TDR

ADQUISICION DEL SERVICIO DE SOLUCIÓN DE RESPALDO Y RESILIENCIA PARA EL CENTRO DE DATOS DEL ESTADO DOMINICANO.

ANTECEDENTE Y JUSTIFICACIÓN

La Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), tiene al Datacenter Del Estado Dominicano, que funge como centro de servicio tecnológico para las instituciones gubernamentales, no solo como su centro de datos institucional, tambien como sitio de respaldo de las instituciones gubernamentales, para cumplir con la continuidad y garantía del funcionamiento de las operaciones en cuanto a información tecnológica se refiere.

El principal problema que enfrenta el Datacenter 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 a 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, Esto 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.

Para soportar la nube, el centro de datos cuenta con una infraestructura convergente para abastecer las demandas institucionales de contingencia o sitio principal. 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.

OBJETIVO GENERAL

Adquirir una solución tecnológica para la institución la cual se puedan cubrir las necesidades inmediatas y futuras en cuanto a reciliencia cibernetica para poder sobrevivir a un ataque de ransomware y garantizar la recuperavilidad sana de los datos criticos de la institucion.

ALCANCE E IMPORTANCIA:

El servicio contemplado en la presente propuesta, SOLUCIÓN DE RESPALDO Y RESILIENCIA que sea diseñado con el fin de garantizar la capacidad y disponibilidad de recursos cuando sean requeridos por las diferentes instituciones.

Objetivos específicos:

La solución debe cumplir con los siguiente objetivos:
Upgrade para aumentar la capacidad del almacenamiento adquirido una Powerstore T5000. Se requieren 10 discos de 15.36 TB SSD.

Infraestructura centralizada para respaldo de 30 TB de datos: VM, aplicaciones y base de datos. La infraestructura de respaldo tambien debe incluir una infraestructura aislada y desconectada que proteja contra ataques ciberneticos y de ransomware las copias de los respaldos.

Solución de SaaS para seguridad de maquinas virtuales

Esto puede que afecte la continuidad de las operaciones y la alta disponibilidad del servicio OgticCloud que utilizan las más de veintiséis instituciones gubernamentales. Adicional, en materia de adopción tecnológica aporta al estado dominicano como iniciativa a la transformación digital que se tiene fomentado en la agenda digital 2030.

A través de esta adquisición se podrá mejorar los servicios para las instituciones que ya están alojadas y la que están en espera de recibir nuestros servicios.

Este servicio ofrece grandes beneficios relacionados principalmente con el rendimiento, disponibilidad y seguridad de los datos Como :

- Todos los servicios digitales.
- OgticCloud.
- Aumento de la fiabilidad: mediante la replicación
- Mejora en el rendimiento
- Mejora en la seguridad de los datos
- Soporte para el despliegue de las infraestructura de los proyectos:

1) Burocracia cero, 2) SIGEI, 3) Data Warehouse Gubernamental, 4) Portal Único de Servicio, 5) Becas, entre otros.

CONDICIONES GENERALES REQUERIDAS

- El oferente deberá proveer, instalar y configurar todos los equipos, hardware y licencias con las características técnicas mencionadas según la tabla de referencias. En adición la solución tiene que venir integrada y certificada de fábrica en todos sus componentes como un solo producto según cada lote.
- El Oferente debe incluir los siguientes entrenamientos al personal de OGTIC.

ENTRENAMIENTOS	1. Instalación y administración del software de backup en su versión más reciente. 2. Instalación y configuración del ambiente aislado de la copia de respaldos contra ransomware.

A. Los equipos ofrecidos por el oferente deben ser entregados en completa operación, a satisfacción de la entidad, con todos los componentes incluidos.

B. Incluir Hojas Técnicas (Datasheets) de los equipos y componentes ofertados.

C. Los equipos deben de ser originales y nuevos de fábrica, no se aceptan equipos reemplazos o remanufacturados.

D. El oferente debe contar con la certificación del o los fabricantes de las tecnologías, que le autoriza a ofrecer los bienes y servicios de su oferta, y a comercializar de manera válida los servicios de soporte e implementación tal cual como son requeridos en el territorio de República Dominicana a entidades gubernamentales y en específico para esta licitación en particular, mediante documentación original firmada y sellada en papel oficial de cada fabricante de las soluciones propuestas.

E. El oferente debe incluir una carta del fabricante, indicando que todos los productos son nuevos, no usados, no remanufacturados, ni reparados; y que los mismos no se encuentran descontinuados ni anunciados fuera de vida.

F. Todas las licencias de software, subscripciones, garantías, etc., deben ser ofertadas y emitidas a nombre de la institución contratante. La institución contratante tendrá el derecho legal de usar las mismas bajo su única, absoluta y completa discreción dentro de cualquiera de sus dependencias oficiales sin que esto implique un cambio de titular de las licencias, subscripciones, etc., ni se incurra en ningún tipo de costo adicional por estos usos. Este requisito no será subsanable.

G. Las ofertas técnicas deben ser presentadas en el formulario de cumplimiento en un formato de manera tal que, al lado de cada requerimiento técnico, en su línea correspondiente, se documente la referencia específica a la documentación técnica original de cada fabricante de los elementos propuestos donde se establece el cumplimiento o no de cada requerimiento. Los oferentes deberán presentar la documentación técnica original de cada fabricante para todas las soluciones y elementos ofertados.

H. El oferente tiene que presentar un plan de trabajo en la propuesta técnica en el cual se especifiquen de forma clara todos los pasos a ejecutar durante el proceso de implementación de los equipos ofertados.

