LOTE 3		
Solución tecnología Centro de Datos y Seguridad		
Ítem	**Cantidad**	***Descripción y Especificaciones Técnicas***
1	1	**1. <u>Cumplimiento con los requerimientos de Especificaciones Técnicas solicitadas, cronogramas y transferencia de conocimiento y certificaciones de la empresa.</u>** **A. <u>Documentación de Cronograma y transferencia de conocimiento.</u>** • Presentación de pruebas de fabricantes ofrecidos. • Presentación de esquema de transferencia de conocimiento de la solución ofertada. • Presentación de cronograma de trabajo y temario que formara parte del entrenamiento ofertado **B. SOLUCION HIPERCONVERGENCIA** a) **CARACTERISTICAS GENERALES** o La solución propuesta debe contar con capacidad nativa de réplica bidireccional desde y hacia el clúster actualmente existente en INTRANT con opciones de replicación en forma síncrona o asíncrona y sin necesidad de software adicional. La replicación debe ser granular a nivel máquina virtual y completamente independiente del hipervisor utilizado soportando incluso la replicación entre ambos clúster aun cuando en ellos se estuvieran utilizando hipervisores distintos. o El proponente deberá incluir los catálogos o manuales para soportar técnicamente cada una de las respuestas. o Suministrar una solución, compuesta por recursos de cómputo, almacenamiento, gestión centralizada, software de Hiperconvergencia de forma integrada homologada y preinstalada de fábrica que aproveche los componentes locales de cada unidad y cree una plataforma de Nube Privada distribuida con capacidad de crecimiento modular ilimitado en el mismo clúster donde todas las funcionalidades estén basadas en el software y no dependan de un componente de hardware específico para su funcionamiento. o El software de Hiperconvergencia debe poder implementarse sobre diferentes fabricantes de hardware x86. o El software de Hiperconvergencia debe poderse implementar sobre servidores con procesadores Intel o AMD. o El proponente deberá hacer entrega de la infraestructura mínima para el correcto funcionamiento de la solución ofertada. Esta deberá ser instalada y configurada correctamente por parte del Fabricante o el proponente con ingenieros debidamente certificados. o La solución ofertada debe incluir el hipervisor que permita la creación del ambiente virtual de la entidad. Este debe incluir el soporte y actualizaciones a nuevas versiones sin costo adicional durante el periodo de garantía. Tanto el hipervisor como el software de Hiperconvergencia deben ser del mismo fabricante. o El software de Hiperconvergencia ofertado deberá estar calificado como líder en el cuadrante mágico de Gartner más reciente para infraestructura Hyperconvegente (HCI MQ) e igualmente sea calificado como líder en el

último reporte de infraestructura Hyperconvegente de "Forrester Wave".

- La solución debe incluir de forma nativa una arquitectura que provea a nivel de hardware y software un esquema de alta disponibilidad de tal forma que, ante la falla de un nodo, se mantenga operativo el clúster sin afectar el desempeño de las aplicaciones, este esquema no debe incorporar elementos que hagan la función de testigo (witness, quorum o similar).
- La solución de Hiperconvergencia debe estar en capacidad de consolidar diferentes servicios de Storage como Servidores de Archivos y almacenamiento de data no estructurada
- El sistema debe tener la habilidad de exportar capacidad en su pool de almacenamiento definido por software para que sea usada por otros servidores en el mismo datacenter. Esto se logra mediante el uso de los siguientes protocolos estándar de almacenamiento: CIFS/SMB, iSCSI, NFS.
- La solución de Hiperconvergencia debe contar con la funcionalidad para el despliegue a través de un Wizard de Configuración, uno o varios Servidores de Archivos vía NFS y SMB. Esta característica debe consistir en una o varias máquinas virtuales, combinadas en una instancia de servidor de archivos o clúster. Dentro de un único clúster de Hiperconvergencia, se deben poder crear múltiples instancias de servidores de archivos. La capacidad mínima ofrecida para este servicio debe ser de 1 TB.
- El Servidor de Archivos, debe incluir funcionalidades de analítica con las siguientes características:
  - **i.** Tendencias en el consumo de la capacidad del almacenamiento en el tiempo.
  - **ii.** Proveer información de la antigüedad de los datos almacenados en el servidor de archivos.
  - **iii.** Proveer alertas de anomalías que midan operaciones de archivos que exceden un límite predeterminado.
  - **iv.** Medir eventos de negación de acceso a archivos no autorizados
  - **v.** Mostrar la distribución de archivos por tamaño y tipo de archivo
  - **vi.** Mostrar el Top 5 de usuarios activos en un rango de tiempo
  - **vii.** Mostrar Top 5 de Archivos accedidos en un rango de tiempo
  - **viii.** Proveer Información de Auditoría que muestre la actividad de un usuario o dirección IP o archivo o carpeta en un rango de tiempo determinado.
- La solución de Hiperconvergencia debe estar en capacidad de ofrecer una solución de almacenamiento de objetos. Este almacenamiento debe soportar la API de S3 para usos como Backup, retención a largo plazo, Big Data y DevOpsLa capacidad ofrecida para este servicio debe ser mínimo 2 TiB.

b) **CARACTERISTICAS DEL HIPERVISOR**

- La administración de la plataforma completa debe ser desde una misma consola de gestión basada en web sin requerir la instalación de una consola o software adicional.
- Debe ofrecer el servicio nativo para el manejo de imágenes y/o plantillas de máquinas virtuales disponibles para el hipervisor.

