significativa de dichos principios serán puntuadas con un 0 en la memoria técnica preceptiva, justificando la mesa de contratación la correspondiente valoración en la puntuación obtenida.

- El CPD se constituirá como una solución distribuida entre los dos edificios de la Junta General. El concepto de CPD1 y CPD2 seguirá existiendo, pudiendo alojarse carga de trabajo de manera indistinta en cualquiera de las ubicaciones físicas y siendo el centro de datos un único elemento de gestión lógica.
- Los licitadores tendrán a su disposición dos líneas 10Gbe con terminación en fibra monomodo. Desde el punto de vista del tráfico se comportarán como dos fibras oscuras que se configurarán de forma obligatoria para transportar trafico Ethernet. Los licitadores podrán incorporar las VLAN que estimen necesarias o bien encapsular tráfico con otras características (FCoE, iSCSI o similar) siempre como tráfico Ethernet/IP, no estando los enlaces dedicados de forma exclusiva para este proyecto.
- La solución de almacenamiento a suministrar en el Lote 1 para las cabinas principales deberá tener en cuenta que de manera obligatoria se ubicará una cabina en cada una de las ubicaciones. La réplica de información entre las cabinas será síncrona.
- Para los elementos a suministrar y que se indiquen en el pliego y que enumeren fabricantes específicos se deberá entender que son esos fabricantes o equivalentes, ya que la elección de los mismos por parte de la Junta viene promovida por necesidades de compatibilidad de aplicaciones en funcionamiento. A efecto de demostrar la

equivalencia el licitador deberá exponer en su memoria técnica la idoneidad y justificación que le lleva a proponer un fabricante diferente al solicitado.

- La Junta General cuenta con racks con espacio suficiente para ubicar los equipos a suministrar. Las modificaciones del sistema eléctrico de los mismos, en caso de que fuera necesario, corresponden a la Junta General y se realizarán antes de la instalación física de los equipos. Dicha modificación no incluye la disponibilidad de PDU, regletas eléctricas o similar que deberán ser suministrados por el adjudicatario. En caso de que el adjudicatario estime necesario suministrar uno o varios racks adicionales para instalar sus equipos, deberá reflejar dicha situación en su memoria técnica a efecto de valoración por parte de la mesa de contratación.
- Forma parte del proyecto el despliegue una solución de publicación de escritorios y aplicaciones sobre Windows Server RDS. Los licitadores propondrán en su memoria técnica (Lote 1) una solución que contemple el uso de esta tecnología para publicar tanto aplicaciones independientes (RemoteAPP) como escritorios completos para hasta 200 usuarios. En la actualidad esta tecnología se encuentra funcionando en la Junta General sobre tecnología Windows Server 2012.
- Los licitadores tendrán en cuenta la normativa de la Junta General para la elaboración de sus propuestas, teniendo en especial consideración la de Política de Seguridad[1] de la Junta General (BOJG/X/C/29) ya que afecta directamente a los sistemas objeto de este contrato.
- Los trabajos correspondientes a la instalación, puesta en marcha y formación se desarrollarán de manera presencial en las instalaciones de la Junta General.

4 Documentación a entregar: memoria técnica

Los licitadores deberán entregar una memoria técnica para cada uno de los lotes a los que se presenten. En dicha memoria deberán describir claramente el cumplimiento de los requisitos y especificaciones técnicas descritas en el presente PPT (que tienen consideración de mínimos).

La valoración técnica de la oferta únicamente se realizará a partir de la documentación aportada por cada licitador para cada uno de los lotes en los que concurse. Toda referencia económica en la propuesta técnica supondrá la exclusión definitiva del proceso de licitación.

La propuesta técnica deberá incluir al menos los siguientes epígrafes explícitos perfectamente diferenciados:

a) Diagrama y descripción de arquitectura de la solución ofertada.

b) Descripción y explicación del funcionamiento de los sistemas indicando el cumplimiento del pliego y las diferencias que existan con el mismo.

c) Plan de trabajo detallado con actividades, tareas, previsiones y fechas. Se incluirá al menos un diagrama de Gantt con toda la planificación del proyecto.

d) Listado de elementos que componen la propuesta técnica: Descripción/características del elemento, función/objetivo y, en general, cualquier detalle que se considere relevante sobre el elemento a suministrar. Para el Lote 1, estimación de consumo energético del hardware suministrado. Condiciones de garantía y mantenimiento de los elementos suministrados.

[1] https://www.jgpa.es/ps

e) Documentos con especificaciones técnicas de todo el material suministrado para la ejecución del proyecto.

f) Plan de pruebas de aceptación que aseguren la correcta instalación y funcionamiento de los sistemas desplegados.

g) Plan de puesta en marcha de la solución instalada o desplegada.

h) Plan de soporte a posteriori de la solución ofertada: modelo de servicio, características del equipo de soporte.

i) Plan de formación al personal técnico de la Junta General del Principado de Asturias.

Cualquier indicación referida a precio (que será evaluado mediante fórmula matemática) que sea incluida en esta memoria causará la exclusión automática del licitador sin posibilidad de subsanación.