I. Proporcionar un diagrama que ilustren la solución a instalar.

J. Los entrenamientos deben ser oficiales del fabricante e impartidos por el oferente si está certificado o el fabricante, los mismos deben ser impartidos en una localidad externa a las instalaciones de la institución proporcionada por parte del oferente.

REQUISITOS DE LA IMPLEMENTACIÓN

A. El oferente asegura y se hace responsable a través de su oferta técnica, sobre la instalación y configuración de los nuevos equipos ofertados

B. El oferente acepta y se compromete que la oferta técnica es llave en mano y que cuenta con todos los componentes, servicios necesarios para la implementación y puesta en marcha de los nuevos equipos a instalar, exonerando de todo costo económico y de recurso humano adicional

C. En los casos de las soluciones que necesitan funcionar de manera coordinadas y/o integradas, se deben incluir y describir explícitamente todos los componentes de hardware, software, suscripciones, servicios, soporte, instalación, configuración y cualquier otro elemento que sea necesario para que estas soluciones funcionen adecuadamente incluyendo todos los elementos y servicios de integración entre ellas. En sentido general, el requerimiento obligatorio es que todas las soluciones requeridas sean instaladas y configuradas de manera integral y que cumpla con todas las especificaciones del pliego de la licitación, en un formato llave en mano que incluya todos los elementos necesarios para su puesta en funcionamiento integral. Este requerimiento tendrá precedencia sobre cualquier error u omisión en las descripciones particulares de cualquier solución en caso de que esto ocurra.

D. El proveedor debe entrega reporte de certificación de trabajos concluidos y anexar imágenes de los equipos instalados operando con normalidad y toda la memoria técnica del proyecto.

E. La evaluación de la solución será utilizando la modalidad o procedimiento cumple / No cumple, utilizando el formulario anexo “TDR requerimientos y de evaluación 01”.

F. El oferente debe contar con 5 años de presencia en República Dominicana.

G. El oferente debe contar con Experiencia previa en implementaciones de al menos tres (3) proyectos de magnitud y complejidad similar, mostrando carta de referencia de clientes y/o orden de compra del proyecto. En dichos proyectos deben estar incluidas soluciones de:
   - Soluciones de backup
   - Soluciones de repositorios especializados para respaldo a discos
   - Soluciones de ciber resiliencia "ambientes aislados de respaldos" para sobrevivir a un ataque de ransomware.
   - Soluciones de almacenamiento

H. El oferente debe realizar el proceso de instalación e implementación de todos los elementos y equipos que conforman la solución propuesta. Se debe asegurar que la solución quede funcionado basado en los requerimientos de la institución y según las mejores prácticas del fabricante.

I. El oferente debe contar con carta del fabricante para la comercialización de estos productos y que es representante local del mismo.

J. Debe incluirse la asignación de un gerente de proyectos certificado PMP para la implementación y configuración de todas las soluciones ofertadas en esta licitación y durante todo el tiempo que sea necesario y requerido por la institución hasta la conclusión y recepción del proyecto. Se debe incluir en la propuesta el currículo de este gerente de proyectos.

K. Cada oferente debe ofrecer un plan de trabajo preliminar detallado con descripción de tiempos y tareas necesarios para la ejecución de estos trabajos de forma tal que tengan los menores impactos operacionales. Todos los servicios actuales deben mantenerse operacionales en los horarios normales de uso de estos durante los tiempos de implementación de todas las soluciones de este proceso.

L. Debe incluirse y describirse explícitamente el Project Plan en formato de MS Project para la implementación de todas las soluciones ofertadas en este lote, así como los currículos del personal que sería asignado al mismo. El oferente que resulte ganador deberá mantener y actualizar este Project Plan con periodicidad semanal

M. El oferente debe contar con mínimo las siguientes certificaciones y/o acreditaciones o equivalentes, para la instalación, implementación e integración de la solución solicitada. (Este requisito no será subsanable):
   - **Partner Metalico de las marcas a ofertar. (Gold, Premier, Platinum, Titanium)**
   - **Data Center Specialization Architecture**
   - **Certificación en la soluciones de backup.**
   - **Certificación en el Appliance de backup ofertado**

N. El oferente debe con contar con mínimo las siguientes certificaciones y/o acreditaciones o equivalentes, para la instalación, implementación de los ambientes de virtualización, Backup y almacenamiento. (**Este requisito no será subsanable**):
   - Certificación en servicios de implementación en almacenamiento.
   - VMware Data Center Virtualization
   - Certificación en la solución de backup Ofertada.
   - Certificación en la Solución de Almacenamiento para backup ofertada.

O. El oferente debe contar con personal técnico capacitado, este personal debe garantizar el éxito del proyecto y debe contar como mínimo con el siguiente perfil. (Este requisito no será subsanable):

a. **Un (1) Gerente de proyecto**
   - Profesional de la Ingeniería en Sistemas o afines
   - Debe tener mínimo tres (3) años de experiencia en gestión y supervisión de proyectos

b. **Un (1) ingeniero líder del proyecto**
   - Debe contar con la certificación de backup y Appliance de respaldos de la soluciones propuestas (HPE, Nutanix, Cisco, Dell, entre otros). Dicha certificación debe estar vigente y activa.
   - Debe contar con mínimo tres (3) años de experiencia en implementación de proyectos similares.
   - Debe laborar como personal fijo del oferente, por lo menos con antigüedad de seis (6) meses. Para esto debe presentar la documentación de la TSS como evidencia.

