EANA | NAVEGACIÓN AÉREA ARGENTINA

Ministerio de Transporte
Presidencia de la Nación

ESPECIFICACIONES TÉCNICAS

EANA SE (EANA) se encuentra con la necesidad de contratar la "prestación del servicio de Datacenter", según los requerimientos que se mencionan a continuación. Estos servidores deben estar alojados en un Datacenter con características de Tier 3 (o superior) que incluya hardware, canal de comunicaciones, conectividad a internet, gestión y custodia de copias de respaldo y demás servicios asociados a un Datacenter externo con las características necesarias para asegurar la disponibilidad 99,982% con el SLA correspondiente.

Características del Servicio a Prestar:

EANA SE está interesada en tener bajo la modalidad de servicio de Datacenter, la infraestructura necesaria de hardware, software, bases de datos y comunicaciones; desde un Datacenter externo, que garanticen el correcto funcionamiento en desempeño y disponibilidad de las soluciones informáticas requeridas para su gestión.

El oferente de la solución, deberá administrar e integrar en los servicios del Datacenter, la infraestructura de Hardware de servidores, equipos de comunicaciones, cableado eléctrico, condiciones ambientales y de seguridad física, canales de comunicaciones redundantes, conectividad a internet, gestión y custodia de copias de respaldo (Backup) y demás servicios asociados al acceso a sistemas de información y servicios de un Datacenter externo.

El oferente deberá proponer para la implementación, las mejores prácticas y cumplimiento de los niveles de servicio, que permita lograr las condiciones de disponibilidad, desempeño y escalabilidad de los sistemas de información; y que le permita la prestación de los servicios administrados de la infraestructura, las comunicaciones y el mantenimiento de las bases de datos.

La implementación del Datacenter, deberá realizarse de conformidad al cronograma de implementación, lo que implica que los servidores y enlaces deben estar instalados, configurados y disponibles, en un máximo de tres (3) semanas, desde su adjudicación. Esta deberá incluir toda configuración o instalaciones que el oferente deba realizar sobre sus ambientes físicos y Lógicos.

Los servicios administrados que el oferente deberá brindar son:

1) El oferente deberá contar con un Datacenter del tipo TIER 3 o superior, según la norma estándar internacional ANSI/TIA-942 cumpliendo con todas las características que el TIER 3 supone:

a) Disponibilidad del servicio de 99,982%.
b) No más de 1,6 horas año de caída del servicio de Datacenter.
c) Deberá contar con múltiples líneas de distribución eléctrica y de refrigeración.
d) Redundancia de N+1 tanto en componentes, suministro eléctrico y refrigeración, protegiendo por lo menos 72 horas ante una caída total de suministro eléctrico.
e) Deberá tener niveles importantes de tolerancia a fallos al contar con todos los equipamientos básicos redundados incluido el suministro eléctrico, permitiéndose una configuración Activo / Pasivo.

f) Todos los servidores deben contar con doble fuente (idealmente) y en principio el Datacenter no requiere paradas para operaciones de mantenimiento básicas.

2) El oferente deberá tener certificado su Sistema de Gestión de la Seguridad de la Información bajo un marco de referencia o estándar de seguridad internacional (ISAE3402, Norma ISO27001, etc). Asimismo, el alcance del Sistema de Gestión de la Seguridad de la Información debe comprender todos los procesos involucrados en la prestación de los servicios de Datacenter (E2E).

3) Si los activos deben ser dados de baja o eliminados, la información debe ser destruida en forma segura, y el proceso de eliminación deben cumplir con las leyes y normas locales aplicables. Toda la información almacenada en el/los dispositivo/s debe ser borrada de forma segura. Si no es posible o práctico borrarla, el oferente es el responsable primario por la protección de los activos contra el uso, modificación, divulgación o destrucción no autorizados, accidentales o intencionales.

4) El oferente deberá presentar un Plan de Continuidad de Negocio, que contemple la disponibilidad en caso de interrupción de la actividad ante catástrofe, de manera tal que permita, en cualquier momento, continuar realizando la actividad en la República Argentina.