5 División en lotes

Debido a la naturaleza de los sistemas a contratar por la JGPA, se ha decidido dividir los mismos en 3 lotes, que son los siguientes:

- Lote 1: Renovación del centro de proceso de datos
- Lote 2: Suministro de licencias software antivirus con EDR y licencias MFA
- Lote 3: Suministro de licencias O365

6 Lote 1: Renovación del centro de proceso de datos

Este lote comprende el suministro, instalación y configuración de los elementos que conforman el nuevo CPD de la Junta General del Principado de Asturias.

Se entiende que la instalación y configuración básica de los mismos es un requisito para el funcionamiento de los elementos suministrados y como tal, va ligado a la puesta en marcha de la solución.

Toda la infraestructura, software, licencias y elementos que componen la solución se instalarán en paralelo al actual sistema de CPD existente. La Junta General suministrará espacio en los racks existentes, así como alimentación eléctrica en base a lo especificado por el adjudicatario en su memoria. Será responsabilidad del personal de la Junta General la migración de datos e información entre el actual CPD y la nueva infraestructura, así como el paso a producción del nuevo CPD una vez migrada la información.

El adjudicatario deberá suministrar cualquier elemento físico no descrito en la siguiente lista y que sea necesario para la puesta en marcha de la solución. Esto incluye cables de red Ethernet, cables de fibra, regletas PDU, cables eléctricos, etc. El licitador indicará en su memoria técnica el listado total de elementos a suministrar junto con sus características, así como las necesidades de conectividad de la solución de CPD con la red corporativa de la Junta General.

El adjudicatario tendrá por tanto la responsabilidad de realizar el suministro, instalar y configurar los sistemas de forma básica según los requisitos del pliego y su memoria técnica y realizar el traspaso de conocimientos al personal de la Junta General.

6.1 Elementos hardware

6.1.1 Servidores de virtualización

Se suministrarán al menos 5 servidores (denominado clase A) que se repartirán entre el CPD1 y el CPD2 para el entorno de virtualización.

Las características mínimas de los mismos serán:

- Formato 1U
- Doble procesador de 16 cores
- 256GB de RAM en módulos de 32GB o superior
- 2 discos duros locales SSD de al menos 200GB
- Conectividad ethernet 10Gb BaseT con al menos 8 puertos disponibles.
- Doble fuente de alimentación
- Garantía 5 años NBD (siguiente día laborable)

6.1.2 Servidor para backup/copias de seguridad

Se suministrará un servidor (denominado clase B) que se ubicará en el CPD1 para gestionar el sistema de copias y seguridad.

Las características mínimas del mismo serán:

- Formato 1U
- Un procesador de 8 cores
- 128GB de RAM en módulos de 32GB o superior
- 2 discos duros locales SSD de al menos 200GB
- Conectividad ethernet 10Gb BaseT con al menos 4 puertos disponibles.
- Conectividad Fiber Channel 16GB con al menos dos puertos disponibles
- Doble fuente de alimentación
- Garantía 5 años NBD (siguiente día laborable)

6.1.3 Switches para conectividad

Se suministrarán 4 unidades de switches dedicados a la infraestructura a implantar, dos para el CPD1 y dos para el CPD2.

Las características mínimas de los mismos serán:

- Capacidad de enrutamiento en L3
- Soporte para IPv6
- Soporte para 802.1D, 802.1p, 802.1Q, 802.3ad
- Soporte para protocolos de routing: Al menos RIP, OSPF y BGP
- Capacidad de apilamiento o stacking para gestión centralizada de varias unidades y que su comportamiento sea como único equipo a efectos de gestión y de trafico
- Al menos 24 puertos 10Gb Base-T
- Al menos 2 puertos SFP+ o superior
- Al menos 4 transceptores o adaptadores SFP+ para conexión 10GBASE-LR sobre fibra monomodo.
- Capacidad de conmutación: Al menos 600 Gbps
- Garantía 5 años NBD (siguiente día laborable)

6.1.4 Almacenamiento centralizado principal

Se suministrarán 2 sistemas de almacenamiento, uno para el CPD1 y otra para el CPD2. Ambas unidades, que se denominarán Cabina A y Cabina B, deberán ser del mismo fabricante, modelo y características, con la salvedad que se indica en la siguiente descripción.

Las características mínimas de cada una de las cabinas serán:

- Gama Enterprise o cabina de gama empresarial
- Monitorización 24x7 por parte del fabricante del sistema de almacenamiento.
- Doble controladora activo-activo real
- Todos los componentes de la cabina deberán contar con redundancia
- Disponibilidad 99,999% o superior
- 240GB de memoria cache o superior
- Capacidades de conexión sobre iSCSI y Fiber Channel
- Conectividad 10Gb baseT con al menos 8 puertos disponibles (4 al menos por controladora)
- Espacio neto disponible: 15TB en disco SSD/NVMe. El espacio neto se entenderá sin deduplicación/compresión y se calculará una vez aplicados los RAID, discos spare o cualquier sistema de redundancia de disco que permite la cabina de almacenamiento. El licitador propondrá el sistema de RAID y discos de reemplazo que considere adecuado según las mejores prácticas del fabricante de la solución. El destino de este espacio de

almacenamiento será el alojamiento de las máquinas virtuales y volúmenes de datos de la infraestructura de virtualización.