- Debe permitir la adición en caliente de recursos de memoria y capacidad de almacenamiento a una máquina virtual
- Debe incluir la funcionalidad de ubicación inteligente de máquinas virtuales utilizando estadísticas de uso de CPU/RAM/almacenamiento del clúster en tiempo real de manera que se garantice a las cargas de trabajo el mejor acceso posible a los recursos. Esta funcionalidad debe venir habilitada por defecto.
- Debe incluir un portal de auto aprovisionamiento de recursos de cómputo y almacenamiento que permita la asignación de recursos a áreas de desarrollo o pruebas con la capacidad de creación de catálogos de máquinas virtuales. Debe soportar autenticación en este portal mediante el directorio activo.
- Debe poder ser actualizado desde la misma consola gestión del sistema Hyperconvegente a las últimas versiones sin disrupción del servicio.
- Debe incluir las herramientas necesarias para ver todas las estadísticas funcionales y operacionales del clúster a nivel de máquina virtual.
- Debe permitir definir reglas de afinidad y anti-afinidad entre los nodos del clúster
- Debe permitir entregar y gestionar direccionamiento IP dinámico y estático para máquinas virtuales sin requerir productos adicionales de terceros
- Debe soportar alta disponibilidad para las máquinas virtuales y ante la caída de un nodo, las maquina virtuales se reinicien de forma automática en otro nodo.
- Debe soportar la compatibilidad automática entre diferentes modelos y generaciones de CPUs del mismo fabricante sin necesidad de configuraciones manuales para este propósito.
- Debe permitir la creación, clonación, borrado, y protección mediante puntos de restauración automáticos de máquinas virtuales.
- Debe permitir la definición de redes virtuales (SDN) mediante un switch virtual distribuido en todo el clúster con soporte y mapeo de vlans, link aggregation, y visualización de estadísticas de red sobre los puertos físicos del switch TOR.
- Debe permitir la migración en caliente de Máquinas virtuales en el clúster entre diferentes nodos.
- El Hipervisor debe incluir funciones que permitan el manejo de reservas de recursos para garantizar la alta disponibilidad en situaciones de clúster no homogéneos

c) **CARACTERISTICAS DEL HARDWARE DE HIPERCONVERGENCIA**

- La solución debe estar compuesta por cuatro (4) nodos de máximo 2 unidades de Rack cada uno con los siguientes componentes mínimos por nodo:
  i. 2 x procesadores Intel Xeon Silver Processor 4210 (2.2 GHz, 10 cores, Cascade Lake)
  ii. 512 GB RAM DDR4
  iii. 4 x 8TB HDD
  iv. 2 x 1.92TB SSD
  v. 1 x Dual-port, SFP+ Network Adapter

vi. 3 años de soporte 24 horas los 7 días de la semana en hardware
vii. 3 años de licenciamiento de software
viii. Fuentes de poder redundantes
ix. Ventiladores redundantes

d) **CARACTERISTICAS DEL SOFTWARE DE HIPERCONVERGENCIA**

- La solución debe soportar al menos 3 diferentes tipos de hipervisores tales como VMware ESXi, Microsoft Hyper-V y/o una distribución basada en KVM. Igualmente debe estar soportada la instalación del software en instancias de nube pública como AWS.
- El sistema Hyperconvegente debe llevar a cabo las tareas de compresión y deduplicación completamente en software sin requerir el uso de ninguna tarjeta PCI ni dispositivo de hardware especializado para esta labor. La compresión debe ser configurable ya sea en línea (tiempo real) como post-proceso usando un intervalo configurable por el administrador.
- Las funcionalidades de compresión y deduplicación deben poder activarse o desactivarse por parte del administrador del sistema y en cualquier momento. Ya sea que ambas estén activas o solo una de las dos en el clúster.
- La solución debe poder ejecutar tareas de compresión y deduplicación a lo largo de todo el clúster y no limitadas al contenido de los discos de cada nodo.
- El sistema de Hiperconvergencia debe contar con mecanismos de eficiencia de espacio como, Compresión y Deduplicación que se ejecuten en software tanto para clúster con almacenamiento híbridos (SSD + HDD) como para clúster de almacenamientos de solo estado sólido indistintamente.
- En el mismo clúster se debe poder mezclar nodos con distintos tipos de almacenamiento (hibrido y solo estado sólido)
- La solución de Hiperconvergencia debe estar en capacidad de presentar su almacenamiento a servidores externos al clúster por medio de iSCSI.
- La solución debe soportar Windows Failover Clustering, tecnología que permite alta disponibilidad para aplicaciones configuradas en clúster (sobre el sistema operativo Windows Server 2012 R2 o superior) para que transparentemente realice el failover hacia otra VM ubicada en el mismo o en diferente host.
- Debe poder instalarse en el mismo clúster, nodos con:
  i. Diferentes configuraciones de CPU (número de cores y diferentes generaciones de procesador).
  ii. Diferente tamaño de RAM
  iii. Diferente capacidad de almacenamiento y tipo (hibrido con discos rotacionales y de estado sólido, como también nodos con almacenamiento todo de solo estado sólido)

(Todas las tecnologías de Alta Disponibilidad (HA) deben funcionar tal como fueron diseñadas aún con clúster heterogéneos.)

- La solución debe permitir agregar nodos solamente de capacidad de almacenamiento sin agregar simultáneamente capacidad de cómputo al

clúster.

