"ADQUISICIÓN DE SERVIDORES DE COMPUTO HIPERCONVERGENTE Y ALMACENAMIENTO INMUTABLE"

ESPECIFICACIONES TÉCNICAS

ITEM 1. SERVIDOR DE COMPUTO Y ALMACENAMIENTO HIPERCONVERGENTE			
Características	**Descripción Técnica**	**Mínimo Exigido**	**Cumple / No Cumple**
MARCA	Especificar	EXIGIDO	
MODELO	Especificar	EXIGIDO	
NÚMERO DE PARTE	Especificar	EXIGIDO	
PROCEDENCIA	Especificar	EXIGIDO	
CANTIDAD	1 (uno)	EXIGIDO	
CARACTERISTICAS	Deberá contar con Nodos/Servidores que en conjunto formen un Cluster de Cómputo y Almacenamiento del tipo Hiperconvergente, con capacidad de Gestión del Cluster Hiperconvergente, así mismo deberá contar con una plataforma de virtualización.	EXIGIDO	
FACTOR DE FORMA	Chasis para Rack standard compatible con EIA-310D	EXIGIDO	
TAMAÑO MÁXIMO DE LA SOLUCIÓN	hasta 8U	EXIGIDO	
ARQUITECTURA DE PROCESADORES	Tipo x86 64 bits.	EXIGIDO	
CAPACIDAD TOTAL DE PROCESAMIENTO	Deberá contar con procesadores que brinden una capacidad total de al menos 256 núcleos de 2.5 GHz, cada procesador deberá contar con al con 37.5 MB de memoria caché o superior.	EXIGIDO	
CAPACIDAD TOTAL DE MEMORIA	Al menos 12,288 TB, 4800MHZ, DDR5, RDM en el cluster.	EXIGIDO	
CAPACIDAD DE ALMACENAMIENTO TOTAL	Al menos 737,28 TB RAW en discos NVMe SSD de capacidad instalada en el cluster.	EXIGIDO	
ADMINISTRACIÓN	El marco de administración debe proporcionar una interfaz de usuario gráfica intuitiva. Toda la información se debe organizar y presentar a través de áreas bien definidas con el propósito de lograr un acceso sencillo a los datos operativos. Debe ofrecer la capacidad de definir y administrar una infraestructura convergente completa desde cualquier dispositivo.	EXIGIDO	
CONEXIÓN LAN	Mínimo 2 (dos) interfaces Ethernet con 2 puertos 10GbE/25GbE con módulos SFP de 25GbE de corta distancia por cada servidor/nodo/host. (4 puertos en total). Debe poder funcionar con cualquier switch Ethernet 1GbE/10GbE/25GbE. Todos los cables Fibre Channel necesarios para la conexión LAN deberán ser proveídos.	EXIGIDO	
VENTILADORES Y FUENTES DE ALIMENTACIÓN	El sistema de ventilación (coolers) y el sistema de alimentación provisto, deberán estar preparados para soportar la instalación completa del chasis con sus bahías completas, sin producir una degradación general del sistema. Las fuentes de alimentación deberán ser redundantes.	EXIGIDO	
ALIMENTACIÓN ELÉCTRICA	La alimentación Eléctrica de los servidores/nodos/hosts deberá ser de tipo Redundante (1+1): 220 voltios corriente alterna monofásico.	EXIGIDO	
	Frecuencia en Hertz	50/60	
HERRAMIENTA / CONSOLA DE GESTIÓN O ADMINISTRACIÓN	• La interfaz de administración deberá ser accedida mediante un browser y estar basada en HTML5. • Proveer una única vista para todo el entorno manteniendo múltiples puntos de acceso. • La consola de Administración deberá ejecutarse sobre los mismos servidores/nodos/hosts del Clúster que administra, aprovechando la tolerancia a fallos del mismo (Ej. La consola debe permanecer disponible ante la falla de cualquiera de los servidores/nodos/hosts). • Proveer accesos alternativos basados en SSH y/o interfaces seriales remotas estilo IPMI. • Contener autenticación LDAP, Active Directory y certificados firmados por SSL. • Contemplar integración mediante el uso de REST API a otras soluciones de administración, a fin de facilitar la integración con ambientes de monitoreo actuales. • Tener la capacidad de facilitar una consola gráfica, que permita visualizar los recursos utilizados por las máquinas virtuales (VM) independientemente del tipo de hipervisor.	EXIGIDO	

ALMACENAMIENTO	Debe contar con un sistema de almacenamiento distribuido definida por software y proveer las siguientes funcionalidades: • Cada nodo/host, deberá contar con su propia controladora de almacenamiento. • Esquema de capas en forma automática (auto-tiering) entre los diferentes niveles, memoria, disco de estado sólido (SSD) y discos mecánicos (HDD) en tiempo real. • Deduplicación en la ingesta de información, en los discos de estado sólido (SSD) y en los discos mecánicos (HDD). • Compresión tanto en línea y en reposo. • La solución debe soportar Erasure Coding, para mejor aprovechamiento del almacenamiento. • Snapshots basados en punteros. • Sistemas de clones de máquinas virtuales. • Capacidad de usar Erasure Coding para poder hacer uso eficiente del espacio en discos mecánicos (HDD).	EXIGIDO	
