# FICHA TECNICA PARA ADQUISICION DE BIENES O SERVICIOS

| | | |
|---|---|---|
| | Proceso: Compra y Contrataciones | Código: FR-CYC-004 |
| | Versión: 01 | Fecha: 05-May-2022 |

| Dirección o División Solicitante: | Indique si es un Bien o Servicio |
|---|---|
| Dirección de Tecnología de la Información y Comunicación | Bien |

**Código del Catálogo de Bienes y Servicios (CBS)**

4321 - Equipo informático y accesorios

**DETALLE REQUERIMIENTO**

| Nombre del Bien o Servicio: | Código Dynamics: | Cantidad: |
|---|---|---|
| PROYECTO IMPLEMENTACION SITIO ALTERNO PARA CONTIGENCIA | SOC2022-000261 | 1 |

**Descripción del Bien o Servicio**

Adquisición de una solución de respaldo de datos, continuidad operación y recuperación antes desastres, que permita a INAPA garantizar la integridad de su data y poder seguir operando en caso de un desastre, tanto de forma local como desde un lugar alterno.

**Especificaciones Técnicas**

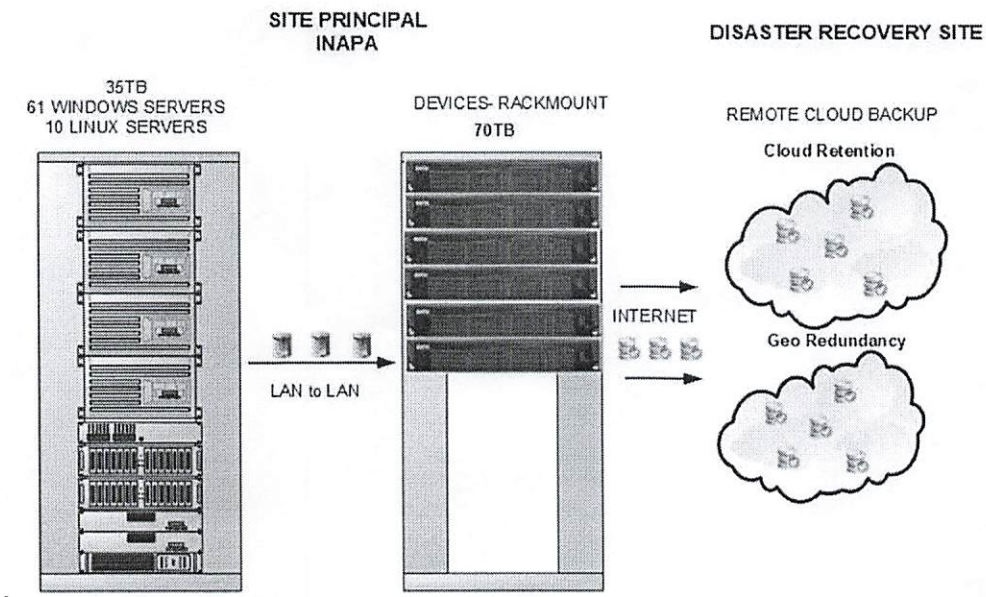
| | |
|---|---|
| 1- La solución requerida debe proveer licencias ilimitadas para la protección de los Servidores y/o estaciones de trabajo requeridas por un periodo de tres (3) años. | 2 -La solución debe permitir la virtualización completa (incluyendo el Sistema Operativo) desde el dispositivo, device o appliance en caso de contingencia en la misma red LAN local, tanto de servidores físicos como virtuales, así como laptop o Workstation, sin depender de la infraestructura de INAPA para garantizar la continuidad de operacional. |
| 3 -Se deben incluir todas las funcionalidades requeridas en estos requerimientos, así como las licencias y equipos necesarios para las mismas por un período de tres (3) años. | 4 -La solución debe permitir el respaldo de los siguientes sistemas operativos y versiones de Windows: Windows XP Service Pack 3, Windows Storage Server 2003, Windows Server 2003 Service Pack 2, Windows Server 2008 R2 Service Pack 1 o superior, Windows Small Business Server 2011, Windows 7 Service Pack 1, Windows 8 , Windows 8.1, Windows 10 , Windows Server 2012, Windows Server 2016, Windows Server 2019. |
| 5 -La solución debe permitir el respaldo de los siguientes sistemas operativos y versiones de macOS: macOS versión 10.10 (Yosemite), macOS versión 10.11 (El Capitan), macOS versión 10.12 (Sierra). | 6 -La solución debe permitir desde su repositorio virtualizar usando los recursos del Hipervisor de la institución en un ambiente virtual VMware. |
| 7 -La solución debe contar y poder ser gestionada, administrada y monitoreada directamente a través de una consola centralizada y/o un portal centralizado de gestión de la solución de respaldo y continuidad del negocio. | 8 -La solución debe permitir el respaldo de los siguientes sistemas operativos y versiones de Linux : Red Hat Enterprise Linux/CentOS 6.6 hasta 6.10, Red Hat Enterprise Linux/CentOS 7.x, Ubuntu 16.04, Ubuntu 18.04, Debian 9 /10 , Fedora 29/30/31 , open SUSE Leap 15, open SUSE Leap 15.1 , open SUSE Leap 42.3 , Oracle Enterprise Linux 6 y 7, SUSE Linux Enterprise 12 SP 3 / SP 4 / SP 5, SUSE Linux Enterprise 15 y 15 SP 1 |
| 9 -La solución debe permitir respaldos desde cada 5 minutos en adelante. | 10 -La solución debe de realizar una verificación Local (Local Verification) de la integridad y/o de la salud del File System y de cada volumen a proteger. |
| 11 -La solución debe de incluir detección de Ransomware integrada. | 12 -La solución debe de incluir Screenshot Verification. Cada copia de seguridad realizado debe ser virtualizado para validar que se trate de imágenes funcionales y validas. |
| 13 -La solución debe permitir la exclusión de volúmenes no deseados. | 14 -La solución debe de incluir verificación de aplicaciones como Microsoft SQL Server, Microsoft DHCP Server, Microsoft Active Directory Domain Server y Microsoft DNS Server. |
| 15 -La solución debe permitir la exclusión VSS Writers de Windows. | 16 -La solución debe permitir crear NAS Share. |