- La solución debe permitir agregar nodos solamente de capacidad de cómputo sin agregar simultáneamente capacidad de almacenamiento al clúster.
- La solución debe permitir agregar discos de diferente tipo (rotacionales y/o estado sólido) con diferente capacidad en cada nodo.
- La solución debe incluir la funcionalidad de replicación asincrónica nativa de datos (sin requerir la instalación de software adicional) que cumpla con los siguientes requerimientos básicos: Replica a nivel de máquina virtual de forma granular
    i. Mecanismos de compresión de los datos a ser replicados.
    ii. Replicación bidireccional entre dos centros de datos.
    iii. Posibilidad de limitar el ancho de banda usado por la replicación desde la interfaz de administración de la solución Hyperconvegente.
    iv. Soporte para integrar la solución con el servicio VSS (Volume Shadow Copy Service) de Microsoft.
    v. Replicar máquinas virtuales entre dos hipervisores diferentes convirtiendo la máquina virtual de un hipervisor a otro de forma automática
- El sistema Hyperconvegente debe soportar nodos con Self-Encrypting Drives (SEDs)
- El sistema debe contar con un nivel de aseguramiento (hardening) aplicado de fábrica y asimismo contar con un mecanismo nativo para automatizar la remediación de las desviaciones con respecto al hardening que puedan ocurrir durante todo el ciclo de vida de la solución, sin la ejecución de tareas manuales por parte de un administrador.
- El fabricante debe documentar las mejores prácticas de seguridad para su plataforma HCI y debe ponerlas a disposición de sus clientes.
- El sistema Hyperconvegente debe proveer un mecanismo de snapshot que:
    i. Haga uso de la técnica Redirect-on-Write para la eficiencia de espacio
    ii. Sea independiente de cualquier funcionalidad de snapshot heredada del hipervisor.
- La solución debe incluir la opción de configurar un factor de replicación 2 o 3 (en los casos que aplique) a nivel de contenedor de almacenamiento permitiendo que diferentes factores de replicación puedan ser activados en el mismo clúster simultáneamente.
- El sistema debe incluir una "Papelera de Reciclaje" la cual permita restaurar una Máquina Virtual eliminada completamente, sin depender de herramientas de terceros o soluciones de Backup externas.
- El sistema debe ofrecer la capacidad de mantener consistente la replicación de un grupo de volúmenes y/o máquinas virtuales de tal manera que los snapshot se tomen en el mismo punto en el tiempo. La detención de la réplica de uno de los volúmenes o Máquinas virtuales en el grupo de consistencia debe detener la réplica de todo el grupo.
- El sistema debe proveer la capacidad de programar la toma periódica de snapshots a máquinas virtuales, sin depender de funcionalidades heredadas

del hipervisor

- El sistema debe soportar la creación de un disco virtual cuya capacidad es mayor a la capacidad disponible en el nodo en que reside. Todas las tecnologías de Alta Disponibilidad y protección de datos con que cuente la solución deben estar disponibles para un disco virtual con esta característica.
- El sistema debe contar con la habilidad nativa de alojar snapshots en la nube pública de Amazon (AWS) o Microsoft (Azure) sin requerir ningún producto adicional del fabricante ni de terceros
- El sistema debe hacer uso de una porción de la memoria RAM asignada como cache de lectura
- El sistema debe hacer que todos los SSD instalados estén disponibles como medio de almacenamiento primario, y no solamente para almacenar metadatos o para hacer cache.

e) **CARACTERISTICAS DE ADMINISTRACION DE HIPERCONVERGENCIA**

- La solución debe entregar el detalle a nivel de disco virtual, como mínimo las siguientes estadísticas: Latencias de escritura y lectura, IOPS de escritura y lectura, cantidad de datos leídos de cache, cantidad de datos leídos de SSD, cantidad de datos leídos de HDD, cantidad de datos activos (Working Set) y el porcentaje de I/O aleatorio (no secuencial). Esta información debe estar disponible sin requerir la instalación de ningún componente adicional del mismo fabricante o de terceros
- La solución deberá proporcionar un mecanismo de actualización del software de la infraestructura completa del clúster (servicios de Storage, firmware de los nodos, versión de BIOS e hipervisor) directamente desde la consola web y de forma no disruptiva, es decir, sin necesidad de reinicio de las máquinas virtuales ni indisponibilidad del servicio.
- La solución también debe soportar integración mediante el uso de REST API a otra solución de administración para facilitar la integración con ambientes de monitoreo actuales.
- La solución debe proveer un mecanismo para ingresar un nodo en modo de mantenimiento, modo en el que se debe preservar no sólo la disponibilidad de los datos sino asegurar la redundancia configurada para los datos desde el mismo momento en que el nodo queda en modo mantenimiento. Este comportamiento se debe mantener incluso si el clúster sólo tiene 3 nodos.
- La solución debe proporcionar una herramienta que pueda generar - gráficamente - un mapa de los componentes de infraestructura que conforman la solución HCI.
- La solución debe incluir una funcionalidad que automática y periódicamente haga una revisión al estado de salud de todos los componentes tanto de hardware como de software del clúster y entregue un reporte detallado para la resolución de problemas
- La solución debe incorporar una tecnología estándar en la industria para ejecutar chequeos de integridad de los datos, y no debe proveer ninguna opción para que un usuario o administrador deshabilite esta funcionalidad.

- En la solución no debe haber puntos únicos de falla en la capa de administración de la solución, todos los nodos en el sistema deben tener un módulo de software nativo en el sistema Hyperconvegente que permita hacer la administración centralizada de todo el clúster. Esta funcionalidad no debe implicar configuraciones adicionales a la del sistema.
- La solución debe incluir una funcionalidad que notifique automáticamente al fabricante acerca de condiciones de error de manera proactiva
- La solución debe incluir una funcionalidad que ejecute tareas de optimización automatizada de recursos, que permita realizar proyecciones de capacidad, tareas de planeación, basadas en tecnologías como machine learning
- La solución debe incluir una funcionalidad que realice detección de anomalías, basadas en análisis de comportamiento para generar alertas tempranas.
- La solución debe tener la capacidad de aprender el estado o condición normal de todos los elementos bajo su gestión, a lo largo del tiempo, y alertar cuando las condiciones son anormales, en lugar de esperar a que las condiciones estén violando alguna regla, política o umbral. Todo esto basado en análisis de comportamiento / machine learning.
- La solución debe incluir una función que permita al grupo de TI crear tareas automatizadas para acciones de remediación o troubleshooting, basadas en alertas a través de un Wizard de Configuración.
- La solución debe incluir un catálogo de acciones que se inicien automáticamente, ante la activación de una alerta específica. Por ejemplo, esta funcionalidad debe, ante una alerta de recursos de una VM, tener la opción de aumentar dichos recursos, generar una notificación vía correo, Slack, Servicenow o Teams y ejecutar cualquier acción adicional usando Powershell o SSH.