	• Debe existir un sistema que permita que a lo largo del tiempo los datos más accedidos por una VM corriendo en cualquiera de los servidores/nodos/hosts, tengan siempre una copia en el almacenamiento del servidor/nodo/host local, de manera que la lectura pueda realizarse a velocidad local en la mayoría de los accesos. Este mecanismo debe converger y actualizarse de manera automática si la VM es movida/trasladada a otro servidor/nodo/host. • Thin Provisioning tanto para máquinas virtuales, como a nivel de contenedor/datastore. • Capacidad de réplica en forma sincrónica o asincrónica. • La réplica de los datos debe poder configurarse con granularidad por Máquina Virtual (VM).	EXIGIDO	
	• Debe poder replicar contra otro/s Cluster/s en el sitio local o en sitios remotos de manera sencilla. El oferente deberá validar los requerimientos e incluir todos los componentes y licencias que sean necesarios para que la réplica de datos entre clusters sea posible. Adicionalmente, la solución de réplica debe de permitir replicar máquinas virtuales entre hipervisores diferentes para poder facilitar la migración de un hipervisor a otro. • El almacenamiento debe estar diseñado especialmente para ambientes virtualizados. Debe ser compatible mínimamente con VMware, Hyper-V y AHV de Nutanix. • La arquitectura de almacenamiento debe permitir que cada servidor/nodo/host vaya integrado con una controladora para gestionar los recursos de almacenamiento en un cluster, y para todas las máquinas virtuales. Estas controladoras deben comunicarse entre sí, permitiendo gestionar el acceso desde múltiples servidores/nodos/hosts a los datos replicados.	EXIGIDO	
	• El servidor de almacenamiento no requerirá de switches de Fibre Channel ni FCoE para su funcionamiento. Solamente utilizará IP sobre Ethernet estándar (no deberá ser obligatorio configurar características específicas como Jumbo-Frames, ni otras características especiales para lograr que el Cluster opere correctamente). • Deberá tener la capacidad de distribuir los datos dentro del cluster y adicionalmente poder replicarlos internamente, para poder asegurar su disponibilidad. El factor de réplica puede ser configurado en modo 2 ó 3, dependiendo de la cantidad de nodos instalados. • Mínimamente deberá tener la capacidad de realizar respaldos a AWS (Amazon Web Services) y Microsoft Azure.	EXIGIDO	
ESCALABILIDAD	• Escalabilidad. Proveer un crecimiento lineal, estable y predecible en su rendimiento a medida que se agreguen servidores/nodos/hosts. Soportar un crecimiento en servidores/nodos/hosts, que incrementen la capacidad de procesamiento, memoria y almacenamiento. El clúster una vez establecido debe ser capaz de crecer de a un servidor/nodo/host por vez. • Deberá soportar crecimiento lineal con servidores/nodos/hosts heterogéneos, o de diferentes modelos para maximizar recursos de procesamiento, memoria o almacenamiento según se requiera. • Proveer la factibilidad de crecimientos modulares evitando así el sobre dimensionamiento del proyecto. El crecimiento tiene que ser en forma granular de hasta un servidor/nodo/host por vez incrementando los recursos globales de procesamiento, memoria, y almacenamiento en forma simultánea de todo el cluster y en diferentes proporciones, para poder acomodarse a los diferentes requerimientos.	EXIGIDO	
TIPOS DE NODOS	Se debe poder integrar servidores/nodos/hosts con diferentes características que le permitan adaptarse a los requerimientos de cada una de las aplicaciones y formando un clúster mixto. Los tipos de nodos esperados son: • Intensivos en CPU/Memoria. • Intensivos en Almacenamiento. • Nodos solamente con discos SSD.	EXIGIDO	