| | |
|---|---|
| 17 -La solución debe permitir crear iSCSI Share disk. | 18 -La solución debe permitir la expansión del espacio del dispositivo en línea sin downtime. |
| 19 -La solución debe permitir restauración independiente de Archivos o Directorios (File and Folder). | 20 -La solución debe permitir restauración de volumen(s) a un iSCSI target. |
| 21 -La solución debe permitir restauración un restore point a un ESX host. | 22 -La solución debe permitir exportar las imágenes en formato VHD, VHDX, VMDK, or VMDK-linked. |
| 23 -La solución debe permitir restauración usando la opción de Bare Metal Restore (BMR) sin importar la marca o modelo del hardware utilizado por INAPA para hacer una restauración (restore back) a un sistema físico o un sistema virtual. | 24 -La solución debe permitir la replicación entre dispositivos o cajas ejecutando una réplica en "nube privada". |
| 25 -La solución debe ser capaz de activar la IP del sistema original de formar manual (debe ser colocada manualmente) una vez se active en el virtualizador local o nube; esto con el fin de evitar conflictos con la IP original de los servidores. | 26 -La solución debe tener la autenticación y seguridad de doble autenticación para permitir la entrada a la Consola Administrativa Centralizada (Dashboard) de la solución. |
| 27 -La solución debe permitir realizar upgrade de RAM en el mismo dispositivo o device (appliance). | 28 -La solución debe permitir realizar upgrade de discos para expandir o añadir más espacio en el mismo dispositivo (appliance). |
| 29 -La solución debe permitir la encriptación de las imágenes de manera local, usando cifrado en AES de 256 bits en formato de modo XTS. | 30 -La solución debe permitir que los datos permanezcan protegidos por el cifrado AES-256 bit durante todo el proceso de sincronización, almacenamiento y replicación. |
| 31 -La solución debe conectarse o integrarse con el Active Directory del cliente. | 32 -La solución debe permitir configurar el horario de Respaldo (Backup) Local por Servidores de forma independiente. |
| 33 -La solución debe permitir activar o virtualizar varias imágenes simultaneas de diferentes servidores en el mismo dispositivo o device o caja (appliance) y/o permitir la recuperación de datos al mismo tiempo de diferentes imágenes. | 34 -La solución debe indicar la salud (System Health) del dispositivo (appliance), así como la información de los discos, memoria, cpu, velocidad y temperatura. |
| 35 -La solución debe permitir la capacidad de recuperación granular para Microsoft Exchange, SharePoint y SQL Server. | 36 -La solución debe permitir la pausa de los respaldos (backup) de cada Servidor o estaciones que fungen dentro del core operacional de forma independiente. |
| 37 -La solución debe permitir crear las políticas de retención local de las imágenes personalizadas, donde se pueda indicar el periodo de tiempo que se guardaran las imágenes diarias, semanales y mensuales. | 38 -La solución debe incluir reportes diarios, semanales o mensuales y notificaciones de alerta tanto de fallos, críticos, o advertencias (warnings) o diagnósticos de Log para ser recibidas vía correo electrónico de forma automática. |
| 39 -La solución de incluir la función de archivado del agente, es decir permitir guardar la data de un server que no será más nunca respaldado dentro del mismo dispositivo (appliance). | 40 -La solución debe permitir comparar dos imágenes o puntos de recuperación para determinar que archivos han cambiado, son nuevos o han sido borrados entre ambas imágenes comparadas. |
| 41 -La solución debe permitir el borrado de las imágenes de forma independientes de cada servidor sin alterar la secuencia de los respaldos, retención, ni impactar en la restauración o virtualización de los servidores. | 42 -La consola de administración centralizada debe permitir la visualización de eventos como respaldos ejecutados, imágenes sincronizadas e incluso los screenshot verification. |
| 43 -La consola de administración de la solución debe permitir ver el estado de los agentes instalados, así como la cantidad de RAM, CPU, ultimo respaldo ejecutado, Sistema operativo de cada servidor. | 44 -La solución propuesta debe poder ser gestionada completamente en nube sin requerimiento de servicios en las premisas, con posibilidad de arquitectura hibrida. |
| 45 -La solución debe incluir la funcionalidad de aplicar cambios en la configuración en las políticas de backup de manera inmediata a todos los servidores o estaciones envueltas en la solución de forma simultánea. | 46 -La solución debe incluir reportes del servicio de manera automática ya sea semanales y/o mensuales. |
| 47 -La solución debe permitir un RPO (punto de recuperación en el tiempo) máximo de 4 Horas. | 48 -La solución debe permitir un RTO (tiempo de retorno en línea) máximo de 1 hora. |
| 49 -El oferente debe suplir para fines del backup local uno o más equipos que tengan las siguientes características mínimas: Capacidad mínima de almacenamiento 70 TB, CPU Intel Xeon 40/80, Memoria RAM local 1TB, 4 x 100GbE, 6U Maximo, Power Supply Redundante | 50 -La solución requerida debe proveer licencias ilimitadas en la nube para la protección de los servidores y/o estaciones de trabajo requeridas por un periodo de tres (3) años. |
| 51 -Se deben incluir todas las funcionalidades requeridas en estos requerimientos, así como las licencias y equipos necesarios para las mismas por un período de tres (3) años. | 52 -La solución debe poder ser gestionada, administrada y monitoreada directamente a través de la misma consola centralizada que se utilizara para el dispositivo (appliance) tanto en la nube como de manera local. |
| 53 -La solución debe permitir la virtualización completa (incluyendo el Sistema Operativo) desde la nube en caso de contingencia en la misma red LAN local, de servidores tanto físicos como virtuales, así como laptop o workstations, sin depender de la infraestructura de INAPA para garantizar la continuidad de operacional. | 54 -La solución debe replicar en la nube los mismos servidores que se encuentran respaldados en el dispositivo (appliance). |