f) **CARACTERISTICAS DE SOPORTE A CONTENEDORES**

- La solución de Hiperconvergencia debe contar con un plugin validado para proveer almacenamiento persistente nativo para Docker, listado como Docker Volume Plugin en Docker Hub.
- La solución debe proveer un driver compatible con el estándar CSI (Container Storage Interface) soportado por Kubernetes 1.9 o superior, y que incluya las siguientes funcionalidades:
  i. Raw Block
  ii. Snapshot
  iii. Expansión
  iv. Cloning
- La solución de Hiperconvergencia debe brindar aporte certificado para la plataforma Reda OpenShift
- La solución de Hiperconvergencia debe contar, de manera nativa y sin la adquisición de software o productos adicionales del fabricante o de terceros, con una funcionalidad para automatizar la gestión del ciclo de vida de clúster Kubernetes nativos y con compatibilidad upstream completa.

B. SOLUCION RED E INTERCONEXIÓN DE CENTRO DE DATOS ALTERNO

1. Se require que la solución proveerá la conectividad que permita migrar y escalar en el futuro de manera transparente soportando enlaces de conectividad de 1G, 10G, 25G,40G,y 100G.
2. La plataforma debe brindar protección de la inversión, entregando grandes búferes, escalabilidad de capa 2 y capa 3 altamente flexible y rendimiento para satisfacer las necesidades cambiantes de nuestro centro de datos virtualizados y los entornos de nube automatizados.
3. El equipo debe poder trabajar en modo independiente, o mediante gestión centralizada administrado por el controlador de Red SDN.
4. Se require incluir los cables y conectores para interconectarlos estos dos equipos a dos similares existentes a distancia corta a velocidad de 10 Gbps mínimo de manera redundante.
5. Que ofrezca velocidad de línea, baja latencia y sin pérdidas a velocidades de 10/25/40/100 Gigabit Ethernet, Funciones de canal de fibra sobre Ethernet (FCoE) y canal de fibra, se debe incluir el licenciamiento para soportar la funcionalidad.
6. Las interfaces principales debe ser de Fibra óptica, soportando mínimo 48 Puertos que puedan operar desde 1, 10, o 25 Gbps.
7. Las interfaces de Uplink debe soportar mínimo 6 puertos operando a velocidades de 40 y 100 Gbps , también deben soportar una combinación de 1, 10, 25, 40, 50, y 100 Gbps ofertando la flexibilidad para la migración .
8. El equipo debe cumplir con las normas siguientes: FC-FEC y RS-FEC habilitado para soporte de 25-Gbps.
9. Se requiere que el equipo opere con latencia por debajo de 1 Microsegundo.
10. Se requiere que el equipo soporte Fibre Channel a 16 y 32 Gbps, incluir licencia requerida.
11. Factor de forma 1RU
12. Requiere el soporte basado en estándar VXLAN EVPN fabrics, incluyendo soporte de multi-site jerárquico.
13. Se requiere integraciones líderes en la industria para las principales aplicaciones de administración de configuración de DevOps, incluyendo los siguientes:
    - Ansible, Chef, Puppet, SALT
    - Amplia compatibilidad con el modelo nativo YANG y OpenConfig estándar de la industria a través de RESTCONF / NETCONF.
14. Throughput minimo de ancho de banda de de 3.6 Tbps
15. Modulos de fan 3+1
16. Soporte mínimo de 1.2 billones de paquetes por segundo (bpps)
17. Entradas MAC address table: 512,000
18. Debe proveer sin importar el patrón de tráfico ni las características habilitadas predecible, consistencia de la latencia del tráfico sin importar el tamaño del paquete, patrón de tráfico, o características habilitas.
19. Cantidad de entradas ACL soportadas 7000
20. Cantidad de entradas VLAN soportadas 4096
21. Cantidad de instancias VRF requeridas 16,000

22. Se requiere soporte para 64 ECMP.
23. Arquitecturas BGP de tres niveles, que permiten estructuras de red IPv6 horizontales y sin bloqueo a escala web
24. Soporte de MPLS, y MPLS TE.
25. Soporte de protocolo completo para conjuntos de protocolos de enrutamiento de Unicast y multidifusión de capa 3 (para IPv4 e IPv6), debe incluir los siguientes:
    i. BGP,
    ii. Open Shortest Path First (OSPF),
    iii. Enhanced Interior Gateway Routing Protocol (EIGRP),
    iv. Routing Information Protocol Version 2 (RIPv2),
    v. Protocol Independent Multicast Modo disperso (PIM-SM),
    vi. Multidifusión
26. Alta disponibilidad
    - Fuente de alimentación módulos de ventilador y módulos de expansión reemplazables en el campo y reemplazables en caliente
    - Redundancia de energía 1+1 2 Fuentes de Poder de 500W
    - Redundancia de módulo de ventilador N+1
27. Estandares de la industria:
    - IEEE 802.1p: CoS prioritization
    - IEEE 802.1Q: VLAN tagging
    - IEEE 802.1s: multiple VLAN instances of Spanning Tree Protocol
    - IEEE 802.1w: rapid reconfiguration of Spanning Tree Protocol
    - IEEE 802.3: Ethernet
    - IEEE 802.3ad: LACP
    - IEEE 802.3ae: 10-Gigabit Ethernet
    - IEEE 802.3by: 25-Gigabit Ethernet
    - IEEE 802.3bg: 40-Gigabit Ethernet
    - IEEE 802.3bm: 100-Gigabit Ethernet
    - SFP28 support
    - QSFP28 support
    - Remote Monitoring (RMON)
28. Integración con Sistema par existente
    - Se requiere los servicios profesionales para la instalación, configuración y puesta en funcionamiento en Alta Disponibilidad de estos dos nuevos Switches y que a la vez sean interconectados con los dos switches actualmente existentes en el Data Center mediante enlaces de Fibra Óptica Redundantes, las empresas oferentes deben considerar todos los componentes necesarios para lograr esta interconexión, a la vez, se requiere que realicen una explicación detallada tanto de la arquitectura, así como también de la forma en la cual será realizada.
    - Los servicios profesionales deben ser realizados en sitio por ingenieros capacitados y con el nivel de certificación recomendado por los fabricantes de la solucion para este tipo de implementaciones. **(Incluir Certificaciones)**
29. Servicios de Soporte y Garantía.
    - Debe contar con una garantía directamente de fábrica.
    - Debe tener un SLA mínimo de 24x7x4.