- Soporte para RAID 1, 5 y 6
- Posibilidad de conexión de discos SAS, NL-SAS y SSD
- Capacidades para provisionamiento ligero de volúmenes (Thin provisioning)
- Capacidades para Tiering dinámico.
- Capacidad para realizar al menos 512 snapshot por LUN
- Capacidad de crecimiento del sistema de almacenamiento mediante expansiones
- La cabina denominada Cabina A deberá incluir adicionalmente espacio neto disponible de 100TB en discos SAS/NL-SAS. El espacio neto se entenderá sin deduplicación/compresión y se calculará una vez aplicados los RAID, discos spare o cualquier sistema de redundancia de disco que permite la cabina de almacenamiento. El licitador propondrá el sistema de RAID y discos de reemplazo que consideré adecuado según las mejores prácticas del fabricante de la solución. El destino de este espacio será el alojamiento de los datos audiovisuales resultado de la actividad de la Junta General.
- Soporte 5 años 24x7 con tiempo de respuesta 4 horas

A modo de resumen, el adjudicatario suministrará dos cabinas con las anteriores características, una con 15TB SSD/NVMe y otra con 15TB SSD/NVMe y 100TB SAS/NL-SAS. Ambas cabinas tendrán replica síncrona sobre los volúmenes alojados en los discos SSD/NVMe y que tendrán alojadas los datos de la infraestructura de servidores.

6.1.5 Almacenamiento para copias de seguridad/backup

Se suministrará un sistema de almacenamiento para realizar la copia de seguridad a disco, que denominaremos Cabina C.

Las características mínimas del mismo serán:

- Procesador de 4 núcleos o superior
- 16GB de RAM o superior
- Doble fuente de alimentación
- Espacio neto disponible: 180TB. El espacio neto se entenderá sin deduplicación/compresión y se calculará una vez aplicados los RAID, discos spare o cualquier sistema de redundancia de disco que permite la cabina de almacenamiento. El licitador propondrá el sistema de RAID y discos de reemplazo que considere adecuado según las mejores prácticas del fabricante de la solución.
- Conectividad 10Gb baseT con al menos 2 puertos disponibles
- Conectividad 1Gb baseT con al menos 4 puertos disponibles
- Protocolos de acceso al almacenamiento: Al menos CIFS, NFS e iSCSI
- Garantía 5 años NBD (siguiente día laborable)

6.1.6 Autocargador Fiber Channel

Se suministrará un autocargador con conectividad FiberChannel para realizar la copia de seguridad a cinta.

Las características mínimas del mismo serán:

- Una unidad de cinta LTO 8 o superior. Si se suministrara una LTO de superior nivel, tanto las cintas limpiadoras como las cintas y las etiquetas deberán corresponder al nivel LTO suministrado.
- Conectividad FC 8Gb o superior
- Al menos 8 ranuras de cartucho
- Deberán suministrarse 2 cintas limpiadoras
- Deberán suministrarse 20 cintas LTO 8
- Deberá suministrarse un mínimo de 100 etiquetas de código de barras LTO 8
- Garantía 5 años NBD (siguiente día laborable)

6.1.7 Thin client

Se suministrarán 5 Thin client (sin monitor) con su correspondiente teclado y ratón. Estos equipos deberán integrarse en la solución de publicación de escritorio y aplicaciones con tecnología RDS/RemoteApp de Microsoft.

Las características mínimas de los mismos serán:

- Soporte hasta dos monitores con resolución 4k
- Al menos 2GB de RAM
- Al menos 8GB de disco local (memoria flash o equivalente)
- Tarjeta de red Ethernet 1Gb
- Soporte para conectividad inalámbrica WIFI
- Al menos dos puertos USB 3.0
- Puerto de audio con micro/altavoces.
- Soporte VESA

A efecto de elección del Thin Client el licitador deberá tener en cuenta que el objetivo de los mismos es el uso de la conexión a la solución Microsoft RDS/RemoteApp que se implantará con el nuevo CPD. El licitador propondrá el modelo que estime adecuado para dicho requisito, teniendo en cuenta las características físicas mínimas del mismo, pero sobre todo teniendo en cuenta el destino de este equipamiento.

6.2 Elementos software y licencias

6.2.1 Licencias Microsoft

6.2.1.1 Licencias Microsoft Windows Server 2022 Standard 16 core (o equivalente)

Se suministrará como mínimo un total de 30 licencias Microsoft Windows Server 2022 Standard 16 core.

6.2.1.2 Licencias Microsoft Windows Server 2022 Standard CAL User (o equivalente)

Se suministrará como mínimo un total de 200 licencias Microsoft Windows Server 2022 Standard CAL User.

6.2.1.3 Licencias Microsoft Remote Desktop Services CAL User (o equivalente)

Se suministrará como mínimo un total de 200 licencias Microsoft Remote Desktop Services CAL User.

6.2.2 Licencia Oracle Database Standard Edition 2 (o equivalente) para un procesador

Se suministrará licencia de Oracle Database Standard Edition 2 para un procesador con un año de soporte de fabricante.