ALTA DISPONIBILIDAD	La infraestructura de Cómputo y Almacenamiento deberá ser distribuida y completamente definida por software, armando un clúster con las siguientes características: • Filesystem con capacidad de recuperación ante la falla de un disco o de un servidor/nodo/host completo que forma parte de la solución. • La protección de los datos deberá ser realizando múltiples copias de los datos en los discos pertenecientes a más de un servidor/nodo/host, de manera a garantizar que los datos sigan disponibles aún luego de la falla de algún componente o incluso la falla de un servidor/nodo/host completo (tolerancia a fallos). • Esta protección de datos deberá realizarse entre los múltiples servidores/nodos/hosts que componen el Clúster, de manera distribuida (no estando limitado a un esquema 1+1)	EXIGIDO	
	• En caso de una falla, la solución basada en Software debe actuar de manera automática creando nuevas copias múltiples de los datos, de manera de mantener el nivel de protección hasta tanto se reemplace el componente que haya fallado (Auto-Saneamiento de la solución)	EXIGIDO	

OPERACIONES INTELIGENTES, GOBERNANZA DE COSTOS Y AUTOSERVICIO	El servidor hiperconvergente debe contar con características de nube pública y privada que se detallan a continuación: - Reporting - Dashboard customizable - Prónostico y planeamiento de capacidad - Detección de uso ineficiente de recursos y corrección de tamaño correcto - Monitoreo de SQL Server - Descubrimiento de aplicaciones - Auto-tunning con herramientas de Machine Learning - Medición de costos para recursos de Nubes Privadas - Optimización y visibilidad de Nubes - Presupuesto y contracargo (chargeback) - Marketplace de auto-servicio - Orquestación Avanzada	EXIGIDO	
INTEGRACIÓN CON PLATAFORMA DE NUBE	• Debe tener la capacidad de integrarse con plataforma de nube, pudiendo ser mínimamente Google Cloud Platform, Microsoft Azure o AWS, y lograr migraciones o autoescalar instancias o contenedores de la infraestructura local a la nube si hubiera la necesidad. • Debe proveer una consola de gestión unificada de los recursos locales y de nube.	EXIGIDO	
INFRAESTRUCTURA DE NUBE	• El oferente deberá disponibilizar infraestructura o recursos de nube que permitan la ejecución de Instancias, así como también contenedores. • La infraestructura de nube debe poder alojar instancias migradas desde la infraestructura local, como así también debe permitir autoescalar recursos a nube. • La infraestructura de nube debe tener la capacidad de soportar carga de al menos 40 cores, 350 GB de RAM y 1,5 TB de almacenamiento	EXIGIDO	
LICENCIAMIENTO	El Oferente deberá proveer todas las licencias necesarias para que el cluster se encuentre debidamente cubierto y pueda operar sin inconvenientes de cumplimiento con la marca.	EXIGIDO	
ACCESORIOS	Todos los accesorios requeridos para entregar el equipo en perfecto estado de operación (Módulos, software, patch cords, power cord, rackmount kit)	EXIGIDO	
CAPACITACIÓN	Se deberá proveer un curso de capacitación, destinado a 4 (cuatro) técnicos del BNF. La capacitación deberá ser del tipo On The Job Training, con una carga horaria de al menos 20 horas.	EXIGIDO	
IMPLEMENTACIÓN E INTEGRACIÓN	**El oferente adjudicado deberá implementar la solución, previendo todas las** -actividades de montaje, instalación en general, configuración y puesta en funcionamiento. La implementación deberá ser coordinada con los técnicos de la Gerencia de Area de TI del BNF.	EXIGIDO	
Garantía y Soporte	El servidor debe contar con una garantía de 36 meses, la misma se iniciará con la puesta en funcionamiento del equipo adquirido. Debe incluir recambio de parte y/o equipos por RMA. El SLA requerido para la garantía debe ser del tipo 24x7x4 (24 horas al día, 7 días de la semana, con un tiempo de respuesta de hasta 4 horas.) El Oferente, a través de una constancia emitida por el Fabricante, garantizará por un periodo mínimo de 3 (Tres) años que estará en condiciones de proveer repuestos para los equipos suministrados.		