- Garantizar el reemplazo de piezas y partes, o del equipo completo en caso de presentar algún desperfecto o falla durante el funcionamiento.
- Los oferentes deberán entregar una carta de compromiso indicando que se comprometen a cumplir con este requerimiento y a entregar los contratos de garantía registrados en el fabricante a nombre de la empresa contratante.

C. **TIRADO DE FIBRA**

1. Se requiere que el oferente realice tiradas redundantes de fibra óptica desde el edificio principal del INTRANT hasta el edificio de Licencias, como forma de interconectar el centro de datos principal con el centro de datos secundario.
2. La fibra óptica a utilizar debe cumplir con los siguientes requerimientos:
   - Debe ser un tipo de fibra adecuada para uso en distribución y líneas de transmisión de alto voltaje.
   - La fibra no debe requerir de cable mensajero, siendo totalmente auto soportable
   - Posibilidad de instalación de sin mensajero y sin cables de amarre
   - El cable debe tener bloqueo de agua utilizando tecnología de núcleo seco, por lo tanto, no debe tener compuestos de inundación

Capacidad de fibra óptica

1. El cableado de Fibra Óptica debe contar con:
   - Al menos 12 hilos de transmisión
   - Todos los hilos deben fusionarse en ambas localidades.
   - Deben incluirse los materiales necesarios para la instalación en postes del tendido eléctrico
   - Se deben incluir 25 metros de holgura cada 200 metros
2. Como parte de los entregables, se requiere un reporte de validación de la fibra óptica que incluya los siguientes elementos:
   - Pruebas de conectividad entre localidades.
   - Pruebas OTDR
   - Pruebas de potencia recibida medida en ambos lados

D. Gestión de eventos e información de seguridad

- Licencia Base
- Licenciamiento para 450 Endpoints
- Licenciamiento para 1400 EPS
- Licenciamiento por 12 Meses
- 250 indicadores de Compromiso

Funcionalidades obligatorias de la solución:

1. La solución SIEM debe proporcionar una arquitectura distribuida a escala con las siguientes características:
   - Todos los componentes de la Colección, de aquí en adelante referidos como Colectores, se proporcionan como un dispositivo virtual.
   - Los recolectores envían datos de eventos al nivel de almacenamiento y

correlación

- Los recolectores pueden almacenar datos en caché en caso de que el recolector pierda comunicación con el motor de correlación principal, luego que la comunicación se reestablezca el recolector deberá de enviar los datos almacenados en caché en caso de una implementación distribuida.
- Los recolectores comprimen los datos antes de enviarlos al nivel de almacenamiento y de correlación.
- Los recopiladores se comunican con el nivel de almacenamiento y correlación a través de HTTPS. La dirección de comunicación es DESDE los recopiladores al nivel de almacenamiento y correlación.
- Si falla un colector, se puede implementar un colector de reemplazo simplemente volviendo a registrar el colector con el nivel de almacenamiento y correlación. Los recopiladores no se configuran individualmente, sino que se administran centralmente y no debe haber ninguna configuración específica, aparte de la información de la dirección IP para volver a implementar un recopilador.

Nota: no debe existir ningún licenciamiento adicional para el despliegue de n recolectores.

- Los recolectores deben ser capaces de procesar 10K EPS.
- Los recolectores deberían poder procesar la información de NetFlow.
- Los recopiladores también deberían actualizar automáticamente los nuevos analizadores cuando se actualicen nuevos analizadores en el sistema de gestión central de SIEM

2. El nivel de almacenamiento y correlación de SIEM al que ahora se hace referencia como SIEM Cluster debería:

Utilizar dispositivos virtuales (VA) en lugar de físicos segundo. Los VA debe proporcionarse para: Vmware, Hyper-V KVM iv.
Imagen de AWS disponible

El SIEM Clúster puede escalar agregando VA adicional al clúster.