| | |
|---|---|
| 55 -La solución debe crear y generar la VPN- VLAN de manera autónoma en caso de Desastre sin necesitar otros oferentes (all in one). | 56 -La solución debe de incluir un mínimo de 42 puntos de recuperación en el primer año (Inter diarios a diarios después de 7 días, diarios a semanales luego de 2 semanas, semanales a mensuales luego de 6 semanas) y contar con una retención de las imágenes en la nube de manera infinita con punto de recuperaciones por cada año luego del primer año, sin limiten en cuando a espacio ocupado. |
| 57 -La solución debe permitir que los datos permanezcan protegidos por el cifrado AES-256 bit durante todo el proceso de sincronización, almacenamiento y replicación. | 58 -La solución debe ser única e integral que permita la protección completa de cada sistema (Server físico o virtual), la continuidad del negocio en caso de falla y la recuperación contra desastre (Nube) sin la intervención de 3eros aplicativos o soluciones adicionales u otras plataformas, todo debe ser manejado bajo el mismo oferente y panel de control. |
| 59 -La solución debe permitir configurar el horario de sincronización de la imagen a la Nube individual por servidor. | 60 -La solución debe permitir restringir la velocidad de sincronización a la nube o upload, así como configurar porcentaje % de uso, horario con porcentaje (%) de uso y numero de imagen de subida al mismo tiempo. |
| 61 -La solución debe permitir activar o virtualizar todas las imágenes en la nube y permitir la recuperación de datos al mismo tiempo de diferentes imágenes sin costos adicionales en ningún momento. | 62 -La solución debe permitir el pausar la sincronización a la nube de cada servidor de forma independiente. |
| 63 -La solución debe permitir la continuidad operacional de una empresa usando las imágenes en la Nube, así como de forma integrada con el dispositivo local (Appliance). | 64 -La solución debe permitir el borrado en la nube de las imágenes independientes de cada servidor sin alterar la secuencia de los respaldos, retención, ni impactar en la restauración o virtualización de los servidores. |
| 65 -La solución debe permitir la visualización de eventos como imágenes sincronizadas e incluso los screenshot verification. | 66 -La solución debe permitir mantener en producción todos los servidores en la nube de manera ilimitada de ser necesario por la institución sin limitación en cuanto a uso de memoria RAM, CPU, y ancho de banda, por tiempo de uso indefinido sin costo adicional. |
| 67 -La solución debe incluir la replicación de las imágenes fuera del territorio nacional para mitigar el riesgo País. | 68 -La solución debe ofrecer al menos dos copias de la data en nube, de cada uno de los backups, ubicadas en dos centros de datos distantes geográficamente (geo-redundancia). |
| 69 -El oferente debe permitir realizar la carga inicial hacia la nube través de un dispositivo físico para reducir el tiempo de Upload. | 70 -Los centros de datos en la nube deben cumplir con el estándar internacional Service Organi¬zation Control 2 (SOC2) |
| 71 -El oferente de la nube debe por lo menos ofrecer 2 ubicaciones geográficas independientes. | 72 -El oferente de la nube debe ofrecer el servicio de soporte 24/7 directo del oferente. |
| 73 -El oferente de la nube debe garantizar que la data almacenada en la nube siempre este encriptada (AES-256) | 74 -El oferente debe asegurar que el acceso a los servidores por parte del personal de soporte sea a través de los protocolos de seguridad "RSA SSH keys" y con doble factor de autenticación. Los password no deben contener menos de 22 caracteres. |
| 75 -El acceso al centro de datos debe ser vigilado 24/7 y debe ser requerido el escaneo biométrico y proveer una bitácora de eventos. | 76 -El oferente debe garantizar un plan de recuperación contra desastre ofreciendo un mínimo de 90 días de backup de la data en un lugar alterno. |
| 77 -El oferente debe garantizar que el data center cuente con redundancia en luz, conectividad y control de temperatura. | 78 -Los dispositivos (Appliance) deberán tener garantía total en piezas y servicios por un periodo de 3 años. |
| 79 -En caso de un evento de fuerza mayor y los dispositivos (Appliance) se encuentren damnificados, el oferente deberá reponerlos sin costo alguno. | 80 -El oferente deberá incluir el mantenimiento y las actualizaciones de todos los softwares incluidos por un periodo de 3 años. |
| 81 -La solución debe incluir soporte local 24/7 por un periodo de 3 años, con tiempo de respuesta no mayor a 1 hora. | 82 -La solución debe incluir el soporte directo del fabricante 24/7 por un periodo de 3 años, con tiempo de respuestas no mayor a 2 horas. |
| 83 -El fabricante deberá proveer una persona de contacto dedicada para el soporte de la solución mediante una certificación. | 84 -El oferente de la solución para los casos de soporte local debe proveer una plataforma en la cual el personal de la institución podrá tener sus credenciales, crear y dar seguimiento a los casos de soporte. |
| 85 -El fabricante deberá permitir abrir casos de soporte vía web, teléfono u email. | 86 -La solución debe incluir las certificaciones de forma ilimitada a los ingenieros o personal técnico de la institución. |