5) El oferente deberá contar con seguridad física que contemple lo siguiente:

a) Detección temprana de incendios, por sistema de aspiración. El oferente deberá informar sobre las marcas y modelos instalados.
b) Detección de incendios, por medio de detectores de humo y gases de combustión.
c) Extinción de incendios manual, con extintores manuales para el tipo de instalación.
d) Es deseable que el oferente disponga de personal de Seguridad y Seguridad contra incendios en Sitio.
e) El oferente deberá contar con un sistema centralizado de control de accesos, por medio de tarjetas de proximidad y/o control biométrico, para el ingreso a áreas sensibles. Se requiere el detalle del tipo y marca de sistema implementado.
f) El sistema de control de acceso, deberá sincronizar su reloj con el del CCTV. Deben referenciar al mismo servidor NTP con el cual se sincronizan el equipamiento informático.
g) Los eventos de apertura y acceso a través de puertas con lectoras de proximidad y/o dispositivos biométricos, deben ser registrados y almacenados por un período no menor a un (1) año. Los registros deben estar disponibles online.
h) El oferente deberá contar con la capacidad de asignar privilegios de acceso según rol funcional. En caso de utilizar credenciales, las mismas deben ser intransferibles, deben contar con la imagen del titular de forma que esta no pueda ser removida. Se deberá informar los perfiles de acceso (privilegio) que tengan incumbencia con el servicio.
i) El oferente deberá ofrecer visibilidad a los registros del sistema de control de accesos mediante un portal de solo lectura (auditoría).
j) El oferente deberá ofrecer informes periódicos, bajo demanda, de los eventos de acceso a salas/bastidores/áreas sensibles referidas en el servicio.
k) El oferente deberá poseer un plan de continuidad en caso de indisponibilidad del sistema de control de acceso. Se requiere detalle sobre los procesos de recuperación y plan de contingencia.
l) El oferente deberá contar con la capacidad de provisionar control de acceso biométrico. Informar el tiempo de provisión y tecnología empleada.
m) El oferente deberá ofrecer el cronograma de mantenimiento preventivo y correctivo de las instalaciones, así como también el informe del estado del sistema de control de acceso, bajo demanda.

6) El oferente deberá presentar certificados de los subsistemas, otorgadas por las entidades competentes, referidos a:

a) Certificado de Equipos de Aire Acondicionado.
b) Certificado de Planta Eléctrica.
c) Certificado de Detección y Extinción de Incendio (Norma IRAM 3579).
d) Certificado de Equipos de UPS.
e) Otros certificados relevantes.

7) A fin de demostrar la experiencia del oferente, el mismo deberá aportar DOS (2) contratos terminados dentro de los TRES (3) años anteriores a la fecha de presentación de la propuesta. El objeto de cada contrato certificado, deberá ser similar al objeto del presente proceso de selección, es decir que cada uno deberá cumplir con "PRESTACIÓN DEL SERVICIO DE DATACENTER QUE INCLUYA HARDWARE, CANAL DE COMUNICACIONES, CONECTIVIDAD A INTERNET, GESTIÓN Y CUSTODIA DE COPIAS DE RESPALDO Y DEMÁS SERVICIOS ASOCIADOS A UN DATACENTER EXTERNO". Las certificaciones deberán estar en papel membrete en original de la entidad contratante, y deberán contener Como mínimo la siguiente información:

Nombre del Contratante.
Nombre del Contratista.
Objeto del Contrato.
Fecha de inicio.
Fecha de terminación.
Fecha de expedición de la certificación.
Firma de quien expide el certificado.
Cumplimiento a Satisfacción.

8) De no cumplirse con los requisitos y/o no presentarse la certificación con los requisitos anteriormente mencionados, o si la información es incompleta, EANA solicitará se subsane las deficiencias y, si esto no sucede en el tiempo indicado, se rechazará la propuesta.
9) El oferente deberá contar con soporte 7x24x365.
10) El oferente deberá contar con un Datacenter del tipo "multicarrier", o sea, deberá permitir que EANA contrate vínculos de datos con otros proveedores, como por ejemplo Telefónica, Telecom, CenturyLink, Metrotel, Claro, etc.
11) El oferente deberá poseer el storage y los servidores certificados y homologados por y para SAP/HANA. Asimismo, deberá demostrar fehacientemente la certificación correspondiente.
12) El oferente deberá presentar el diseño o configuración de la solución que soportará los servicios indicados, previo al inicio de la implementación. En la revisión del cronograma de implementación se podrá realizar un ajuste de las capacidades y el diseño final.
13) Recuperación ante desastres de servidores en el Datacenter.
14) Administración, custodia y recuperación de Backups. Previa verificación del resultado exitoso de las copias realizadas.
15) La instalación y configuración de los enlaces de comunicaciones (Switching "Físicos y Virtuales", Router y Firewall).
16) El oferente deberá proveer un acceso a Internet de 100 Mb (o superior) para asignar a la red virtual donde estarán alojados los servidores.
17) Implementar y Configurar las reglas de protección perimetral firewall, IDS, IPS, Proxy, Balanceo de Cargas, Anti DDoS, Web Application Firewall.
18) Administración del Firewall, actualización de protecciones, bloqueo de puertos y acceso VPN, previo control de cambios aprobado por EANA SE.