Esta capacidad de escalamiento debe:

a. Proporcione correlación de reglas distribuidas en tiempo real en memoria en todos los componentes del clúster.

b. Proporcione reportes distribuidos y reportes analíticos a través del Clúster SIEM. Esto debe ser automático y el usuario no debería necesitar especificar qué componente necesita ejecutar una búsqueda En el sistema de gestión central de SIEM.

c. El Clúster de SIEM no debe limitar la cantidad de datos de eventos que se almacenan. Este límite solo debería ser la cantidad de almacenamiento que

se proporciona.

d. El SIEM Clúster debería ser capaz de escalar, esto significa que el SIEM Clúster puede comenzar con un solo VA y escalar agregando más VA. Los datos de eventos se pueden almacenar en un disco virtual cuando se trabaja con un solo VA y también en NFS cuando se trabaja con el SIEM Clúster (VA múltiples). Nota: no debe existir ningún licenciamiento adicional para el despliegue nuevos VA.

e. El SIEM Clúster debe poder escalar a más de 500K EPS.

f. El SIEM Clúster debe poder almacenar tanto el registro de eventos brutos como el registro de eventos analizados / datos normalizados.

g. No debería haber ningún requisito para un nivel de "almacenamiento" separado que filtre o envíe un subconjunto de eventos reenviados por los recopiladores a un nivel de correlación. El SIEM Clúster debe poder procesar cada evento reenviado por el nivel de colección.

h. Los datos del evento deben almacenarse en un modo comprimido.

i. El SIEM Clúster no debe usar una base de datos relacional (MS SQL, Postgresql, MySQL, Oracle) para almacenar los datos del evento. Se debe usar una base de datos moderna para almacenar datos de eventos como una base de datos no SQL.

j. Una base de datos relacional se puede usar para almacenar plantillas, incidentes y otra información estructurada.

k. Él VA debe ejecutarse en Linux y tener la capacidad de actualizar los paquetes del sistema operativo.

3. El SIEM debe ser capaz de recopilar contexto adicional más allá de los datos de registro de los dispositivos y esto debe lograrse mediante:

Descubrir activamente los dispositivos dentro de la red sin un agente y usar protocolos estándar tales como:

- SNMP
- WMI
- VM
- SDK
- OPSEC
- JDBC
- Telnet
- SSH

- JMX

a. Capacidad para controlar el estado y la capacidad de respuesta de los servicios, incluidos DNS, FTP / SCP, TCP / UDP genérico, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SMTP, SSH y Web - HTTP, HTTPS (paso único y paso múltiple).

    a. Los resultados de este monitor de disponibilidad se pueden usar para calcular la capacidad del servicio, como la disponibilidad de un servicio que está disponible al 99%.

b. Una vez descubierta, la inmersión debe presentarse en una Base de Datos de Gestión de Configuración (CMDB) dentro de la solución SIEM y mostrarse como mínimo.
    a. Versión / Firmware / OS instalado en el dispositivo.
    b. Número de serie del dispositivo
    c. Interfaces configuradas en el dispositivo junto con:
        - Nombre de la interfaz
        - IP y subred
        - Estado de la interfaz (habilitado, deshabilitado)
        - Cualquier nivel de seguridad configurado en el dispositivo
        - La velocidad de la interfaz
        - La velocidad y el nombre de la interfaz deben ser editables
    d. Procesos que se ejecutan en el dispositivo o sistema operativo
    e. Alertar cuando hay un cambio en el estado del proceso al monitorear activamente usando protocolos como se describe en los protocolos 3.a. Por ejemplo, alerta cuando un proceso o servicio se detiene.

c. Los dispositivos se deben llenar automáticamente dentro de Grupos en la CMDB, por ejemplo, Grupo de servidores de Windows, Grupo de cortafuegos.

d. Las aplicaciones que se ejecutan en dispositivos deben descubrirse automáticamente y la CMDB debe tener un grupo de aplicaciones que llene automáticamente los dispositivos del grupo. Por ejemplo, el grupo de aplicaciones "Servidores IIS" debe enumerar todos los dispositivos que ejecutan Microsoft IIS.

e. Ser capaz de informar sobre toda la información dentro de la CMDB:

f. Informe sobre el firmware de los dispositivos o el número de versión

g. Proporcione un informe de auditoría con aprobación / falla, ya sea que el dispositivo tenga la versión apropiada de Versión / Firmware / SO instalada en el dispositivo.

h. Una vez que se complete el descubrimiento activo de los dispositivos, el SIEM

debe tener una plantilla incorporada que definirá automáticamente qué métricas se recopilarán para los dispositivos y los intervalos de recolección. Las métricas se deben recopilar usando protocolos que se muestran en la sección 3.a.

i. Las métricas de rendimiento recopiladas deben incluir:
   a. Uso de la interfaz, errores, bytes enviados y recibidos
   b. UPC
   c. Memoria
   d. Disco
   e. Utilización del proceso

4. El SIEM debe proporcionar una interfaz de análisis unificada que permita que el mismo lenguaje de consulta analice tanto los datos de registro como los datos de rendimiento.

5. El sistema debería poder incluir eventos en los recopiladores que no son relevantes o que no son necesarios. Esto no debería afectar ninguna licencia.

6. Tanto los datos brutos, analizados y enriquecidos se deben pasar al clúster SIEM desde los recopiladores.

7. El procesamiento de datos de eventos debe ser realizado por analizadores sintácticos en el sistema.

8. Todos los analizadores deberían poder ser modificados y personalizados.

9. Los analizadores personalizados deberían poder crearse y definirse en la GUI sin acceso CLI.

10. Se pueden agregar nuevos atributos (variables analizadas), dispositivos y tipos de eventos a través de la GUI sin acceso CLI.

11. Los analizadores deben definirse en un marco XML con las siguientes capacidades:

- Capacidad de definir patrones que se repiten como variables.
- Posibilidad de definir funciones para identificar pares clave de valores
- Capacidad para realizar pruebas y funciones de casos
- Capacidad de realizar transformaciones en los datos en la etapa de análisis sintáctico.

12. Los dispositivos se pueden monitorear sin agentes a través de SSH, telnet WMI, JMX y PowerShell.

13. Capacidad de recopilar eventos de Windows a través de WMI y agente.

14. El SIEM debe proporcionar un Agente de Windows que tenga las siguientes capacidades:
    - Agentes administrados centralmente
    - Capaz de recoger registros de archivos de texto en dispositivos con Windows
    - Capaz de recopilar registros de eventos que no sean Seguridad, Sistema y Aplicación
    - Realizar la supervisión de integridad de archivos
    - Realizar el seguimiento del registro
    - Monitor para dispositivos extraíbles
    - Ejecute los comandos de PowerShell y envíe de vuelta la salida como registros
    - Ejecutar comandos WMI y enviar de vuelta la salida como registros
    - El agente de Windows debe enviar datos de eventos a los componentes de SIEM cifrados mediante HTTPS.