	Debe incluir soporte del fabricante las 24 horas del día, los 7 días de la semana, durante un periodo de 36 meses. Además, debe contemplar soporte remoto y presencial del Oferente también las 24 horas del día, los 7 días de la semana, por el mismo período de tiempo. El personal técnico debe encargarse de la migración de las máquinas virtuales desde la infraestructura actual hacia la solución hiperconvergente, así como de la creación de nuevas máquinas virtuales. Esto se debe llevar a cabo hasta que el personal técnico del BNF esté completamente capacitado en la gestión de la nueva infraestructura.		
CONSIDERACIONES GENERALES	• Los equipos no deben tener fecha de finalización de comercialización publicada en la pagina web del fabricante.	EXIGIDO	
	• Todos los equipos a proveer deberán ser nuevos, sin uso y en perfecto estado de funcionamiento. Todo bien a suministrar deberá pertenecer a la línea actual de productos del fabricante, y ser el más reciente estable en dicha línea. • No se tendrán en cuenta las ofertas que no presenten toda la información solicitada en las Consideraciones Generales, ya que ello no ofrecería la suficiente garantía para el buen funcionamiento de los equipos	EXIGIDO	

ITEM 2. SERVIDOR DE ALMACENAMIENTO PARA RESPALDOS			
Características	**Descripción Técnica**	**Mínimo Exigido**	**Cumple / No Cumple**
MARCA	Especificar	Exigido	
MODELO	Especificar	Exigido	
NÚMERO DE PARTE	Especificar	Exigido	
PROCEDENCIA	Especificar	Exigido	
CANTIDAD	1 (uno)	Exigido	
FACTOR DE FORMA	Chasis para Rack standard compatible con EIA-310D	Exigido	
TAMAÑO MÁXIMO DE LA SOLUCIÓN	hasta 4U	Exigido	
ARQUITECTURA DE PROCESADORES	Tipo x86 64 bits.	Exigido	
CAPACIDAD TOTAL DE PROCESAMIENTO	Mínimo 8 núcleos o superior en la solución ofertada.	Exigido	
CAPACIDAD TOTAL DE MEMORIA	Mínimo de 240 GiB en la solución ofertada.	Exigido	
CAPACIDAD DE ALMACENAMIENTO TOTAL	Mínimo de 400 TB RAW en la solución ofertada.	Exigido	
CAPACIDAD DE CRECIMIENTO	El servidor de almacenamiento del servidor debe tener como mínimo 340 TB útiles sin considerar la tasa de duplicación, la compresión, las pérdidas de formato y el área requerida para el sistema del equipo.	Exigido	
TASAS DE TRANSFERENCIA	Debe permitir llegar a tasas de transferencia de 16TB/hr para las operaciones de copia de seguridad y restauración, en sitio productivo.	Exigido	
CARACTERÍSTICAS GENERALES	Debe permitir la futura adición de al menos un controlador más (nodo de procesamiento) al mismo grupo de almacenamiento que actúe en modo activo-pasivo (conmutación por error) o de alta disponibilidad de equilibrio de carga para las tareas de copia de seguridad, de modo que, en caso de que se produzca un error de un controlador (nodo de procesamiento), las actividades de copia de seguridad se puedan redirigir automáticamente al resto de los controladores.	Exigido	
	Ninguno de los modelos ofertados podrá estar listados en el sitio del fabricante como listas de End of Life (EoL), End of Sale y End of Support (EoS) para los próximos 7 años.	Exigido	
	No se aceptarán servidores definidas por software (Dispositivo virtual).	Exigido	
	Debe ir acompañada de todas las licencias de software o hardware necesarias para obtener las funcionalidades requeridas, incluyendo: deduplicación, replicación, replicación con cifrado AES-256 y nivel de protección contra ransomware, esto debe considerar arquitecturas de múltiples sitios y cloud.	Exigido	
	Permitirá el uso de todas las funcionalidades, tecnologías y recursos especificados, de forma perpetua, sin restricciones y sin necesidad de licencias adicionales o gravámenes, ya licenciados para la capacidad máxima de expansión de la solución.	Exigido	
	El hardware componente debe tener la cantidad de memoria y capacidad de procesamiento suficiente para satisfacer las características y el rendimiento requeridos en este documento y según sus especificaciones.	Exigido	
	Debe ser independiente del software de backup, siendo al menos compatible con Veritas NetBackup, IBM Spectrum Protect (TSM), Veeam Backup & Recovery, DELLEMC NetWorker y el software Commvault, asegurando una homologación e integración completa	Exigido	