19) El oferente deberá soportar la conexión de la red virtual, donde se encontrarán alojados los servidores que este servicio requiere, con otras redes tanto por vínculos MPLS, VPN IPSEC, o vínculos dedicados según corresponda. Asimismo, el oferente deberá contar con la posibilidad del armado de una red DMZ para poder publicar servicios directamente a Internet desde la red virtual correspondiente.

20) Se deberá proveer de un entorno de administración (por ej.: una página web) para que EANA realice la administración remota de los equipos (máquinas virtuales), donde se deberán poder realizar las siguientes tareas:

a) Inicio/Apagado/Reinicio de equipos.
b) Poder tomar control remoto de la máquina virtual.
c) Asignación de recursos tales como Memoria/Procesador/Disco/Placa de red/etc.
d) Asignación de parámetros de seguridad.
e) Manejo de la conexión de red de la máquina virtual.

21) El oferente deberá contar con un Centro de Operaciones de Seguridad (SOC por sus siglas en ingles) que contemple los siguientes puntos:

a) Contar con personal altamente calificado en seguridad las 24 horas, los 365 días del año.
b) Dispone de las últimas plataformas de gestión, correlación y análisis.
c) Contar con una sala para tratar casos de alta sensibilidad y de demos, que permite armar maquetas sin afectar a los entornos productivos.
d) Seguir las mejores prácticas del mercado.
e) Servicios de seguridad informática que incluyen la administración de infraestructura de seguridad, monitoreo y correlación de eventos y la gestión de vulnerabilidades.

22) El entorno de administración mencionado deberá permitir el armado de redes virtuales y la posibilidad de distribuir los servidores virtuales en las diferentes redes que se configuren.

23) El oferente deberá proveer acceso SSH/RDP a los servidores según corresponda.

24) El oferente deberá contar con un servicio de housing en caso de que EANA lo requiera.

25) El oferente deberá contar con acceso de VPN a la infraestructura mencionada.

26) El oferente deberá proveer monitoreo, reportes y gestión de alertas sobre las capacidades administradas de procesamiento, almacenamiento y enlaces de comunicaciones. Detalle de los reportes:

a) Capacidades de los servidores, en desempeño (CPU) y utilización de memoria y almacenamiento. Reporte mensual.
b) Habilitar las posibles consultas en línea que EANA así requiera.
c) Generación mensual de reportes de cumplimiento con los niveles de servicio acordados, con indicadores del servicio.
d) Reunión mensual/trimestral de seguimiento y evaluación del servicio con planes de acción de mejoramiento predictivo, preventivo y correctivo.

27) Soporte:

a) El oferente deberá contar con un numero de atención telefónica del tipo 0800, donde se puedan generar incidentes y pedidos de soporte.

b) El oferente deberá contar con un sistema de tickets para que, ante el reporte de un incidente o pedido, el oferente asigne un numero o identificación de este reporte, a fin de realizar el posterior seguimiento del mismo.

c) El oferente deberá contar con atención de incidentes de la infraestructura en el Datacenter, con cumplimiento de niveles de servicio acordados, según el documento que se pide en los “Acuerdos de Niveles de Servicio”.

d) El oferente deberá contar con análisis y gestión integral de los componentes que puedan estar afectando la disponibilidad y desempeño de los servicios.

e) El oferente deberá proveer toda actividad relacionada al correcto funcionamiento de la infraestructura y servicios prestados en el Datacenter.

28) En cuanto a los recursos necesarios para las máquinas virtuales, solicitamos respetar la tecnología de disco correspondiente a cada servidor, detallados en los Requerimientos de los Servidores. En el caso de los servidores con sistema operativo Linux Suse, estos deben contar con disco SSD, mientras que en el resto deben ser SAS/SATA.

EANA | NAVEGACIÓN AÉREA ARGENTINA

Ministerio de Transporte
Presidencia de la Nación

ACUERDO DE NIVELES DE SERVICIO.

El oferente deberá presentar en documento suscrito por el Representante Legal, la propuesta de Acuerdos de Niveles de Servicio, indicando:

- Servicios comprendidos.
- Tiempo de respuesta en Atención, Análisis y Solución de Incidentes.
- Logística de servicios (Procedimientos).
- Disponibilidad de Servicios.
- Condiciones de Cumplimiento de Disponibilidad / Multas o Descuentos por no cumplimiento.
- Niveles de Servicio de Soporte.
- Condiciones de cumplimiento de Niveles de Soporte / Multas o descuentos por no cumplimiento.
- Seguridad (acceso lógico, acceso físico, custodia copias de respaldo).
- Permanencia de servicios.
- Recuperación de servicios (Tiempos).
- Recuperación de Información.
- Contingencias de servicios.
- Confidencialidad.
- Control de cambios.

