



INSTITUTO FEDERAL DE
TELECOMUNICACIONES

"2021: Año de la Independencia"

ANEXO NÚM. 1

Servicios administrados de nube híbrida y soporte operativo



"2021: Año de la Independencia"

- e. El fabricante de cada solución deberá entregar un plan de trabajo detallado al proveedor, quien a su vez deberá consolidar en un único plan de trabajo que deberá entregar al Instituto, en el que se identifiquen actividades, responsables, tiempos y dependencias.
- f. Se deberá actualizar el firmware de los equipos a la última versión estable o versión recomendada por el fabricante de la solución.
- g. La interconexión de los equipos deberá realizarse por personal especializado en cableado estructurado, el cual deberá acreditarse ante el IFT previo a dicha actividad. El cableado UTP y las fibras ópticas deberán quedar perfectamente peinados, siendo responsabilidad del Proveedor considerar los materiales necesarios para dicho fin.
- h. Los fabricantes deberán ejecutar un conjunto de pruebas unitarias a fin de verificar el correcto funcionamiento de cada solución. Posteriormente, será responsabilidad del Proveedor coordinar la ejecución de una prueba integral que involucre la totalidad de la infraestructura que forme parte de la nube privada.
- i. Los fabricantes deberán generar la memoria técnica detallada de implementación de cada solución, siendo el Proveedor responsable de consolidar dichos documentos y hacer una entrega formal al Instituto.

2. Nube pública

El objetivo de este servicio consiste en aprovisionar recursos de cómputo externo al CPD Principal del Instituto bajo un modelo de cómputo en nube a fin de tener acceso a recursos virtuales bajo demanda. La nube pública deberá integrarse por servicios de nube nativa y por el servicio de VMware Cloud (VMC).

2.1. Características generales de la nube pública

- a. La solución propuesta debe encontrarse dentro del documento "Magic Quadrant for Cloud Infrastructure and Platform Services" publicado por Gartner en el mes de julio de 2021⁴.
- b. El fabricante de la solución de nube propuesta debe mantener un sitio Web actualizado y público en Internet donde se pueda consultar:
 - o Términos y Condiciones que rigen el tratamiento de los datos almacenados en la nube.
 - o Lista de subcontratistas autorizados para realizar actividades de procesamiento de datos específicas o actividades de administración de los centros de datos.
 - o Directivas de seguridad y las medidas técnicas y organizativas orientadas a la protección de los datos almacenados en la nube.

⁴ <https://www.gartner.com/document/4004076?toggle=1&refval=306703034&ref=solrAll>



"2021: Año de la Independencia"

- o Catálogo digital de productos y servicios disponibles para consumo, así como el precio unitario de estos. Debe contar con una calculadora de precios, en el que se pueda crear una estimación de costos.
- c. Debe estar reconocido en el sitio Web de VMware como proveedor de nube capaz de ofrecer la solución de VMware Cloud como servicio.
- d. Cuenten con certificaciones vigentes de seguridad emitidas por la autoridad certificadora correspondiente, en relación con los siguientes estándares o certificaciones:
 - o ISO 27001, 27017, 27018
 - o Cloud Security Alliance (CSA) STAR Level 2
 - o Contar con un programa de CIS Security Benchmarks o equivalente
 - o Comprobar que siguen las medidas de la Guidelines for Media Sanitization NIST 800-88 o NIST SP 800-88.
 - o Contar con enlaces conformes con FIPS 140-2 nivel 3
- e. Debe permitir definir clúster en múltiples zonas (2 o más zonas de disponibilidad) con replicación síncrona como mecanismo para robustecer el esquema de alta disponibilidad. La configuración inicial deberá considerar 2 zonas.
- f. Permitir migrar máquinas virtuales actualmente en el sitio hacia la nube sin apagarlas (en caliente) presentando la infraestructura como remota o fuera de sitio en calidad de desborde dentro de la misma red lógica.
- g. Proveer la capacidad de recuperación ante desastres en sitio hacia la nube mediante Software como Servicio (SaaS) completamente gestionado y automático.
- h. Ofrecer un modelo de recuperación ante desastres mediante arquitectura tipo Pilot-light con pruebas, planes, reportes y monitoreo incluidos.
- i. Ofrecer la posibilidad de migrar automáticamente instancias locales a la nube en un escenario de recuperación de desastres.
- j. Las interfaces de red entre los servidores físicos o nodos (hosts) deben ser de al menos 25Gbps.
- k. Los servicios de soporte podrán ser prestados vía remota, de acuerdo con las siguientes características:
 - o El soporte base incluido en el servicio debe ser 5X24 con soporte de nivel productivo sin costo adicional.
 - o Ofrecer el estado del servicio con notificaciones en un sitio web público.
 - o Ofrecer algún sistema de notificaciones a los usuarios cuando exista un mantenimiento programado que podría interrumpir potencialmente la disponibilidad / el tiempo de actividad de las instancias.
 - o Ofrecer mecanismos para evitar interrupciones / tiempos de inactividad de las instancias cuando el proveedor realiza mantenimiento al hardware.
 - o Contar con un servicio de alarmas y/o notificaciones en los siguientes casos:
 - Alarma de umbrales (70% del consumo) para almacenamiento, cómputo y RAM.