c. Un (1) ingeniero especialista en virtualización
   - Debe contar con la certificación de virtualización de centro de datos, nivel profesional emitida por la solución de virtualización ofertada. Dicha certificación debe estar vigente y activa.
   - Debe contar con mínimo tres (3) años de experiencia en implementación de proyectos similares.
   - Debe laborar como personal fijo del oferente, por lo menos con antigüedad de seis (6) meses. Para esto debe presentar la documentación de la TSS como evidencia.

d. Un (1) ingeniero especialista en redes
   - Debe contar con la certificación de ambientes de redes (CCNA, JNCIP, MTCNA, entre otros). Dicha certificación debe estar vigente y activa.
   - Debe contar con mínimo tres (3) años de experiencia en implementación de proyectos similares.
   - Debe laborar como personal fijo del oferente, por lo menos con antigüedad de seis (6) meses. Para esto debe presentar la documentación de la TSS como evidencia.

e. Un (1) ingeniero especialista en servidores
   - Debe contar con la certificación nivel profesional en la implementación de Appliance y/o Nodos de hiperconvergencia. (Nutanix Certified, HPE, Cisco, Dell, entre otros). Dicha certificación debe estar vigente y activa.
   - Debe contar con mínimo tres (3) años de experiencia en implementación de proyectos similares.
   - Debe laborar como personal fijo del oferente, por lo menos con antigüedad de seis (6) meses. Para esto debe presentar la documentación de la TSS como evidencia.

DETALLES DE LA SOLUCION DE SERVICIO:

Descripción de la Solución requerida.

Lote 1: Infraestructura de Respaldo y Bóveda Aislada Protección contra Ransomware

Solución de respaldo: software de respaldo, dispositivos especializados para repositorio de backup y solución de protección ante un Ransonware.

Solución de respaldo y Bóveda protegida contra Ransomware.

Objetivo de la solución:
Solución de respaldo a repositorio a disco con replica, offline, de los respaldos hacia un Sitio de Aislado para protección contra ransomware

Lote 1: Infraestructura de Respaldo y Bóveda Aislada Protección contra Ransomware		
ITEM	**DESCRIPCION**	**CANTIDAD**
INFRAESTRUCTURA DE RESPALDO	**CARACTERISTICAS GENERALES INFRAESTRUCTURA DE RESPALDO**	
	La solución contendrá:	
	Servidor de Respaldo	
	Appliance/Almacenamiento especializado para repositorio de respaldo	
	Software de Respaldo.	
	Infraestructura para Ciber Seguridad de Datos y Resiliencia Cibernética contra RANSOMWARE	
	Requerimiento del Servidor para respaldo	1
	2x Intel Xeon Gold 4314 16-Cores @ 2.4G	
	128 GB RAM DDR4	
	2x 480 GB SSD (Boot)	
	6x 2.4 TB SAS HDD 10k (Data)	
	2x tarjetas a 25GbE, de 2-port c/u	
	3 años de soporte 24x7x4 de hardware	
	3 años de garantía	
	Licenciamiento correspondiente para el servidor (Windows o Linux)	
	Fuentes de poder redundantes	
	Ventiladores redundantes	
	Deberá incluir todos los elementos necesarios para su montaje en RACK	
	2x licencias VMware vSphere Standard	
	Requerimiento para el Appliance o Almacenamiento para Respaldo	1
	La capacidad física utilizable requerida es de 45 TB mínimo, antes de la aplicación deduplicación y compresión.	
	La solución ofertada NO debe de ser un almacenamiento de propósito general (SAN o NAS) utilizado para backup.	

	El almacenamiento para backup NO debe de ser un servidor creado para almacenamiento. Es decir que no debe de ser un servidor con alta capacidad de discos internos y/o externos configurado como repositorio de backup.	
	El equipo debe ser una solución construida para uso especifico de repositorio de respaldo. No debe de ser un servidor configurado para este uso, tampoco puede ser un almacenamiento SAN o NAS configurado para uso de respaldo.	
	La deduplicación y compresión no debe ser postprocesos.	
	La solución debe poder integrarse con cualquier solución de respaldo del mercado.	
	La solución debe poder integrarse con cualquier sistema operativo.	
	La solución debe poder integrase a cualquier aplicación y Base de Datos.	
	La solución debe tener capacidad de crecer agregando discos adicionales.	
	La solución debe poder emular librerías virtuales.	
	La solución debe soportar encriptación para los datos almacenados y en las transmisiones de replicación.	
	La solución debe soportar Inmutabilidad de los datos almacenados mediante políticas de retención.	
	Cuando se utilice replicación los datos transmitidos deben ser enviados deduplicados y comprimidos al equipo remoto.	
	La solución debe poder replicar a equipos similares de menor o mayor capacidad o a modelos diferentes de la familia.	
	Debe soportar replicación bidireccional entre equipos	
	La replicación puede ser de 1 a 1, de 1 a muchos, o de muchos a 1.	
	Se requiere una solución que pueda almacenar 30 copias del backup de 40-TB con un 4% de cambio diario. La solución debe usar deduplicación y compresión. Debe contemplar un crecimiento del 10% por 3 años.	
	Se desea retener 30 copias de backup diario.	
	La solución debe poder crecer al triple de la capacidad solicitada.	
	La solución debe tener un performance mínimo de 8 TB por hora.	
	La solución debe contar con una consola GUI para administración y configuración.	
	La solución debe contar con una CLI para administración y configuración.	
	La solución debe de contar con OS hardened.	
	La solución debe poder ser administrada por Roles.	
	La solución debe soportar la integración con Active Directory.	
	La solución puede soportar usuarios locales y del dominio.	
	La solución debe ofrecer deduplicación y compresión en línea.	
	La solución debe incluir la capacidad de replicacion.	
	La solución debe tener la capacidad de poder almacenar en la nube para retención larga.	
	La solución debe tener la capacidad de poder respaldar VM a la nube para procesos de Disaster Recovery en Cloud VMware.	