| | |
|---|---|
| 87 -El oferente debe incluir un servicio de monitoreo de eventos 24/7 (SOC) y asegurando un tiempo de respuesta no mayor a 24 horas en caso de fallos de los backups. | 88 -El oferente debe realizar todos los servicios de soporte a través de un sistema de tickets en el cual se muestre, fecha del evento, hora del evento, persona responsable y descripción del evento. |
| 89 -El oferente debe poder demonstrar experiencia en implementación de la solución de protección, continuidad y recuperación contra desastre y se valorar la cantidad de instalaciones partiendo de un mínimo de 3. | 90 -El oferente debe poder documentar por lo menos 3 casos de éxito de recuperación antes desastres. |
| 91 -El oferente debe contar con un mínimo de 4 personas certificadas en la solución para ofertar. | 92 -El oferente debe demonstrar mínimo 6 años de experiencia en el manejo de la solución ofertada. |
| 93 -Debe tener un nivel mínimo de partnership "tier 3" o su equivalente con el fabricante de la solución a ofertar. Ej. Gold, Platinum , etc | 94 -El oferente debe contar con personal certificado tanto Nivel 1/Nivel 2/Nivel 3 en la solución a ofertar. |
| 95 -El oferente debe iniciar los trabajos de implementación en un periodo no superior a 15 días posteriores a la recepción del 1er pago. | 96 -El oferente debe cumplir 100% las especificaciones técnicas del pliego |
| 97 -El oferente de debe incluir una carta original del fabricante de la solución, donde se indique que el oferente es distribuidor oficial de esa marca para la República Dominicana y está autorizado a vender y dar servicios a los equipos y solución ofertada. Dicha carta debe ser directa del fabricante de la solución. | 98 -El oferente debe incluir los servicios profesionales para el despliegue de la solución en premisas. |
| 99 -El oferente incluir una prueba de auditoria anual para pruebas de recuperación, continuidad del negocio y/o recuperación contra desastre. | |

