**ESPECIFICACIONES TÉCNICAS**

**(SE MODIFICA El ALCANCE DEL PROYECTO NUMERAL 6 DEL LOTE II)**

**(SE INCLUYE PARTES SOMBREADAS EN DOCUMENTOS TECNICOS ENTREGABLES)**

* + - 1. **Antecedentes:**

La Dirección General de Contrataciones Públicas comenzó su serie de adquisiciones tecnológicas en el periodo 2013-2014, cuando obtuvo el Sistema Informático para la Gestión de Compras y Contrataciones del Estado, conocido como el Sistema Electrónico de Contrataciones Públicas, mediante la licitación DGCP-LPN-003-2013. En ese mismo periodo, mediante la licitación DGCP-CCC-LPN-003-2014, se adquirió la plataforma tecnológica de soporte para el sistema, la cual integraba diversas soluciones tecnológicas, como virtualización VMware, procesamiento Blade HPE C7000, almacenamiento Hitachi, respaldo Veritas, firewalls y balanceadores FortiNet.

Durante los años 2021 y 2023, la Dirección General de Contrataciones Públicas llevó a cabo adquisiciones de sistemas de almacenamiento SAN HPE Primera. En 2021, adquirió el modelo C630 mediante el proceso DGCP-CCC-PEEX-2021-0003, mientras que, en 2023, se adquirió el modelo C650 mediante el proceso DGCP-CCC-PEEX-2023-0003, este con el objetivo de iniciar el proceso de reemplazo del sistema de almacenamiento SAN Hitachi VSP G400, adquirido en el periodo 2014-2015 mediante la licitación DGCP-CCC-LPN-003-2014.

En el año 2024, con el objetivo de actualizar y modernizar de manera integral, la infraestructura tecnológica del Sistema Electrónico de Contrataciones Públicas, la DGCP, adquirió mediante el proceso MH-PT-B-LPI-2024-001 del programa BID-MH-CGR (5505/OC-DR), la infraestructura tecnológica para ampliar y fortalecer el sistema de información actual de contrataciones públicas. Se adquirieron Dispositivos de Respaldo a Disco HPE StoreOnce, Sistemas de Procesamiento Para Virtualización HPE Synergy, Sistema de Monitoreo Dynatrace y se amplió el Sistema de Almacenamiento San HPE Primera C650.

Las recientes adquisiciones han representado un avance significativo en la modernización del Sistema Electrónico de Contrataciones Públicas, fortaleciendo su capacidad de procesamiento, almacenamiento y monitoreo. Estas inversiones han permitido mejorar el rendimiento, la escalabilidad y la disponibilidad del sistema, elementos fundamentales para garantizar la eficiencia y la transparencia en la gestión de las contrataciones del Estado. No obstante, persisten áreas críticas que requieren atención prioritaria, especialmente en lo referente al fortalecimiento de la infraestructura de ciberseguridad, las redes de comunicaciones y los mecanismos de recuperación ante desastres. Abordar estas brechas es esencial para consolidar una plataforma tecnológica robusta, resiliente y alineada con las mejores prácticas internacionales en materia de gestión de sistemas de información públicos.

**Objetivo de la contratación:**

La Dirección General de Contrataciones Públicas busca actualizar su infraestructura tecnológica de ciberseguridad, recuperación ante desastres y servicios TI, así como fortalecer la seguridad de la información y estabilidad del Sistema Electrónico de Contrataciones Públicas. A tal efecto, se requieren cinco (5) lotes cuyos objetivos se consignan seguidamente.

* **Lote 1: Sistemas de Respaldo y Recuperación de Datos**

Su objetivo es garantizar la protección, disponibilidad y recuperación eficiente de la información crítica de la organización frente a incidentes como fallas de hardware, errores humanos, ciberataques o desastres naturales. El sistema se integrará con la infraestructura existente, incluyendo los equipos HPE Primera y HPE StoreOnce, con el fin de mantener un esquema de protección de datos alineado al modelo 3-2-1-1-0, que promueve la resiliencia y la integridad de la información.