	La solución debe poder tener Appliance virtuales en la nube para poder replicar si se requiriera.	
	debe incluir 4 puertos de 10 GbE.	
	Debe tener capacidad de Inmutabilidad	
	Debe integrarse al AD.	
	Debe tener capacidad de Permiso por roles y grupo.	
	Debe conectarse al servidor de backup por protocolo seguro.	
	Debe soportar NFS/FC/HTTP/SMB/CIFS	
	Soporte local 7x24x4 hora	
	Garantía y soporte de 36 meses	
	Debe realizar deduplicación global	
	Debe soportar servidores Windows, Linux, Unix, AS/400	
	Administrable por interface grafica.	
	Que se integre con el software de respaldo.	
	Debe enviar reporte de uso y consumo	
	Debe enviar alertas	
	Debe poder crecer hasta 170 TB mínimo físico utilizable	
	Oferente debe tener al menos un ingeniero certificado en los componentes que conforman la solución.	
	La replicación puede ser de 1 a 1, de 1 a muchos, o de muchos a 1.	
	Requerimientos de Software de respaldo	
	Debe incluir licenciamiento para el respaldo 30 TB minimo de datos	
	El licenciamiento debe ser por capacidad y no debe esta limitado cantidad de servidores fisicos o virtuales en la infraestructura.	
	Administración centralizada mediante GUI y modalidad de línea de comando.	
	La solución de ser licenciada por procesador.	
	Debe cubrir toda la carga de trabajo en los hipervisores y servidores físicos, contemplados en el requerimiento, sin que sea necesario licenciamiento adicional al crecer la carga de trabajo en los equipos existentes.	
	Integración con el Appliance de Backup sin requerimiento de licenciamiento adicional.	
	Integración con Storage Snapshots de la solución de hiperconvergencia sin requerimiento de licenciamiento adicional.	
	La solución debe proveer una Consola de Monitoreo e informes centralizados mediante GUI.	
	La solución debe tener funcionalidad de orquestación para planes de Recuperación y funcionalidad de recuperación rápida.	
	Si fuese requerido, deberá poderse desplegar parcial o totalmente en la NUBE.	
	Debe proveer recuperación granular	
	Debe proveer backup/recuperación de imagen de Máquinas Virtuales.	
	Debe proveer Recuperación Instantánea de Máquinas Virtuales.	

	Debe incluir Ciberseguridad de Datos y Recuperación de Datos.	
	La solución debe ser capaz de respaldar ambientes físicos y virtuales.	
	La solución debe ser capaz de respaldar las principales aplicaciones del mercado:	
	SharePoint, Exchange, Active Directory, Windows Server, SQL Server, DB2, Informix, Sybase, SAP HANA, SAP R3, Oracle, MySQL, Linux Server, VM.	
	Debe administrar y/o utilizar Snapshots del Hipervisor y de los almacenamientos centralizados.	
	Debe poder realizar respaldo en caliente, consistentes, de Base de Datos.	
	Solución de protección de datos que admite cargas de trabajo locales tradicionales, así como cargas de trabajo que se trasladan a la nube.	
	La solución debe tener la capacidad de poder realizar Recuperación ante desastres en la nube	
	Compatibilidad con plataformas heterogéneas en una amplia gama de aplicaciones.	
	Copia de seguridad y recuperación hacia y en la nube.	
	Protección de datos de autoservicio desde interfaces nativas.	
	Soporte para múltiples hipervisores.	
	Recuperación ante desastres.	
	Recuperación ante desastres eficiente en la nube para VMware.	
	Aprovecha la agilidad y la escala de la nube pública.	
	Orquestación y recuperación a la nube pública, y a las instalaciones del cliente.	
	Entornos de varias nubes, incluidos Microsoft Azure, Amazon Web Services (AWS) y VMware Cloud on AWS.	
	Recuperación de aplicaciones interdependiente desde cualquier punto en el tiempo.	
	Monitoreo e informes centralizados.	
	Visibilidad de múltiples sistemas y múltiples sitios.	
	El monitoreo permite la identificación proactiva y la resolución de problemas potenciales.	
	La gestión simplifica la gestión del sistema e incluye la gestión de políticas en todo el entorno.	
	La generación de informes ofrece informes flexibles sobre el estado de la protección de datos con informes automatizados de eventos clave.	
	Alertas automatizadas para análisis de causa raíz.	
	Búsqueda y recuperación con restauración basada en los resultados de la búsqueda.	
	El oferente deberá configurar todas las políticas de backup necesarias al alcance del y que estarán incluidas en el SOW.	
	Infraestructura para Ciber Seguridad de Datos y Resiliencia Cibernética	
	Esta infraestructura estará diseñada para resguardar los respaldos en una Ambiente protegido y aislado que pueda sobrevivir a un ataque cibernético o de ransomware.	