**IMAGENES**



| OTROS CRITERIOS |
| --- |
| **Criterio de Compra o Sustitución** |
| |
| **Criterio de Almacenamiento** |
| |
| **Observaciones** |

Instalación Configuración y Puesta en Marcha de todos los Equipos Activos.

El oferente debe de crear Políticas de Backup Local y Políticas de Backup a la Nube.

El oferente debe configurar toda la estructura de respaldo para los 61 Servidores Windows y 8 Servidores Linux (Ya sean físicos o virtuales) que estén dentro de la lista de compatibilidad o matrix. (No sean Virtualizadores o Hipervisores de VMware o Hyper-V)

Requerimientos Generales del Cronograma de ejecución.

- Configuración inicial de los dispositivos de Backup & Disaster Recovery.
- Montura en Rackmount de uno o los dispositivos envueltos.
- Instalación y Configuración inicial cada uno de los dispositivos.
- Instalación de los agentes en cada Server Físico o Virtual que se protegerá.
- Configuración de horarios, calendarios y retención Nube (Local y Remoto)
- Inicio paulatino de Backup por etapas o fases.
- Inicio de sincronización de las imágenes a la Nube.
- Verificación de cualquier error
- Confirmación y Validaciones.
- Pruebas y Demos.
- Verificación Generar.
- Troubleshotting.

El oferente debe entregar un informe final con el detalle de toda la configuración e incluir una matriz de contacto para posibles consultas del proyecto.

El oferente participante debe de incluir un Diagrama de la solución propuesta.

**Data Center Actual**

EL oferente debe dar mantenimiento a los equipos activos del centro de cómputos actual.

Referencia:

2 Capacidad = 30kva

2 UPS APC Smart-UPS VT -MODELO: SUTPF30KB4F

2 Manteniento preventive InROW P/N: ACRD100

1 Plataforma monitoreo Netbotz 570

**Felix Enrique Diaz Inoa**
Director
Direccion de Tecnologia