EANA | NAVEGACIÓN AÉREA ARGENTINA

Ministerio de Transporte
Presidencia de la Nación

Requerimientos de los servidores:

A continuación, se especifica el detalle de los equipos necesarios:

Entorno	Cant. CPU	Memoria Total (GB)	Storage S.O GB	Storage APP GB	Tecnolgia	Sistema Operativo
DESA	2	4	100	50	SATA/SAS	W. Server 2012/2016 R2
DESA	2	4	100	50	SATA/SAS	W. Server 2012/2016 R2
DESA	2	4	100	50	SATA/SAS	W. Server 2012/2016 R2
DESA	2	4	100	100	SATA/SAS	W. Server 2012/2016 R2
DMZ	2	4	100	50	SATA/SAS	W. Server 2012/2016 R2
DMZ	2	16	100	500	SATA/SAS	Ubuntu 16.04
DMZ	2	16	100	500	SATA/SAS	Ubuntu 16.04
DMZ	2	16	100	500	SATA/SAS	Ubuntu 16.04
DMZ	2	16	100	500	SATA/SAS	Ubuntu 16.04
PRD	2	4	100	0	SATA/SAS	W. Server 2012/2016 R2
PRD	4	8	100	0	SATA/SAS	W. Server 2012/2016 R2
PRD	4	8	100	1024	SATA/SAS	W. Server 2012/2016 R2
PRD	4	8	100	256	SATA/SAS	W. Server 2012/2016 R2
PRD	4	8	100	256	SATA/SAS	W. Server 2012/2016 R2
PRD	4	16	100	1024	SATA/SAS	W. Server 2012/2016 R2
PRD	4	8	100	512	SATA/SAS	W. Server 2012/2016 R2
PRD	4	8	100	512	SATA/SAS	W. Server 2012/2016 R2
PRD	2	4	100	1024	SATA/SAS	W. Server 2012/2016 R2
PRD	4	8	100	514	SATA/SAS	W. Server 2012/2016 R2
PRD	4	8	100	514	SATA/SAS	W. Server 2012/2016 R2
PRD	2	4	100	50	SATA/SAS	W. Server 2012/2016 R2
PRD	2	4	100	50	SATA/SAS	W. Server 2012/2016 R2
PRD	2	16	100	300	SSD	Linux Suse 12/15 for SAP App.
PRD	8	32	100	500	SSD	Linux Suse 12/15 for SAP App.
PRD	64	512	100	1024	SSD	Linux Suse 12/15 for SAP App.
PRD	2	16	100	300	SSD	Linux Suse 12/15 for SAP App.
PRD	8	64	100	1024	SSD	Linux Suse 12/15 for SAP App.
PRD	2	8	100	400	SSD	Linux Suse 12/15 for SAP App.
PRD	24	300	100	1024	SSD	Linux Suse 12/15 for SAP App.
PRD	2	16	100	300	SSD	Linux Suse 12/15 for SAP App.

EANA | NAVEGACIÓN AÉREA ARGENTINA

Ministerio de Transporte
Presidencia de la Nación

MATRIZ DE EVALUACIÓN

Grado de Cumplimiento Servicios de Datacenter

<OFERENTE>

A continuación clasificamos los requisitos de admisibilidad para la evaluación de propuestas de Prestación de S
Datacenter.

Grado de Cumplimiento	Descripción del grado de cumplimiento de los Requisitos de Admisibilidad	Valor
SI	Cumple	1
NO	No cumple	0

Solicitamos al Oferente completar en la tabla a continuación, columna C, con el mejor entendimiento
experiencia del Oferente el Grado de Adherencia (SI ó NO) de los servicios que propone.

Nro. de Requerimiento (identificador)	Requisitos de Admisibilidad	Grado de Cumplimiento	Puntaje Asignado
1	Datacenter TIER 3 o superior.		0
2	Subsistemas (A/A, Planta Eléctrica, Incendio, UPS, otros).		0
3	Certificación ISAE3402, Norma ISO27001, etc.		0
4	Dos contratos terminados.		0
5	Soporte 7x24x365.		0
6	Storage y servidores homologados para SAP/HANA.		0
7	Entorno de administración centralizada de recursos.		0
8	Contar con vínculos VPN site to site / VPN acceso.		0
9	Cumplimiento de Acuerdo de Niveles de Servicio.		0
10	Cumplimiento de requerimientos de servidores.		0
			0

PUNTAJE MÁXIMO	**100**
PUNTAJE OBTENIDO	**0**
% DE CUMPLIMIENTO	**0,00%**

NOTA: Cada Requisito de Admisibilidad (detallado en el cuadro) tiene un puntaje de 10 puntos. La no presentación/subsanación de cualquiera de los Requisitos de Admisibilidad y/o cualquier otro requisito mandatorio que se encuentra en la Especificación Técnica resultará en la descalificación técnica de la oferta.