	Ambiente protegido y aislado será utilizada para tener una segunda copia de los respaldos en un ambiente aislado y desconectado.	
	Ambiente protegido y aislado deberá tener las siguientes características:	
	La solución ofertada debe de ser reconocida por Gartner.	
	La solución ofertada debe de tener, en el mercado, al menos 5 años.	
	Indicar clientes locales que hayan adquirido la solución.	
	Oferente debe tener al menos un ingeniero certificado en los componentes que conforman la solución.	
	Los ingenieros locales deben tener la capacidad de poder ofrecer soporte local de la solución, por lo que deben estar certificados por el fabricante.	
	La solución debe estar correctamente dimensionada para proteger 30 TB de datos Críticos con una retención de 30 copias.	
	El promedio de cambio a considerar para el dimensionamiento de los datos es de un 4% diario.	
	La solución debe ser capaz de realizar deduplicación y compresión en línea de los datos.	
	Debe ser una solución en la premisa, no en la nube.	
	La solución debe incluir todos los componentes de hardware, software y servicios requeridos para que la solución ofertada permita que ante un ataque cibernéticos destructivo o de ransomware, los datos críticos puedan sobrevivir el ataque.	
	Operación	
	La solución debe ser Resiliente y ofrecer la capacidad de poderse recuperar desde ella ante un ataque cibernético destructivo o de ransomware de manera segura.	
	La solución, la cual llamaremos “Ambiente aislado”, debe garantizar la recuperabilidad de datos no comprometidos.	
	La solución debe de ofrecer una infraestructura de Ambiente aislado.	
	La Solución debe de estar aislada de la Red Local.	
	La Solución no debe tener conectividad a Internet. No debe tener conexiones activas hacia el exterior.	
	La Solución debe ser administrada de manera local para mayor seguridad.	
	La Solución no debe permitir comunicación remota hacia ella para su administración.	
	La Solución debe poder enviar Log o Correos de manera segura hacia alguna consola de Monitoreo.	
	La Solución tener la habilidad de poder detectar cualquier vulnerabilidad que pueda comprometer su integridad.	
	El Ambiente aislado, ante algún intento de acceso peligroso, debe poder auto protegerse y emitir alguna alerta.	
	La Solución debe de ser Inmutable.	
	La Solución debe ser una solución aislada mediante Air-Gapped.	
	La Solución debe sobrevivir ante cualquier ataque cibernético destructivo o de ransomware.	

	La Solución debe ser accesible físicamente.	
	La Solución debe de ser una solución descentralizada.	
	La Solución debe ser 100% instalada en la premisa y en todo momento debe ser controlada por "LA INSTITUCION", es decir que no debe de ser una solución en la NUBE.	
	Ante un ataque cibernético destructivo o de ransomware desde "El Ambiente aislado" se debe poder activar un plan de ciber-resiliencia que permita la recuperación de los datos desde ella hacia el sitio principal o hacia una plataforma alterna de recuperabilidad de los respaldos no comprometidos.	
	La Solución debe poder determinar y recomendar cual es el respaldo más reciente y seguro para el proceso de recuperación.	
	La solución debe realizar copias de los backups de "producción" hacia el ambiente aislado de forma segura.	
	La copia de los respaldos de Producción hacia el ambiente aislado debe realizarse mediante comunicación encriptada.	
	La solución debe tener controles para aislar y proteger las copias seguras de datos en el entorno del ambiente aislado.	
	La Solución debe operar de manera autónoma y orquestada sin necesidad de intervención externa para las actualizaciones normales de los datos almacenados.	
	La solución debe estar completamente fuera de línea de la red de producción, excepto cuando recibe actualizaciones.	
	La solución debe estar protegida durante el proceso de actualización.	
	La solución debe tener una interfaz gráfica de usuario (GUI) fácil de operar y API disponibles para la personalización.	
	La solución debe ser capaz de proveer:	
	Recuperación ante ataques de Malware	
	Notificación de vector de ataque.	
	Secuestro de datos (Ransomware).	
	Detalles del archivo dañado	
	Cambios/eliminaciones masivas de datos.	
	Cuentas de usuario violadas.	
	Ejecutables violados.	
	Recuperación de la última copia válida	
	La solución debe proveer protección inteligente para aislar datos críticos, identificar actividades sospechosas y acelerar la recuperación de datos, lo que le permite reanudar rápidamente las operaciones comerciales normales.	
	La solución debe aprender del comportamiento de los datos, y mediante ML/AI poder identificar actividades sospechosas en los Datos.	
	La solución debe ofrecer los pasos para la remediación segura de los efectos ocasionados por el ataque.	
	Cifrado y Autenticación	
	La solución debe utilizar protocolos de seguridad entre el entorno de producción y el entorno del Ambiente aislado.	

	La solución debe usar el cifrado para transferir datos entre los entornos de producción y el Ambiente aislado.	
	Inmutabilidad	
	La solución debe ofrecer una protección equivalente a WORM para los datos almacenados en el Ambiente aislado.	
	La capacidad WORM debe cumplir con los estándares o regulaciones establecidos.	
	La capacidad WORM debe proporcionar un "oficial de seguridad" o una configuración similar que ayude a evitar que el control se vea comprometido.	
	La solución debe proporcionar la capacidad de mantener múltiples copias de datos	
	Analítica	
	La solución debe proporcionar análisis de seguridad en los datos almacenados.	
	La solución debe proporcionar un flujo de trabajo automatizado para el análisis, lo que significa que no se requiere intervención humana para realizar el análisis o entregar resultados.	
	Debe ser capaz de usar Sandbox para archivos sospechosos.	
	La solución debe poder analizar las copias de los respaldos sin necesidad de realizar restauraciones de los datos, es decir, desde su formato de copia de seguridad.	
	Reportaría y Gestión	
	La solución debe proporcionar la capacidad de registrar e informar sobre la actividad de inicio de sesión, errores, incidentes críticos, etc.	
	La solución debe permitir que los informes se envíen de forma segura desde el Ambiente aislado a Producción.	
	Solución de endurecimiento.	
	La solución debe proveer mecanismos que permitan el endurecimiento de los sistemas operativos y los equipos utilizados en el entorno del Ambiente aislado.	
	La solución debe limitar el control de puertos a nivel de comunicación para el proceso de endurecimiento de los equipos en el entorno del Ambiente aislado.	
	Compatibilidad	
	La solución debe ser compatible con todos los principales softwares de copia de seguridad (Veritas, CommVault, TSM, Networker, Avamar, etc.)	
	Servicios	
	Describir los servicios ofrecidos para implementar la Solución	
	Describa los servicios avanzados adicionales que ofrece para mejorar y/o personalizar la Solución.	
	Se deben incluir todos los servicios necesarios para la implementación, instalación, automatización y pruebas de recuperabilidad.	
	Se deben de incluir los servicios para las pruebas y protocolos de recuperabilidad al menos dos veces al año.	
	El oferente debe incluir los servicios de:	
	Creación de las políticas de replicación, de ser necesarias.	
	Requerimientos del Oferente	