	Debe permitir que las aplicaciones Oracle (RMAN) y Microsoft SQL realicen copias de seguridad basadas en upstream (Oracle Stream Backup) y volcado de bases de datos directamente al equipo, a través de CIFS y NFS, sin utilizar software de copia de seguridad para evitar el consumo de sus licencias y sin la necesidad de licenciar volúmenes (TB) o servidores de bases de datos (CPU, Tier, Core) junto al software de copia de seguridad. Si esta característica fuera opcional en el equipamiento ofrecido, se deben incluir todas las licencias necesarias.	Exigido	
	Contar con una interfaz única basada en web o GUI que permita administrar uno o más equipos de la solución no importando su ubicación física, incluyendo opciones para cloud.	Exigido	
	Debe garantizar el deduplicado global, incluso entre distintos nodos de la solución.	Exigido	

	Debe tener mecanismos que protejan contra la inconsistencia de los datos incluso en casos de interrupción abrupta o apagado accidental.	Exigido	
	Debe tener tasas de deduplicación promedio de hasta 15:1 según tipos de datos, entregar documentación.	Exigido	
	Soporte de envío de alertas usando SNMP.	Exigido	
	Integración con herramientas para manejo de syslog centralizado.	Exigido	
	Se deberá proporcionar, junto con la solución de almacenamiento de respaldo, el acceso expreso al 2º nivel de soporte del fabricante (nivel en el que el analista de soporte está calificado para actuar directamente sobre el problema, sin necesidad de una selección previa). El analista de soporte del fabricante debe realizar adicionalmente las siguientes actividades durante todo el período de garantía: actualización de la solución de almacenamiento de respaldo, verificaciones proactivas, aclaración de dudas y apoyo a las actividades de revisión y cambio de la configuración del día a día.	Exigido	
	Capacidad de replicación por hardware con deduplicación entre dos o más sitios. Debe permitir la implementación de topologías de replicación, como 1 a 1, 1 para N, N a 1 y equipos en cascada. La solución debe permitir la replicación de los datos retenidos en la nube pública.	Exigido	
ARQUITECTURA DE LA SOLUCIÓN	La plataforma debe permitir arquitecturas de controladoras o nodos activos - pasivos de mínimo 2 participando en las tareas de backup a disco.	Exigido	
	Los crecimientos de la solución deben permitir aumentar la capacidad de disco usable como la capacidad de cómputo para aumentar el desempeño de la misma. Este crecimiento debe soportar al menos el funcionamiento integrado de treinta (30) appliances (nodos) con diferentes capacidades y manteniendo la deduplicación global, y que estos se comporten como un sistema unificado de almacenamiento.	Exigido	
	Debe tener una configuración que permita realizar los backups y recuperaciones rápidamente Ej.: Sin procesos de rehidratación para backups críticos o en el formato que entregue el software de backup de la entidad. Presentar documentación que explique el proceso.	Exigido	
	Ante la falla de una controladora debe seguir funcionando para las tareas de backup y recuperación.	Exigido	
	Debe suministrarse con discos duros conectables en caliente e intercambiables en caliente, lo que permite su reemplazo sin necesidad de interrumpir el funcionamiento de la solución.	Exigido	
	Debe entregarse con arreglos de disco duro tipo RAID-6 configurados de manera tal que tolere la falla de hasta 2 (dos) discos duros y tener al menos 1 (un) disco de hot-spare para cada grupo RAID, para los discos destinados al almacenamiento de datos de respaldo.	Exigido	
	Debe admitir simultáneamente accesos de lectura y escritura por los protocolos CIFS, NFS y OST.	Exigido	
	Debe permitir la ejecución de procesos de backup y restore en paralelo.	Exigido	
	Debe tener capacidades de tolerancia a fallos de discos, fuentes de alimentación y ventiladores.	Exigido	
	Debe permitirle replicar los datos a través de la red IP (WAN/LAN).	Exigido	
	Debe implementar mecanismos de validación de coherencia para los datos deduplicados almacenados, lo que garantice que estén en buen estado durante las copias de seguridad, las restauraciones y las replicaciones. La tecnología debe reparar automáticamente los datos que no sean consistentes con las rutinas realizadas. El mecanismo debe ser nativo del equipo, y no se aceptan scripts para dar servicio a este artículo.	Exigido	
	Debe poseer capacidades de crecimiento horizontal, esto es, la capacidad de incorporar capacidad de forma modular e integrada proporcionando con cada módulo: CPU, Memoria, Conectividad y Capacidad de Almacenamiento. Este crecimiento debe realizarse de forma transparente y sin generar silos de información dentro de la infraestructura.	Exigido	