15. El SIEM debe proporcionar acceso basado en roles para restringir el acceso a los datos y también restringir el acceso a la GUI.
16. El SIEM debería ser capaz de descubrir Active Directory y LDAP y mostrar el directorio en la GUI.
17. El directorio se puede usar en condiciones de filtro dentro de informes y análisis

18. Los métodos de autenticación externa deben ser compatibles e incluyen:
    - Directorio Activo
    - LDAP
    - RADIUS

19. Posibilidad de integrar feeds de Threat Intelligence (TI):
    - Integración de archivos CSV se puede realizar a través de la GUI
    - Soporte para:
        - Direcciones IP
        - Dominios
        - Hashes
        - URLs
    - Cada TI puede admitir hasta 200.000 entradas
    - Se deben proporcionar varias integraciones a TI comerciales y del fabricante de la solución de SIEM.
    - Se debe proporcionar una cantidad de integraciones a Open Source TI en la caja
    - Posibilidad de correlacionar datos de TI en tiempo real, en memoria contra datos de eventos.
    - Posibilidad de correlacionar datos de TI con datos de eventos históricos

20. Capacidad de consultar eventos en una vista analítica en un modo de transmisión,

de modo que se informe sobre eventos antes de almacenarlos en el disco.

2. Experiencia de la empresa:

- El Oferente debe tener Certificación emitida por los diferentes **fabricantes de los equipos actuales** donde especifique que es Partner de los mismos.
- El Oferente deberá entregar una **certificación por parte de los fabricantes propuestos**, avalando la calidad y experiencia del oferente en este tipo de solución.
- **Experiencia del oferente para bienes y servicios similares:**
  - Años de fundada ➔ **mínimo 5 años**
  - Presentación del Registro Mercantil.
  - Certificación de la DGII
  - Certificación de la TSS
  - Registro Proveedores del Estado (RPE)
    - Nota: Cada una de esta documentación debe estar al día y actualizada.
  - Presentar experiencia de implementación de proyectos de envergadura similar a este proyecto:
    - Presentar Dos (2) o mas Proyecto de implementación en cada una de las soluciones requeridas.
    - Presentación de diagramas de implementación.
  - **Certificación de la empresa.**
    - El suplidor de la solución debe presentar una certificación por parte del fabricante indicando que está avalado para vender e instalar los componentes propuestos, incluyendo la siguiente certificación:
    - Advanced Data Center Architecture Specialization.
    - Para el Ítem de SIEM se requiere la acreditado vigente como Advantage, o equivalente según la marca de la solución presentada.
    - El partner debe estar acreditado como vigente como Partner Gold o Premier Partner.

3. Visita obligatoria.

1) La no participación en la visita de un oferente descarta la posibilidad de su participación en este proceso

4. Plan de Trabajo para la implementación del Proyecto:

El oferente deberá presentar un plan de trabajo que contenga las actividades principales requeridas para cada componente del proyecto, su contenido, duración, y relaciones entre sí, etapas, las fechas de entrega y de los informes a producirse en el proceso de obtención de cada componente esperado. El plan de trabajo propuesto deberá ser consistente con el enfoque técnico y la metodología, demostrando una compresión del proyecto y habilidad para traducirlos en un plan de trabajo factible.

El Plan de Trabajo deberá elaborarse con base en las mejores prácticas

recomendadas por el Project Management Institute (PMI) y conforme a los requerimientos especificados en este documento.

- Se evaluará:

a) El apego al uso de las normas PMI en cuanto la gestión de proyectos.
b) La correcta descripción de los entregables y su visibilidad en el cronograma de trabajo.
c) Que la metodología y el cronograma este firmado por un gerente de proyecto certificado, un PMP.
d) Presentación de cronograma de implementación.

5. **Estructura del equipo de trabajo**

Se solicita que las empresas oferentes cuenten con un equipo de trabajo la cual este compuesta por el siguiente personal:

a. Gerente de Proyecto
b. Encargado técnico del proyecto
c. Ingeniero de campo 1
d. Ingeniero de campo 2
e. Ingeniero de campo 3
f. Ingeniero de campo 4

Competencias del personal propuesto:

a. Gerente de Proyecto

Responsabilidades:

Es la persona que tendrá a su cargo coordinar todas las actividades a nivel general necesarias para que el proyecto se lleve a cabo de acuerdo con los objetivos y alcances planteados.

Competencias requeridas:

- Ing. en Sistemas.
- Debe poseer de manera activa y vigente la certificación de PMP.

b. Encargado técnico del proyecto

Responsabilidades:

Es la persona que tendrá a su cargo coordinar todas las actividades de carácter técnico necesarias para que el proyecto se lleve a cabo de acuerdo a los objetivos y alcances planteados, por lo que se requiere que sus competencias se relacionen con las diferentes tecnológicas requeridas en el proyecto, este tendrá bajo su responsabilidad coordinar las responsabilidades de los dos ingenieros de campo.

Debe cumplir con el siguiente perfil:

- Ing. en Sistemas.
- Poseer por lo menos diez (10) años de experiencia como profesional del área afines.
- CCIE Enterprise Infrastructure o R&S.
- Designing Cisco Data Center Infrastructure (DCID)

Estar asignado y dedicado 100% en premisa a este proyecto

c. Ing. De campo 1

Responsabilidades:

Es la persona que tendrá a su cargo ejecutar las tareas relativas a la preparación, configuración, e integración de las soluciones de Networking de Data Center requeridas en el proyecto y estará bajo las directrices del encargado técnico del proyecto.