	Debe de estar certificado en la solución de respaldo, al menos un ingeniero.	
	Debe brindar soporte local sobre la solución ofertada.	
	Debe brindar asistencia ante cualquier requerimiento de la solución 24x7x365 con 4 horas.	
	Constancia de al menos tres o más proyectos vendidos de esta solución en Republica Dominicana.	
	Debe estar certificado en almacenamiento de repositorio de respaldo.	
	Debe incluir constancia de al menos 10 clientes con la solución de repositorio de respaldo.	
	La solución debe contar con administrador del proyecto.	
	La solución debe contar con la participación de un ingeniero certificado en la solución para la fase de	
	Componentes de la Solución de del Ambiente aislado y protegida de Datos	
	Software de Administración y Automatización	1
	Software de Analítica y Reporte (Para 30 TB de Datos de Respaldo)	1
	Appliance/Almacenamiento de repositorio de las copias de respaldo	1
	Debe tener las mismas características que el de Backup	
	60 TB Usable antes de deduplicación y Compresión	
	4x 10 Gbits Ethernet SFP	
	Dual Power Supply	
	Soporte y garantía Critical 7x24 4 horas, 3 Years	
	Este Appliance debe cumplir con los mismos requerimientos del repositorio de la solución de respaldo. (Requerimiento para el Appliance o Almacenamiento para Respaldo)	
	Switch 12 Puertos 10 GbE	1
	12 x 10GBaseT, 3 x 100GbE QSFP28	
	Dual Power Supply	
	Soporte y garantía Critical 7x24 4 horas, 3 Years	
	Servidor para Administración y Automatización	1
	2x Intel 4314 2.4G, 16-Cores	
	256 GB RAM	
	Controladora RAID con 4 GB Cache	
	8x 2.4TB 10K RPM SAS 12Gbps 512e 2.5in Hot-plug Hard Drive	
	2x 2 M.2 Sticks 480GB (RAID 1)	
	Dual, Hot-plug, Redundant (1+1)	
	2x C13 to C14, PDU Style	
	1x Dual Port 10GbE BASE-T Adapter	
	Soporte y garantía Critical 7x24 4 horas, 3 Years	
	Servidor para Software de Analítica y Reporte	1

	2x Intel 4314 2.4G, 16-Cores	
	256 GB RAM	
	Controladora RAID con 4 GB Cache	
	8x 2.4TB 10K RPM SAS 12Gbps 512e 2.5in Hot-plug Hard Drive	
	2x 2 M.2 Sticks 480GB (RAID 1)	
	Dual, Hot-plug, Redundant (1+1)	
	2x C13 to C14, PDU Style	
	1x Dual Port 10GbE BASE-T Adapter	
	Soporte y garantía Critical 7x24 4 horas, 3 Years	

Lote 2: Upgrade Almacenamiento ALL-FLASH		
ITEM	**DESCRIPCION**	**CANTIDAD**
UPGRADE DE ALMACENAMIENTO	**CARACTERISTICAS GENERALES INFRAESTRUCTURA DE RESPALDO**	
	SSD 15.36 TB para PowerStore T5000	**10**
	Soporte y mantenimiento por 36 meses	
	Instalación y configuración.	
	Creación de LUN y asignación a servidores.	
	Discos deben ser suplidos directamente por el fabricante	
	NO se aceptan discos adquiridos en el mercado GRIS.	
	Debe mostrar carta del fabricante de la adquisición.	

Lote 3: Solución SaaS para Seguridad de la carga de trabajo (VM)		
ITEM	**DESCRIPCION**	**CANTIDAD**
Seguridad de la carga de trabajo	**Seguridad de la carga de trabajo (Ambiente de máquinas y/o servidores virtuales)**	**100 VM**
	Como una plataforma basada en Alertas, todas las alertas pueden ser enviadas a una gran variedad de sistemas como SIEM, SOAR y otras plataformas de agregación de logs. Por ejemplo, Splunk, QRadar, and LogRythm; Mensajes son enviados vía syslog.	
	Debe admitir implementaciones tanto en infraestructuras actuales como en infraestructuras nuevas de Data Center. La solución de Telemetría propuesta debe proporcionar información completa que incluye detalles sobre variaciones entre paquetes dentro de un flujo, detalles de los proceso y paquetes de software instalados en un servidor y sus vulnerabilidades.	
	Debe contar con soporte para Windows, Linux (distintas versiones), AIX, Kubernetes y openshift 4.X	