	Se deben entregar con todos los ventiladores que soporte el chasis y deben ser módulos redundantes.	Exigido	
	Deberá poseer la capacidad de crear particionamientos lógicos que permitan segregar los accesos, designando roles y permisos sobre cada uno de los mismos.	Exigido	

	Debe ser compatible con los protocolos de supervisión SNMP y Syslog.	Exigido	
	Se debe permitir la definición de políticas de retención de inmutabilidad protegidas (proteger la información de no ser eliminada ni modificada por un plazo determinado de tiempo) por validación de doble rol (Administrador y Seguridad) para garantizar que no se produzcan cambios no autorizados.	Exigido	
	Debe contar con recursos para el monitoreo remoto por parte del fabricante, como la notificación Call-Home, para la verificación proactiva de componentes de hardware en una situación de falla o pre-falla.	Exigido	
CONECTIVIDAD	Todos los nodos, controladoras de la solución deben tener puertos IPMI o similar para administración.	Exigido	
	Debe poder incluir en sus crecimientos nodos o controladoras con configuraciones de red de 1Gbps, 10Gbps, 25Gbps.	Exigido	
	Todos los nodos, controladoras de la solución deben soportar bonding o unión de interfaces de red para mejorar el rendimiento, la fiabilidad y la redundancia de la red.	Exigido	
	Debe contar con todos los cables y accesorios necesarios para su conectividad según cantidad de puertos requeridos e integración con la infraestructura existente.	Exigido	
SEGURIDAD	Debe tener protección contra ransomware para los datos de copia de seguridad retenidos. Dicha protección debe ser del dispositivo de almacenamiento ofrecido, funcionar de forma automática y transparente, es decir, trabajar independientemente del software/utilidad de copia de seguridad, no puede depender del desarrollo de scripts de integración, no puede requerir acciones o actividades manuales sobre los datos retenidos y debe garantizar la inviolabilidad (inmutabilidad) de los datos incluso si el software de copia de seguridad o el entorno operativo donde opera está bajo el control del atacante (hacker, malware). Dicha protección debe garantizar que, incluso en situaciones en las que el atacante intente caducar el contenido de las copias de seguridad a través del catálogo de software de copia de seguridad, los datos retenidos puedan recuperarse del dispositivo de copia de seguridad proporcionado durante un período de días (hasta 30 días). Debe permitir la partición en capas, con separación lógica de volúmenes de datos.	Exigido	
	Se deben incluir funcionalidades de inmutabilidad y aislación de datos para protección frente a ataques de Ransomware.	Exigido	
	El nivel de protección contra ransomware de la solución debe ser independiente a la aplicación de backup.	Exigido	
	La propuesta debe tener una arquitectura que tenga copias de los datos protegidos sin estar expuesta a la red.	Exigido	
	Debe incluir niveles de protección basados en hardware y software ante apagados repentinos no programados, como fallas en el fluido eléctrico.	Exigido	
	Debe estar integrado con Microsoft Active Directory 2012 y versiones posteriores para la autenticación y la definición del perfil de acceso. También debe permitir la configuración de doble factor de autenticación para el acceso a la gestión del sistema a través de la integración con sistemas de contraseñas desechables (contraseña de un solo uso - OTP), como Google Authenticator, Microsoft Authenticator o similares.	Exigido	
	Debe permitir configurar usuarios y grupos basado en roles incluyendo roles de solo visibilidad, administradores, operadores, y roles de seguridad para el nivel de protección contra ransomware.	Exigido	
INTEGRACIÓN Y COMPATIBILIDAD	Se deberá garantizar la integración y compatibilidad entre las soluciones propuestas presente Lote, así como a la Infraestructura existente en la Institución.	Exigido	
IMPLEMENTACIÓN	El Oferente adjudicado deberá implementar la plataforma ofertada de manera integrada a las soluciones propuestas en el presente llamado, así como, a la infraestructura existente en la Institución.	Exigido	
	Para la implementación de la solución ofertada, el oferente adjudicado deberá disponer de ingenieros capacitados.	Exigido	
GARANTÍA Y SOPORTE	La solución propuesta deberá incluir soporte y garantía del fabricante por 36 meses.	Exigido	
	La oferta debe incluir soporte del Oferente del tipo 24x7 por el periodo de garantía.	Exigido	