6.2.3 Licencias Vmware vSphere (o equivalente)

Se suministrará licencia VMWare vSphere Standard (o equivalente) con suscripción básica para un mínimo de 10 procesadores, que cubrirán la licencia del sistema de virtualización para los 5 servidores solicitados. Si el licitador oferta por encima del mínimo de servidores indicados, deberá incluir las correspondientes licencias de vSphere Standard (o equivalente) a efecto de incorporar los servidores adicionales a la infraestructura de virtualización.

Se suministrará una licencia de Vmware vCenter Server Standard (o equivalente) con suscripción básica. Esta licencia permitirá la gestión centralizada de la infraestructura de virtualización.

Las licencias suministradas tendrán 5 años de soporte y suscripción básica.

6.2.4 Software de copia de seguridad

Se suministrará una nueva solución de software para realizar la copia de seguridad de los sistemas implantados a disco y a cinta.

Las características mínimas de la misma serán:

- Mínimo de 50 instancias a proteger, independientemente de la carga trabajo (física o virtual). El número de instancias a proteger podrá aumentar a futuro con la adquisición de las suscripciones o licencias correspondientes.
- El producto deberá permitir realizar copia de seguridad tanto a nivel de virtualización como a nivel detallado por cada una de las máquinas (a nivel de fichero, estado del sistema, etc.). No se admitirá como solución de backup sistemas basados únicamente en snapshots.
- El producto incluirá la capacidad de copiar en caliente con módulos específicos al menos las siguientes tecnologías: Oracle Database, SQL Server, Microsoft Active Directory y MySQL.
- El producto permitirá realizar copia de seguridad de al menos los siguientes entornos
    - Virtualización sobre tecnología VMWare
    - Virtualización sobre tecnología Hyper-V
    - Servidores Microsoft Windows Server
    - Servidores Linux
    - Amazon AWS
    - Microsoft Azure
    - Archivos compartidos
- La solución deberá permitir una gestión de la copia de seguridad mediante políticas o reglas de copia y retención, facilitando el ciclo de vida de la información salvaguardada
- La solución debe contemplar el aislamiento del sistema de copias de seguridad frente a ataques de ransomware. El licitador expondrá en su memoria técnica como la solución propuesta se enfrenta a esta problemática.
- La solución deberá estar integrada con los elementos que forman parte del suministro y en general el proyecto, con especial atención a la cabina de almacenamiento para copia a disco y el autocargador LTO. El licitador expondrá en su memoria técnica cómo se integra la solución a efecto de valoración de la misma por parte de la mesa de contratación.
- La solución debe permitir realizar copias de seguridad de Office 365, hasta 200 buzones de correo. El licitador indicará en su memoria técnica una descripción de cómo se realiza la copia de seguridad del entorno Microsoft 365 (capacidades propias del producto, uso de productos de terceros o acompañantes, etc.).
- El producto suministrado tendrá 5 años de soporte y suscripción básica.

6.3 Servicios profesionales de puesta en marcha y soporte de segundo nivel de la solución

El adjudicatario deberá desplegar los elementos que componen este lote teniendo en cuenta las siguientes consideraciones

- La solución que conforma la nueva arquitectura del CPD de la Junta General deberá coexistir en el tiempo con el actual sistema en producción.
- Una vez realizada la adjudicación definitiva, el adjudicatario establecerá el plan de trabajo definitivo en base a una toma de datos detallada y a los tiempos de provisión de equipos y licencias. Este plan de trabajo deberá ser aprobado por el responsable del contrato y establecerá el calendario de implementación del nuevo centro de datos.
- La decisión del paso a producción del nuevo CPD corresponderá al personal de la Junta General. Este paso se realizará en coordinación con el adjudicatario para contar con soporte in situ del personal asignado al proyecto en la fecha que se concrete.
- El adjudicatario deberá:
    - Realizar la instalación física del equipamiento: cabinas, servidores, equipos de comunicaciones y en general cualquier elemento hardware objeto del contrato.
    - Realizar la configuración lógica del equipamiento hardware
    - Realizar la configuración lógica y despliegue de software objeto del contrato: Hypervisores y virtualización, solución de copia de seguridad
    - Realizar una configuración básica de un sistema de publicación de escritorios y aplicaciones sobre tecnología Microsoft RDS sobre Windows Server 2022 (o superior en caso de que las licencias suministradas correspondan a una versión más reciente).
        - Instalar los diferentes servidores y roles en base a la arquitectura propuesta
        - Realizar un piloto de publicación de aplicaciones y escritorios con cinco aplicaciones seleccionadas por parte de la Junta General.
        - Las aplicaciones seleccionadas corresponderán a productos de uso interno y a aplicaciones de uso común (Microsoft Office, navegadores de internet).
        - Dado que en el Lote 2 se licita una solución de múltiple factor de autenticación (MFA) que deberá estar integrada con la solución RDS objeto de este lote, el adjudicatario del Lote 1 deberá coordinarse con el adjudicatario del Lote 2 a efecto de integrar dicha solución. No será en ningún caso responsabilidad del adjudicatario del Lote 1 asegurar el funcionamiento de la solución MFA más allá de la adecuada diligencia y colaboración que debe prestarse para dicha integración.
- Realizar cualquier trabajo asociado a la puesta en marcha que sea necesario para que los sistemas objetos del contrato puedan pasar a producción.
- Realizar la formación en los términos indicados en la memoria técnica.
- Independientemente del soporte de fabricante o de la garantía de los equipos y software suministrado, el adjudicatario deberá prestar un soporte técnico de segundo nivel de

toda la solución implantada en el Lote 1. Este soporte tendrá las siguientes características mínimas:

- Atención 8x5, de lunes a viernes en horario de oficina durante 5 años
- Interlocución con fabricantes para escalado de incidencias de soporte
- Gestión y resolución de consultas técnicas sobre los elementos objeto del lote
- Soporte para actualización evolutiva de los elementos objeto del lote (subida de firmware o versiones)
- Atención prioritaria en 24x7 para situaciones de caída completa del centro de datos. Este soporte podrá exigir, a decisión del responsable del contrato, la presencia in situ de técnicos del adjudicatario durante el evento de caída.
- Acuerdos de nivel de servicio (ANS) aplicables:
  - Catalogación de incidencias en baja, media, alta y crítica
  - Tiempo de respuesta para todas las incidencias excepto crítica: 4 horas
  - Tiempo de respuesta para incidencia crítica: 1 hora
  - Tiempo de resolución de incidencias críticas: 4 horas salvo causa justificada
- El adjudicatario entregará mensualmente un informe con los datos correspondientes al uso del soporte técnico de segundo nivel a efecto de verificar el cumplimiento de los ANS.

7 Lote 2: Suministro de licencias software antivirus con EDR y licencias MFA

Este lote comprende el suministro, instalación, puesta en marcha y formación de los elementos que se solicitan.

7.1 Software antivirus con EDR

El actual panorama de la ciberseguridad ha demostrado que las amenazas y riesgos a los que se enfrentan las organizaciones están en continua evolución y requieren una respuesta adecuada a dichos retos. A medida que la delincuencia informática avanzada y los ataques dirigidos se especializan, cada vez es más difícil mantener una protección adecuada a las infraestructuras tecnológicas.

Para mejorar la capacidad de respuesta de la Junta General del Principado ante esta situación, se solicita el suministro de una solución de antivirus con capacidades de EDR para sustituir a la existente en la actualidad.

Las características mínimas de la solución serán las siguientes

7.1.1 Elementos a proteger y vigencia

La solución dará protección completa a los siguientes elementos

- 160 estaciones de usuario Windows 10
- 70 servidores, incluyendo Windows Server y Linux
- 70 dispositivos móviles

La solución tendrá un periodo de vigencia de 36 meses (3 años), bien sea por suministro de licencia de uso y soporte o por suscripción.

7.1.2 Requisitos generales

- Todos los requisitos especificados deberán ser cubiertos por un único fabricante. Es decir, no se aceptarán soluciones que requieran vincular, enlazar o integrar distintas plataformas, consolas o productos de diferentes fabricantes. La gestión de la solución se realizará desde un navegador Web en la medida de lo posible.
- La solución deberá ser 100% nativa en cloud (nube). No se requerirá la instalación de ningún elemento físico o virtual en las instalaciones de la Junta General con la excepción de los agentes ligeros de software en cada elemento a proteger (endpoint).
- Los servicios en cloud del fabricante deberán estar alojados en centros de datos de la Unión Europea. El producto deberá estar cualificado como categoría MEDIA o ALTA en el ENS a fecha de presentación de las ofertas. A efecto de verificar la cualificación el licitador podrá presentar la documentación correspondiente o bien referenciar su producto en la guía CCN-STIC-105 "Catálogo de Productos y Servicios de Seguridad de las TIC" publicada por el Centro Criptológico Nacional.
- La solución deberá garantizar la continuidad del servicio y su disponibilidad 24x7x365. El licitador indicará en su memoria técnica la descripción de la arquitectura y cómo la solución propuesta cumple este requisito.
- La interfaz de usuario administrador/gestor de la solución podrá estar protegida con autenticación de dos factores.
- La solución debe proporcionar un control de acceso basado en roles para permitir el acceso y gestión de la misma con diferentes niveles de administración.
- La solución debe proporcionar una API robusta para integrarse con herramientas de terceros. El licitador indicará en su memoria técnica los datos sobre el funcionamiento de la API, incluyendo ejemplos de integración con productos estándar en el mercado (SIEM o herramientas de ticketing).

7.1.3 Requisitos técnicos del agente

- Sistema de agente simplificado.
- El agente a desplegar en los elementos protegidos deberá ser compatible y soportado en al menos los siguientes sistemas:
    - Windows Server 2019
    - Windows Server 2016
    - Windows Server 2012R2
    - Windows Server 2012
    - Windows 10
    - Windows 11
    - Servidores Linux x86_64
- La solución deberá ser compatible con sistema operativo Android e iOS
- El agente a desplegar debe ser ligero. Esto implica que se debe garantizar que el consumo de recursos por parte del mismo sea limitado. Cada licitador indicará en su memoria técnica cómo la solución propuesta gestiona el consumo de recursos a efecto de valoración.
- El agente a desplegar debe ser compatible con infraestructuras físicas y virtuales.