	Debe contemplar todas las acciones mencionadas en el framework de MITRE ATTACK y enviar alertas al reconocer dichas acciones, más allá de la restricción provista por la segmentación.	
	Debe establecer una línea de base de comportamiento, y realizar análisis e identificación de desviaciones en el comportamiento del tráfico del server.	
	Debe integrarse con F5, Citrix y Cisco firepower para concatenar los flujos de los clientes a los balanceadores y de los balanceadores a los servidores reales. Debe poder hacer enforcement en dichos dispositivos de forma nativa sin software adicional.	
	Debe integrarse con soluciones de NTA (Network Traffic Analytics) para identificar comportamiento malicioso.	
	Debe integrarse con soluciones de SDN para tomar el 100% de los flujos de la red. Por ejemplo, ACI.	
	Debe permite una aplicación coherente de la política en entornos híbridos, incluidas las cargas de trabajo que se ejecutan en la nube, y debe permitir una identificación más sencilla de las anomalías para una seguridad sin confianza (zero-trust).	
	Debe permitir a los administradores simular su política de lista blanca y evaluar su impacto antes de aplicarla en la red de producción. Esta capacidad le permitirá al administrador ver cómo esta política de lista blanca afectaría el tráfico real que fluye a través de la red. Además, el administrador debe poder ver inmediatamente qué flujos se clasificarán como compatibles, no compatibles o eliminados.	
	Debe permitir adicionar al menos 32 tags a cada dispositivo, ya sea en formato manual, conectando con VCenter o de forma automática con SERVICENOW.	
	Debe permitir desarrollar y aplicar automáticamente políticas de cumplimiento de la seguridad en toda la infraestructura en función de la actividad real de las aplicaciones, las cargas de trabajo y los dispositivos. Esto debe permitir crear un modelo seguro y de confianza cero que se aplica no solo a dispositivos generalmente estáticos, como servidores y dispositivos de red, sino también al mundo dinámico de las aplicaciones.	
	Debe permitir determinar el comportamiento de los servidores mediante la línea de base de los procesos que se ejecutan en el servidor, identificando cualquier desviación de esas líneas de base. La solución propuesta, debe contar con algoritmos para hacer coincidir estas desviaciones con los patrones de ejecución de malware, permitiendo una detección más rápida de anomalías. Esta asignación de patrones de comportamiento debe incluir amenazas de alto impacto como Specter y Meltdown.	
	Debe permitir identificar claramente que tráfico es permitido y/o bloqueado por la política. También debe	
	Debe permitir implantarse Cloud (SaaS en la nube de Oracle), virtual y on-premise.	
	Debe permitir trabajar sin agente, colectando flujos, labels y pudiendo configurar políticas en AWS, Azure y GCP.	
	Debe poder extender la visibilidad a los Workstation mediante Anyconnect.	

	Debe poder integrarse de manera nativa con la solución de control de acceso a la red, Cisco ISE, para poder identificar usuarios y aplicar políticas según grupos de AD. Esto debe ser aplicado también para la VPN.	
	Debe poder recibir de forma nativa flujos de AWS VPC, Cisco ASA y Meraki. Debe poder recibir protocolos standard como NETFLOW y ERSPAN.	1
	Debe poder recibir información de un feed de STIX/TAXII de contar el cliente con ello.	
	Debe poder relacionar e informar las acciones realizadas por los distintos procesos e indicar si dichos procesos tienen vulnerabilidades.	
	Debe poseer diferentes dashboards con información clara del estado de los dispositivos.	
	Debe proporcionar datos de los componentes de la aplicación y algoritmos de análisis de comportamiento. Permitiendo identificar grupos de aplicaciones y sus patrones de comunicación y dependencias de servicio.	
	Debe proveer capacidades de aprendizaje automático para reducir drásticamente las entradas humanas necesarias para comprender los patrones de comunicación.	
	Debe realizar segmentación basada en listas blancas, que permite a los operadores controlar la comunicación de red dentro del data center, lo que permitirá implementar un modelo de confianza cero (zero-trust).	
	Debe soportar upgrade automático de software sensor.	
	Debe tener la capacidad de permitir, de forma proactiva, poner en cuarentena a los servidores cuando se detectan vulnerabilidades y bloquear la comunicación especifica relacionada con una vulnerabilidad hasta que se instale el Patch homologado.	
	Deber permitir realizar detección de vulnerabilidades y exposiciones comunes asociadas con los paquetes de software instalados en los servidores, sin instalar una herramienta adicional.	
	El agente a utilizar debe soportar múltiples sistemas operativos, y debe trabajar con el Firewall original del sistema operativo donde funcionará para evitar conflictos con el mismo o perdida de soporte.	
	El agente de la solución a ofertar no debe modificar bajo ninguna circunstancia el Kernel del sistema sobre el cuál se ejecuta.	
	El agente debe tener un consumo de CPU y memoria reducido, no necesitando de actualización de firmas para su funcionamiento y pudiendo restringir el consumo de recursos en el server.	
	El agrupamiento de los servers con diferentes vulnerabilidades afectados por políticas, deben ser seleccionados automáticamente y al instalarse el patch, deben salir de la restricción de la misma forma.	
	El enforcement de la política debe realizarse con el firewall nativo del host en el cual está ejecutando el agente, sin modificar la aplicación del firewall de host. Para Windows debe contar con la posibilidad de trabajar con WAF (Windows advanced firewall) y WFT (Windows filtering Platform).	

