

BOLETIN DE ACLARACIONES NRO. 2
“ADQUISICIÓN SISTEMA DE RESPALDOS”
CÓDIGO: EC-L1253-P00009

El presente BOLETÍN DE ACLARACIONES se lo emite según lo estipulado en las Políticas para la Adquisición de Bienes y Obras financiadas por el Banco Interamericano de Desarrollo GN-2349- 15, en la Sección B. Documentos de Licitación, en el numeral 2.25 “(...) Toda información, aclaración, corrección de errores o modificación adicional de los documentos de licitación se debe enviar a cada uno de los posibles oferentes que adquirieron los documentos de licitación originales, con tiempo suficiente respecto a la fecha fijada como límite para la recepción de las ofertas, a fin de que los oferentes puedan tomar medidas apropiadas. De ser necesario, se debe prorrogar la fecha límite. El Banco debe recibir una copia (por escrito o en forma electrónica) y debe ser consultado con respecto a una notificación de no objeción cuando el contrato esté sujeto a revisión ex-ante (...); y, en cumplimiento a la Solicitud de Ofertas en la Sección I. Instrucciones a los Oferentes (IAO) en el numeral 8. Aclaraciones al Documento de Licitación, en consideración a la etapa de preguntas, esta comisión procede con la elaboración del siguiente boletín de aclaraciones a las preguntas realizadas por los participantes:

1. En el archivo de Especificaciones Técnicas, página 87, se solicita: “Estar diseñada para soportar un esquema de alta disponibilidad, sin puntos únicos de falla (fuentes de poder, arreglos de discos, interfaces de conexión, funcionamiento en clúster, entre otros).”

Pregunta: En este ítem se solicita “funcionamiento en clúster”, por favor indicar si se deben colocar 2 equipos en clúster para cada repositorio. Sino por favor indicar como se necesita la configuración para el funcionamiento en clúster. Al ser equipos especializados en backup no usan características de clúster, a menos que se coloque equipos de almacenamiento de propósito general.

RESPUESTA:

Estimado oferente favor remitirse al Boletín de Enmiendas No. 5, Enmienda No. 1

2. En el archivo de Especificaciones Técnicas, página 88, se solicita: “En caso de que la capacidad del enlace entre el CPD principal – CPD alterno (180 Mbps) no sea suficiente para asegurar el correcto funcionamiento de la solución, el proveedor podrá instalar un enlace dedicado con un proveedor de servicio exclusivo que asegure la ejecución de la réplica entre los repositorios 1 y 2. “. Pregunta: Por favor indicar si la replica entre los repositorios 1 y 2 será de la capacidad total de cada repositorio sino indicar el porcentaje. De igual manera indicar si la replica será bidireccional o solamente unidireccional.

Handwritten signatures and initials:
A
A

RESPUESTA:

- La réplica entre los repositorios 1 y 2 será de la capacidad total, a excepción de la capacidad asignada para realizar pruebas de respaldos y restauraciones regulares.
 - El tráfico de transferencia de la réplica del repositorio 1 al repositorio 2 será unidireccional.
3. En el archivo de Especificaciones Técnicas, página 88, se solicita: “Encendido y apagado del software de respaldos.”. Pregunta: Por favor indicar a que se refiere con encendido y apagado del software de respaldos. Generalmente para deshabilitar una aplicación se baja el servicio asociado con el sistema operativo. ¿O se refiere a encendido y apagado de los repositorios?

RESPUESTA:

Estimado oferente favor remitirse al Boletín de Enmiendas No. 5, Enmienda No. 2

4. En el archivo de Especificaciones Técnicas, página 89, se solicita: “Las versiones de respaldos deben ser inmutables, es decir no podrá modificarse o borrarse luego de que la versión del respaldo sea considerada consistente y libre de malware (como por ejemplo ransomware). Estimada entidad, se indica Las versiones de respaldos deben ser inmutables, es decir no podrá modificarse o borrarse luego de que la versión del respaldo sea considerada consistente y libre de malware, pero no se especifica de qué forma se considerará que el respaldo está libre de malware. Según los consultores internacionales como Gartner, para detectar malware tipo ransomware, se debe contar con una herramienta de Machine Learning para poder detectar el ransomware. Por favor indicar si la responsabilidad de emitir el informe de que la versión de respaldo esta libre de malware tipo ransomware será de la institución o debe ser realizada por el proveedor a través de alguna herramienta de machine learning?”

RESPUESTA:

Favor referirse a lo determinado en la Sección VI. Requisitos de los Bienes y Servicios Conexos, numeral 3.2.1. Componentes de Infraestructura. Características de seguridad, Pág. 89:

...