Debe cumplir con el siguiente perfil:

- Ing. en Sistemas.
- Poseer por lo menos diez (10) años de experiencia como profesional del área afines.
- CCIE Enterprise Infrastructure o R&S.
- Cisco Certified Network Professional Data Center CCNP Data Center
- Cisco Certified Network Professional Security CCNP Security

Estar asignado y dedicado 100% on site a este proyecto

NOTA: La empresa debe presentar certificaciones del personal propuesto mostrando ser parte del personal fijo de la misma.

d. Ing. De campo 2

Responsabilidades:

Es la persona que tendrá a su cargo ejecutar las tareas relativas a la preparación, configuración, e integración de las soluciones de cómputo Hyperconvegente requeridas en el proyecto y estará bajo las directrices del encargado técnico del proyecto.

Debe cumplir con el siguiente perfil:

- Poseer las siguientes certificaciones:
- Nutanix Platform Professional (NPP)
- Nutanix Certified Professional (NCP)

NOTA: Debe laborar como parte del personal fijo de la empresa y figurar como en nómina por un tiempo mínimo de seis meses.

e. Ing. De campo 3

Responsabilidades:

Es la persona que tendrá a su cargo ejecutar las tareas relativas a la preparación, configuración, e integración de las soluciones de SIEM, y de Firewall requeridas en el proyecto y estará bajo las directrices del encargado técnico del proyecto.

Debe cumplir con el siguiente perfil:

- Tecnólogo en Redes o Similar
- NSE 4 Network Security Professional
- NSE 5 Network Security Analyst.
  (En varios de los productos incluyendo SIEM o similar en la marca propuesta.)
- NSE 7 Network Security Architect

Poseer por lo menos cinco (05) años de experiencia como profesional implementando la solución.

NOTA: Debe laborar como parte del personal fijo de la empresa y figurar como en nómina

por un tiempo mínimo de seis meses.

f. Ing. De campo 4

Responsabilidades:

Es la persona que tendrá a su cargo ejecutar las tareas relativas a la preparación, configuración, e integración de las soluciones de automatización requeridas en el proyecto y estará bajo las directrices del encargado técnico del proyecto.

Debe cumplir con el siguiente perfil:

- Tecnólogo en Redes o Similar
- Poseer las siguientes certificaciones:
- Cisco Certified DevNet Associate
- Cisco Certified DevNet Professional CCNP DevNet
- Cisco Certified DevNet Specialist - Enterprise Automation and Programmability

NOTA: Debe laborar como parte del personal fijo de la empresa y figurar como en nómina por un tiempo mínimo de seis meses.

- **SE REQUIERE LA PRESENTACION DE LAS CREDENCIALES PARA VALIDAR LOS REQUERIMIENTOS DE COMPETENCIA SOLICITADAS.**

Tomar en cuenta para implementación de solución.

- Esta propuesta es para la adquisición de productos para la expansión del sistema del Cómputo, sistema de redes de Data Center y como también de una herramienta de seguridad y monitoreo de evento de nuestra plataforma de TI, como parte de la iniciativa de reestructurar nuestro centro de datos alterno dentro de la institución y es **OBLIGATORIO PARTICIPAR EN TODOS SUS ARTÍCULOS.**

- El oferente deberá integrar con los equipos existentes.

- El oferente deberá hacer entrega de los equipos mencionados aquí, instalados y configurados (proyecto llave en mano).

- El oferente deberá transferir conocimiento de los equipos.

- El Oferente debe tener Certificación emitida por los diferentes **fabricantes de los equipos actuales** donde especifique que es Partner de los mismos.

- El Oferente deberá entregar una **certificación por parte de los fabricantes de los equipos propuestos**, avalando la calidad y experiencia del oferente en este tipo de solución.
- *Se coordinará una visita a las áreas a trabajar con todos los interesados, se informará el día y la hora de esta de acuerdo con el Cronograma.* ***VISITA OBLIGATORIA.***
    - *La no participación en la visita de un oferente descarta la posibilidad de su participación en este proceso.*
- No se aceptarán ofertas parciales o incompletas, todos los oferentes deberán proponer la totalidad del lote en que desea participar con la descripción de cada ítem. Quien haga propuesta parcial, insuficiente o incompleta se auto-descalifica sin más trámite.
- El Oferente debe incluir las garantías de los fabricantes en cada uno de los artículos de la solución.
- Serán habilitado para el sobre B aquellos oferentes que alcancen al menos un 80% de la puntuación de la evaluación técnica. Donde el valor de evaluación del sobre A es de 20% restante para completar un 100% .

Evaluación técnica del oferente	
Requisitos:	**Puntaje**
Cumplimiento con los requerimientos de Especificaciones Técnicas solicitadas, cronogramas y transferencia de conocimiento y certificaciones de la empresa. El oferente debe cumplir 100% con los requerimientos de cada ítem para poder obtener la totalidad de los puntos, de lo contrario obtendrá una puntuación de cero (0).	40
Visita obligatoria.	15
Plan de Trabajo para la implementación del Proyecto.	10
Estructura del equipo de trabajo:	15
TOTAL OFERTA TECNICA	**80**

Evaluación económica del oferente	
Requisitos:	**Puntaje**
Precio total Lote 3 El oferente con precio total menor en el lote tendrá un puntaje de 10 puntos, el segundo precio total menor del lote un puntaje de 7 puntos, el tercer precio total menor del lote puntaje de 5 puntos, y los restantes un puntaje de 0 puntos	10
Presupuesto detallado (Precio por artículo) Todo oferente que no incluya el precio de algún ítem tendrá un puntaje de 0 puntos	10
TOTAL OFERTA ECONÓMICA	**20**