- La solución propuesta deberá disponer de capacidades de securización basadas en tokens o mecanismo similar para controlar la instalación/desinstalación de los agentes.
- El agente deberá permitir actualizaciones de software controladas por los administradores de la solución.
- El agente deberá enviar la telemetría extraída de su funcionamiento, así como los detalles forenses a la plataforma cloud en tiempo real. En caso de falta de conectividad entre el elemento protegido y el servicio en el cloud, el propio agente se encargará de almacenar y custodiar la información hasta que se restaure la conectividad, momento en que se realizará el envío.

7.1.4 Requisitos de la solución: funcionalidades de seguridad

- La solución debe comunicar las alertas de detección en tiempo real y proporcionar informes y cuadros de mando en tiempo real.
- La plataforma debe proporcionar un registro de auditoría de la actividad de los usuarios de la misma.
- El acceso bajo demanda a los metadatos relacionados con todas las amenazas generadas desde la plataforma deberá permanecer accesible durante al menos 30 días.
- El acceso bajo demanda a los detalles forenses de todas las amenazas detectadas por la plataforma deberá retenerse y permanecer disponible durante al menos 30 días
- El acceso bajo demanda al registro histórico completo de todos los eventos deberá retenerse y permanecer accesible durante al menos 30 días.
- La solución posibilitará la obtención de una réplica offline de los datos de los sensores para su análisis (descarga, exportación o mecanismo alternativo).

7.1.5 Requisitos de la solución: automatización ante eventos y orquestación

- La solución permitirá la creación de flujos de trabajo.
- Los disparadores de las acciones deben poder provenir de detecciones, auditoría de datos en el cloud o ejecución de flujos de trabajo.
- Acciones de respuesta. La solución debe incluir al menos las siguientes. El licitador describirá en su memoria técnica de forma detallada cómo funciona el mecanismo de respuesta.
    - Contención de red de un endpoint
    - Obtención y borrado de ficheros del endpoint.
    - Obtención de procesos y conexiones del endpoint

7.1.6 Requisitos de la solución: prevención y detección

- La solución propuesta deberá contar con capacidades de última generación que utilicen técnicas de aprendizaje automático/machine learning para la prevención previa a la ejecución de malware conocido y desconocido. Entre las capacidades de detección y

prevención deben incluirse la detección de técnicas, tácticas y procedimientos susceptibles de ser utilizados por agentes maliciosos.

- Las capacidades preventivas deben estar disponibles tanto en línea como fuera de línea, es decir, deben poder aplicarse las políticas definidas independientemente de si el puesto de trabajo o servidor se encuentra o no conectado a la red.
- Debe permitir la puesta en cuarentena de malware detectado y ofrecer la posibilidad de restaurar o poner en lista blanca los archivos de cuarentena directamente desde la plataforma de gestión.
- Debe disponer de la capacidad para la generación de listas de autorización y bloqueo de hashes de archivo personalizables
- Debe disponer de la capacidad para la generación de listas de autorización personalizables para archivos y directorios
- La plataforma debe proporcionar capacidades de detección basadas en el análisis de comportamiento posterior a la ejecución de un malware, permitiendo la protección contra las actividades habituales del ransomware (cifrado de archivos, eliminación de archivos sombra, etc.)
- Las prevenciones deben detener los ataques antes de que se produzcan daños en el sistema operativo. Por ejemplo, evitar la inyección de procesos antes de que se produzca, de modo que el proceso objetivo no se vea interrumpido o comprometido.
- La solución debe ser capaz de prevenir el uso malicioso de Powershell y los ataques con scripts
- La solución debe ser capaz de restringir el uso de USB en los endpoints de usuario incluyendo, pero sin limitarse al tipo de dispositivo y la función del mismo.
- La solución debe facilitar acciones de respuesta que incluyan al menos el aislamiento del endpoint o la conexión con el endpoint.
- La solución debe correlacionar y presentar automáticamente la telemetría y los metadatos (IOC) relacionados con el ataque en una línea de tiempo. Por ejemplo, argumentos de línea de comandos, escrituras de archivos, solicitudes DNS, conexiones IP, etc.
- La solución debe soportar la ingestión de IOC (hashes, ip, dominios y url), que se mantendrán en la plataforma por un periodo determinado de tiempo y que serán utilizados durante todo el ciclo de prevención/detección de la plataforma. Debe poder realizarse bloqueo de los IOC de tipo hashes y detección de los IOC de tipo dominio y hash.

- La solución debe correlacionar, cuando sea posible, el vector de infección y la intención de los atacantes de la amenaza en relación con la cadena de ataque, correlacionando con la telemetría, el árbol de procesos y la inteligencia de la amenaza.
- La solución debe proporcionar la capacidad de conectarse remotamente a los sistemas de destino con el fin de recopilar pruebas forenses adicionales (volcados de memoria completos, registro, archivos, etc.) y realizar tareas de remediación tales como cierre de procesos, modificación del registro de Windows, etc.
- La solución debe asociar el contexto del usuario (local o de dominio) con los eventos relevantes en todos los sistemas operativos de Microsoft
- La solución debe ofrecer en cada detección la información relativa al usuario, al host, a las vulnerabilidades presentes en el host, procesos, registro de sistema, actividades de red y resoluciones dns.