La solución ofertada debe contar con técnicas de inteligencia artificial/machine learning al menos en el repositorio 2, tanto para la metadata como para los datos de respaldo, que permitan:

- Analizar las copias generadas para identificar los respaldos saludables y posibles anomalías e incidencias de malware (como por ejemplo ransomware). En caso de que se descubran archivos que hayan sido modificados, éstos deberán reemplazarse con la última versión buena conocida.
- Habilitación y configuración de al menos 3 técnicas de detección de anomalías de los respaldos (cada técnica con un criterio diferente). Se espera que las técnicas usen criterios como: detección de patrones anómalos, tasas de cambio de los respaldos, nivel de entropía, series temporales, entre otros.
- Incluir mecanismos de respuestas configurables cuando se detecta un evento anómalo, e identificar actividades de contención.
- Identificar el punto de recuperación, basado en un respaldo saludable para iniciar con los procesos de restauración.
- Ser capaz de identificar los diferentes vectores de ataques conocidos (como por ejemplo malware - ransomware) en las copias de seguridad de la bóveda como: Cifrado, cifrado parcial, cifrado y cambio de extensión en el nombre, reemplazo del tipo de archivo, combinación única de archivos, movimiento de archivos de sus rutas dentro del sistema de archivos original, entre otros.
- El análisis de los datos respaldados en los repositorios deberá efectuarse al menos en un 60% del total.

...

- La Sección VI. Requisitos de los Bienes y Servicios Conexos, numeral 3.5.1.1. Configuración. Configuración de hardware y software de la solución de respaldos, Pág. 102, 103 :

...

- Se deben ejecutar las actividades de acuerdo con el plan de configuración de la solución ofertada.

...

- Habilitación de las características de inmutabilidad durante todo ciclo de vida del respaldo. Se debe presentar evidencias del funcionamiento de esta característica.

...

- Configuración de la identificación de respaldos saludables usando técnicas de machine learning. Al menos se debe tomar en cuenta:

- Habilitación y configuración de al menos 3 técnicas de detección de anomalías de los respaldos (cada técnica con un criterio diferente). Se espera que las técnicas usen criterios como: detección de patrones anómalos, tasas de cambio de los respaldos, nivel de entropía, series temporales, etc.

- Con el uso de al menos tres técnicas de análisis de comportamiento anómalos se debe clasificar un respaldo como saludable.

- Los modelos de detección de anomalías deben afinarse con los datos generados por los respaldos del SRI.



- Los análisis de puntos saludables deben realizarse en el origen, mientras se realiza la copia y cuando se restaura la información.
- Se debe presentar un análisis prescriptivo de las posibles alternativas de restauración en caso de infección de malware.

5. En el archivo de Especificaciones Técnicas, página 91, se solicita: “Algunos campos de las bases de datos almacenan archivos tipo JSON, XML, PDF, entre otros, lo cual debe ser considerado para el cálculo para la tasa de eficiencia del almacenamiento.”. Pregunta: Por favor indicar un porcentaje del Tamaño Total de las Fuentes Estructuradas que corresponde a los archivos tipo JSON, XML, PDF, entre otros.

RESPUESTA:

Estimado oferente, favor remitirse al Boletín de Enmiendas No. 5, Enmienda No. 3

6. En el archivo de Especificaciones Técnicas, página 94, se solicita: “En caso de activación del CPD alternativo como ambiente de producción, el repositorio 2 debe proveer los mismos niveles de RPO y RTO definidos para el repositorio 1, manteniendo el tiempo de retención de al menos 30 días. El inicio de la activación del CPD alternativo deberá ser comunicada por parte del Administrador del contrato.” Pregunta: Este requerimiento no es posible cumplir ya que al Repositorio 2 solo se envía la última copia de cada día y no las copias de cada hora como se guardan en el Repositorio 1. En ese caso el RPO de Repositorio 1 es de 1 hora, pero el RPO en el Repositorio 2 es de 24 horas.

RESPUESTA:

Estimado oferente favor remitirse al Boletín de Enmiendas No. 5, Enmienda No. 4

7. Estimada entidad en el documento especificaciones técnicas solicita “ En caso de que la capacidad del enlace entre el CPD principal – CPD alternativo (180 Mbps) no sea suficiente para asegurar el correcto funcionamiento de la solución, el proveedor podrá instalar un enlace dedicado con un proveedor de servicio exclusivo que asegure la ejecución de la réplica entre los repositorios 1 y 2. Por favor indicar el porcentaje de consumo del canal en horario de oficina y fuera de oficina, y así establecer la validez para usar este canal para la sincronización o hay que incluir uno adicional. Favor confirmar



RESPUESTA:

El enlace de datos con capacidad de 180 Mbps será dedicado únicamente para el tráfico de réplica de la solución de respaldos ofertada, el cual no tiene ningún consumo actualmente.

En caso de que la capacidad del enlace entre el CPD principal – CPD alterno (180 Mbps) no sea suficiente para asegurar el correcto funcionamiento de la solución, el proveedor podrá instalar un enlace dedicado con un proveedor de servicio exclusivo que asegure la ejecución de la réplica entre los repositorios 1 y 2.

