Informe Pericial

Basados en lo que ampara el articulo No. 3 de la Ley 340-06 de fecha 18 de agosto del 2006, modificada por la Ley No. 449-06 y el Decreto 543-12 de fecha 06 de septiembre del 2012 que aprueba el Reglamento de la Ley de Compras y Contrataciones, la cual establece cuales procesos conforme a la misma entran en la categoría de Proceso por excepción, como proveedor único, tengo a bien rendir un informe pericial del por qué el proceso en cuestión cabe dentro de esta modalidad.

Antecedentes:

El principal problema que enfrenta el Centro de Datos del Estado Dominicano es la ausencia de una solucion de respaldo y resiliencia que cumpla con los estandares de DataCenter y pueda sopor la alta demanda de las instituciones Gubernamentales, mitigando cualquier tipo de ataques, interrupción o desastres que en este concierne. Evitando que pueda afectar la continuidad de las operaciones y la alta disponibilidad del servicio Cloud que utilizan las instituciones gubernamentales importantes, tales como la misma OGTIC. Adicional, en materia de adopción tecnológica aporta al gobierno como iniciativa a la transformación digital que se viene fomentando en la agenda digital 2030.

El Centro de Datos del Estado Dominicano, se construyó con el objetivo de brindar una moderna plataforma donde las instituciones estatales puedan alojar su procesamiento de cómputos, su contingencia y obtener servicios seguros, garantizado alta disponibilidad y ahorros en sus procesos operativos.

Entre los principales servicios brindados se encuentra en operación la Nube computacional, a la que llamamos OGTICLOUD, que ofrece lo siguiente: 1) **Infraestructura como servicio** (IAAS), 2) **Plataforma como servicio** (PAAS), 3) **Software como servicio** (SAAS), 4) **Servicio de alojamiento de portales**, 5) **Alojamiento de correos institucionales, entre otros.**

Por otro lado, también se brindan servicios a proyectos de índoles gubernamental como lo son: La plataforma de interoperabilidad, El programa burocracia cero, Gobierno eficiente, FirmaGOB, El Sistema Integrado de Gestión Institucional (SIGEI), El Data Warehouse Gubernamental, entre otros.

Debido a la alta demanda de los proyectos que se están desarrollando en el Centro de Datos del Estado Dominicano surge la necesidad de adquirir la **SOLUCIÓN DE RESPALDO Y RESILIENCIA,** el cual consiste en una plataforma de equipos con una Infraestructura centralizada para respaldo de 30 TB de datos: VM, aplicaciones y base de datos. La infraestructura de respaldo también debe incluir una infraestructura aislada y desconectada que proteja contra ataques cibernéticos y de ransomware realizando las copias de los respaldos.

En vista al proyecto ya mencionados, fue necesario solicitar la adquisición de la solución de respaldo y resiliencia, creado con la necesidad de cumplir con las peticiones de alto volumen y flujo de datos por parte de las instituciones del Estado Dominicano.

Justificación Solución de Respaldo y Resiliencia

Cabe destacar que los riesgos de un ataque cibernético o de ransomware van en aumento, todas las semanas al menos una empresa es atacada y secuestrados sus datos, los pagos requeridos son cuantiosos y se daña o lesiona la reputación comercial de las empresas afectadas.

En cada caso de un ataque cibernético la empresa e instituciones deja de operar por días o semanas, en cada ataque las empresas e instituciones sufren pérdidas cuantiosas de datos.

La probabilidad de que ocurra un evento de ataque cibernético o de ransomware es bastante alta, incluso la probabilidad de que ocurra un evento de este tipo es mayor a cualquier otro tipo de riesgo tradicional.

Las estrategias de protección de datos, recuperación ante desastres y continuidad operativas debe ser reevaluadas y rediseñadas para poder **sobrevivir a un *ataque cibernético destructivo o ransomware.***

A través de la Solución de Respaldo y Resiliencia, lograríamos cubrir los siguientes puntos:

- Cubrir las altas demandas de conexiones simultaneas al Centro de Datos del Estado Dominicano.
- Protege contra programas malignos(malware), exploits y sitios web maliciosos en tráfico cifrado y no cifrado.
- Recuperación ante desastres y continuidad operativas.
- Prevenir y detectar ataques conocidos y desconocidos utilizando inteligencia artificial.
- Seguridad e integridad del flujo de la información trasmitida.

Recomendación:

Con todo lo antes mencionado se recomienda realizar la contratación del servicio de equipos de comunicaciones y seguridad firewall para el Centro de Datos del Estado Dominicano, con el objetivo de continuar nuestras operaciones y cubrir la alta demanda actual de nuestros clientes.

Es necesario realizar la contratación del servicio de equipos de comunicaciones y seguridad firewall para los servicios de conectividad ya existentes y proyectados en el Centro de Datos del Estado.

A espera de que este informe sea útil para una acertada decisión en la contratación del servicio, se despide de usted.

Kaking Choi
Director del Centro de Datos del Estado
KC.-