	Hacer enforcement sobre otros dispositivos (firewalls: Cisco, Palo Alto, Checkpoint, Fortinet, Dell, Juniper, etc.) debe ser posible, aunque haya que incluir un módulo adicional opcional.	
	identificar tráfico bloqueado por otros dispositivos ubicados entre los servers.	
	La instalación del agente no debe requerir reinicio del sistema operativo.	
	La plataforma debe proveer API de desarrollo abiertas.	
	La plataforma debe recopilar y almacenar datos completos del flujo de tráfico. Además de la visibilidad en sus servidores, pudiendo implementar sensores de software en máquinas virtuales de infraestructura de escritorio virtual (VDI) para la visibilidad en entornos VDI. Luego, puede consultar estos datos con fines de visibilidad y análisis forense en todo el centro de datos y utilizar estos datos para solucionar problemas de red y aplicaciones.	
	La plataforma debe verificar si alguno de los paquetes de software tiene vulnerabilidades de seguridad de la información conocidas enumeradas en la base de datos de vulnerabilidades y exposiciones comunes (CVE). Cuando se detecta una vulnerabilidad, debe poder encontrar detalles completos, incluidos la gravedad y la puntuación de impacto, y ubicar todos los servidores que tienen instalada la misma versión del paquete. También debe predefinir políticas con acciones específicas, como poner en cuarentena a un host, cuando los servidores tienen paquetes con ciertas vulnerabilidades.	
	La plataforma ofertada debe contar con capacidades de autocontrol y autodiagnóstico, lo que permita eliminan la necesidad de tener experiencia en Big Data para operar con ella. El soporte de hardware y software debe ser cubierto 100% por el fabricante.	
	La plataforma ofertada no debe depender de licencias o hardware de terceros. Debe ser completamente llave en mano.	
	La plataforma ofertada, debe admitir una combinación de requisitos de infraestructura que incluye una nube pública, una infraestructura legada (legacy), una infraestructura virtualizada, en plataforma bare-metal y en containers.	
	La plataforma propuesta debe monitorear los paquetes de software instalados, la versión del paquete, el nivel de parche, etc. Se deben incluir al menos, 19 años de información de vulnerabilidad y exposición.	
	La solución debe cumplir con, al menos, los siguientes requerimientos:	
	La solución debe proveer prevención de exfiltración de datos.	
	La solución debe realizar un descubrimiento automático de las políticas mediante un motor de inteligencia artificial. Es requerido contar con versionado de las políticas.	
	La solución debe ser capaz de recopilar información basada en agente, utilizar soluciones de software basados en distintos tipos de flujos (ERSPAN, NETFLOW, IPFIX, NSEL, etc.) desplegados en toda la infraestructura del data center.	
	Las comunicaciones de los dispositivos deben ser guardados por largos periodos de tiempo para poder realizar investigaciones y mostrar cumplimiento con auditorias. Se	

	Las políticas recomendadas deben poder ser verificadas antes de aplicarlas comparándolas con tráfico real que tuvo la aplicación por un periodo al menos de un mes.	
	México y toda Latinoamérica para dar un soporte local ante cualquier necesidad.	
	Se debe contar con Clientes y partners con experiencia en Chile, Brasil, Colombia, Argentina, Bolivia,	
	Se debe contar con más de 40 clientes de distintas verticales en la región. Por ejemplo: sector Bancario, organismos de impuestos, organismos de fiscalización de sector financiero, retail, Manufactura, comunicaciones, oil&gas, etc.	
	Se debe contar con soporte en español, portugués e inglés por parte del fabricante.	
	Se debe proveer todo el hardware necesario para correr el software. Incluyendo soporte de hardware y software.	
	Se debe tener stock de repuestos en el país en caso de falla del hardware.	
	Se requiere una plataforma que aborde los desafíos de la protección de la carga de trabajo en la nube híbrida mediante el uso de aprendizaje automático no supervisado, análisis de comportamiento y enfoques algorítmicos.	

Condiciones Generales Aplicables para esta licitación

Tiempo de entrega:
Plataforma de Hiperconvergencia: 12 semanas, presentar carta del fabricante con el tiempo de entrega estimado y carta del oferente con el compromiso de entrega.

Forma de pago:
- 20% con la firma del contrato
- 20% con la orden al fabricante y entrega del plan de trabajo
- 40% con la entrega de los equipos
- 20% con la entrega del proyecto

OBLIGACIÓN DE OFRECER SOLUCIONES COMPLETAS, INTEGRADAS Y FUNCIONALES

En sentido general, el requerimiento obligatorio es que todas las soluciones requeridas sean instaladas y configuradas de manera tal que se cumplan los con los requerimientos de la en un formato llave en mano que incluya todos los elementos necesarios para su puesta en funcionamiento integral. Este requerimiento tendrá precedencia sobre cualquier error u omisión en las descripciones particulares de cualquier solución en caso de que esto ocurra. Este requerimiento no será subsanable

CONDICIONES DE GARANTIA DEL SERVICIO

Garantía, Soporte y Mantenimiento Técnico

Debe incluirse y describirse explícitamente la Garantía, el Soporte y Mantenimiento Técnico a todas las soluciones tanto de Hardware, incluyendo la sustitución de piezas, como de Licencias de Software, incluyendo actualización de estos, servicios de suscripción, y cualquier otro elemento necesario en cada una de las soluciones propuestas. Estos soportes deben ser por un tiempo de 3 años a partir de la puesta en marcha de la solución con un tiempo de respuesta de 4 horas y cobertura 7X24 para todas las soluciones requeridas. Este requerimiento tendrá precedencia sobre cualquier error u omisión en las descripciones particulares de cualquier solución en caso de que esto ocurra. Este requerimiento no será subsanable.