- La solución debe ofrecer una vista gráfica que permita observar el árbol de procesos relacionado con una detección.

7.1.7 Requisitos de la solución: búsqueda activa de amenazas

- La solución propuesta debe supervisar la actividad de procesos de los endpoints enviando de forma continua y en tiempo real información de eventos y detalles forenses a la plataforma cloud.
- La solución debe incluir capacidades de búsqueda histórica y en tiempo real totalmente personalizables.
- La solución debe proporcionar la capacidad de realizar una búsqueda de eventos sin procesar a través de toda la telemetría de eventos recopilada
- La solución debe proporcionar consultas predefinidas para todas las actividades relacionadas con el usuario y el punto final
- La solución debe proporcionar consultas predefinidas para artefactos forenses (por ejemplo, hash, dominio, eventos sin procesar, claves de registro)
- La solución debe proporcionar un informe que demuestre la cronología completa de los eventos de un proceso
- La plataforma debe permitir realizar búsquedas utilizando la interfaz de usuario. Estas búsquedas deben poder incluir: hashes específicos, nombres de fichero, parámetros de líneas de comandos, direcciones IP, dominios, eventos sin procesar, claves de registro, etc. La solución debe mostrar información detallada de cada endpoints en lo relativo a: Procesos y servicios, comandos ejecutados por herramientas de administración, actividad de Scripts, actividades relativas a registro, tareas programadas y políticas de Firewall, Actividades de red.

7.2 Solución de autenticación de factor múltiple (MFA)

La Junta General, a efecto de proteger adecuadamente el entorno de teletrabajo y acceso remoto corporativo, quiere implantar una solución de autenticación de factor múltiple. Esta solución permitirá mejorar la seguridad de acceso a los recursos protegidos, pudiendo incorporar una verificación adicional al par usuario/contraseña como podría ser una notificación al dispositivo móvil, un OTP (one time password), un token o una aplicación.

Dada la variabilidad de soluciones MFA que existen en el mercado, se exponen a continuación los requisitos mínimos que tendrá que tener la misma a efecto de que cada licitador proponga la que considere más adecuada.

7.2.1 Requisitos generales

- 200 usuarios protegidos con soporte y suscripción a 3 años

- Compatibilidad con entorno LDAP/Directorio activo para provisión de cuentas
- Seguridad multifactor en base a recursos o aplicaciones protegidas
- Autenticación mediante Push, QR y OTP
- Posibilidad de usar tokens hardware
- La solución debe ser compatible al menos con Microsoft Remote Desktop Services y soluciones VPN basadas en Radius.
- Se valorará que la solución permita la protección del inicio de sesión en equipos Windows 10/11.
- Se valorará la compatibilidad de la solución con productos de terceros como podrían ser Office 365, Google, etc.
- La solución debe contar al menos con una aplicación de autenticación para móvil (Android/IOS) de tal manera que se puedan usar dispositivos de terceros ajenos a la Junta.

El licitador entregará en su memoria técnica, tal como especifica este pliego en el apartado 4, los datos para la correcta valoración de la solución por parte de la mesa de contratación.

7.3 Servicios profesionales de puesta en marcha y formación

El adjudicatario deberá desplegar la solución de Antivirus con EDR y la solución de MFA en la Junta General.

Este despliegue incluirá al menos:

- Parametrización inicial en base a toma de requisitos una vez adjudicado
- Despliegue y parametrización personalizada de consolas
- Para el caso del antivirus con EDR, despliegue de agente sobre un subconjunto de elementos a proteger (puestos de usuario, servidores y teléfonos móviles).
- Para el caso de la solución MFA, construcción de un entorno de producción con ejemplos de autenticación fuerte.
- Definición de un conjunto de políticas base que puedan ser usadas como ejemplo o plantillas del sistema en producción.
- Formación de ambas soluciones al personal técnico de la Junta General del Principado de Asturias
- Independientemente del soporte de fabricante o de la garantía de los equipos y software suministrado, el adjudicatario deberá prestar un soporte técnico de segundo nivel de toda la solución implantada en el Lote 2. Este soporte tendrá las siguientes características
    - Atención 8x5, de lunes a viernes en horario de oficina durante 3 años
    - Interlocución con fabricantes para escalado de incidencias de soporte
    - Gestión y resolución de consultas técnicas sobre los elementos objeto del lote
    - Soporte para actualización evolutiva de los elementos objeto del lote (subida de versiones)

- Acuerdos de nivel de servicio (ANS) aplicables:
  - Catalogación de incidencias en baja, media, alta y crítica
  - Tiempo de respuesta para todas las incidencias excepto crítica: 4 horas
  - Tiempo de respuesta para incidencia crítica: 1 hora
  - Tiempo de resolución de incidencias críticas: 4 horas salvo causa justificada
- El adjudicatario entregará mensualmente un informe con los datos correspondientes al uso del soporte técnico de segundo nivel a efecto de verificar el cumplimiento de los ANS.

La responsabilidad del paso a producción de los sistemas objeto de este lote corresponde a la Junta General, y será llevada a cabo por personal propio, una vez se realice la formación y el traspaso de conocimientos.

Los licitadores indicarán en su memoria técnica toda la información relativa a la puesta en marcha y la formación de las soluciones a efecto de valoración por parte de la mesa de contratación.

8 Lote 3: Suministro de licencias O365

Dentro del proceso de transformación del centro de datos la Junta General necesita actualizar y renovar el conjunto de licencias de Microsoft Office que en la actualidad están en uso en la organización.

Este producto, ampliamente usado en prácticamente la totalidad de organizaciones e instituciones públicas, se encuentra ampliamente vinculado a la informática corporativa como requisito para el funcionamiento de alguna de las aplicaciones internas de la Junta, como puede ser AGORA (tramitación parlamentaria) y Sicalwin y Firmadoc (contabilidad y tramitación de expedientes).

Así, por tanto, para realizar la integración del modelo de publicación de escritorios y aplicaciones en los nuevos servidores que se van a desplegar y para dotar a la institución de un sistema de trabajo colaborativo en grupo (orientado a la necesidad de teletrabajo) se estima que la solución mas adecuada es dotar al personal de la institución de licencias Office 365, que permitirán cubrir los requisitos y las necesidades indicadas.

8.1 Licencias a suministrar

Se solicita el suministro y suscripción de las siguientes licencias de Microsoft Office 365

- 200 licencias Microsoft Office 365 Empresa Estándar a 3 años (36 meses)

8.2 Servicios profesionales: formación y traspaso de conocimientos

El adjudicatario deberá realizar una formación y traspaso de conocimientos sobre la suite Office 365 Empresa Estándar al personal de la Junta General, a efecto de que los funcionarios responsables de la operación del producto puedan gestionarlo con el conocimiento suficiente.

Esta formación incluirá al menos

- Descripción general de la suite: Productos incluidos, capacidades
- Integración de O365 en redes empresariales: Identidades, interconexiones y sincronización de datos. Asignación de licencias
- Autenticación en O365. Posibilidades en redes empresariales. Integración con federación de identidades (ADFS)
- Microsoft Teams: Gestión del ciclo de vida, administración básica
- Exchange 365: Administración general de la plataforma
- Usos prácticos de entornos 365. Arquitecturas híbridas, gestión de colas de correo, elementos de seguridad y mejores practicas en SPF, DKIM, DMARC, etc.

La responsabilidad del paso a producción de los sistemas objeto de este lote corresponde a la Junta General, y será llevada a cabo por personal propio, una vez se realice la formación y el traspaso de conocimientos.

Los licitadores indicarán en su memoria técnica toda la información relativa a la propuesta sobre la puesta en marcha y la formación de las soluciones a efecto de valoración por parte de la mesa de contratación.

Independientemente del soporte de fabricante o de la garantía de los equipos y software suministrado, el adjudicatario deberá prestar un soporte técnico de segundo nivel de toda la solución suministrada en el Lote 3. Este soporte tendrá las siguientes características

- Atención 8x5, de lunes a viernes en horario de oficina durante 3 años
- Interlocución con fabricantes para escalado de incidencias de soporte
- Gestión y resolución de consultas técnicas sobre los elementos objeto del lote
- Soporte para actualización evolutiva de los elementos objeto del lote (subida de firmware o versiones)
- Acuerdos de nivel de servicio (ANS) aplicables:
  - Catalogación de incidencias en baja, media, alta y crítica
  - Tiempo de respuesta para todas las incidencias excepto crítica: 4 horas
  - Tiempo de respuesta para incidencia crítica: 1 hora
  - Tiempo de resolución de incidencias críticas: 4 horas salvo causa justificada
- El adjudicatario entregará mensualmente un informe con los datos correspondientes al uso del soporte técnico de segundo nivel a efecto de verificar el cumplimiento de los ANS.

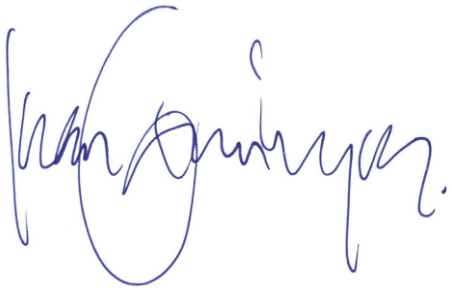
Oviedo, 21 de julio de 2022

DE: EL JEFE DEL SERVICIO DE TECNOLOGÍAS E INFRAESTRUCTURAS

A: LETRADO MAYOR

Adjunto se remite la Propuesta de Pliego de Prescripciones Técnicas que han de regir en el Concurso, por procedimiento abierto, para la renovación del centro de proceso de datos de la Junta General del Principado de Asturias.

EL JEFE DEL SERVICIO DE TECNOLOGÍAS E INFRAESTRUCTURAS



Juan Ángel Domínguez García