* **Lote 2: Ampliación Infraestructura Ciberseguridad y Redes**

Busca fortalecer la disponibilidad, el rendimiento y la escalabilidad de la infraestructura tecnológica que soporta tanto las operaciones de ciberseguridad como la infraestructura de redes que da soporte a los servicios críticos institucionales.

* **Lote 3: Protección Correo Electrónico y Concienciación.**

Busca fortalecer las capacidades de protección del correo electrónico institucional frente a amenazas avanzadas como phishing, malware y suplantación, así como también mejorar la cultura de ciberseguridad mediante programas de concienciación dirigidos a los usuarios.

* **Lote 4: Servidor Hiperconvergente.**

Busca consolidar y optimizar la infraestructura tecnológica de los servicios de ciberseguridad mediante la adquisición de un servidor hiperconvergente de alto rendimiento, que permita unificar computo, almacenamiento y conectividad en una sola plataforma escalable.

* **Lote 5: Capacitaciones**

Su finalidad es proveer habilidades técnicas necesarias al personal operativo que gestiona la infraestructura tecnológica del Sistema Electrónico de Contrataciones Publicas.

* + - 1. **Alcance del Proyecto Respecto a cada Lote:**

La Dirección General de Contrataciones Públicas actualizará y modernizará, la infraestructura tecnológica de ciberseguridad, redes de comunicaciones y los sistemas para respaldo y recuperación de datos del Sistema Electrónico de Contrataciones Públicas. Este proyecto implica la sustitución de los componentes de infraestructura existentes y la inclusión de nuevos equipos de vanguardia que se alineen con estándares internacionales reconocidos y actualizados, asegurando la compatibilidad con la infraestructura tecnológica actual.

En este contexto, se busca implementar tecnologías de última generación que no solo mejoren la eficiencia operativa, sino que también promuevan la interoperabilidad y la adaptabilidad. Los bienes ofertados deben ser capaz de evolucionar con los cambios tecnológicos, garantizando la sostenibilidad a largo plazo, la compatibilidad con futuras actualizaciones y requisitos, así como la escalabilidad necesaria para soportar el crecimiento proyectado durante los próximos cinco años.

El listado de bienes requeridos que deberán ser presentados por los oferentes se describirán junto con las características generales para cada lote, comprendiendo lo siguiente:

* ***Lote 1: Sistemas de Respaldo y Recuperación de Datos***

1. Software Empresarial para Copias de Seguridad y Recuperación de Datos
2. Servidor para Software de Copias de Seguridad y Recuperación de Datos
3. Biblioteca de Cintas Magnéticas
4. Dispositivo Respaldo a Disco HPE StoreOnce 5260 (Este equipo es necesario para realizar la replicación de respaldos directamente desde un HPE StoreOnce ya existente en la DGCP sin necesidad de herramientas de terceros)
5. Ampliación de licencias de uso de puertos para switches FC HPE SN6600B
6. Ampliación Blade HPE Synergy 12000
7. Servicios profesionales para instalación, configuración, pruebas, validación, integración y puesta en producción de los bienes ofertados.
8. Servicios Profesionales para instalación, configuración, pruebas, validación e integración con sistema de virtualización en producción.
9. Entrenamientos y Traspaso de Conocimiento

* ***Lote 2: Ampliación Infraestructura Ciberseguridad y Redes.***

1. Ampliación Seguridad Perimetral – Fortigate 601F (Este equipo es necesario para la expansión del security fabric ya existente en la DGCP)
2. Ampliación Seguridad Perimetral - Fortinet Fortigate 401F (Este equipo es necesario para la expansión del security fabric ya existente en la DGCP)
3. Ampliación Infraestructura Seguridad Perimetral Servicio Gestión de Superficie de Ataque Externa (EASM) Fortinet FortiRecon (Este servicio es necesario para la gestión de la superficie de ataque externa y la automatización de respuesta a amenazas)
4. Equipo de Análisis y Gestión de Registros Fortinet Fortianalyzer (Este equipo es necesario para centralizar la recolección, correlación y análisis de eventos de seguridad de los equipos fortinet existentes en la DGCP)
5. Licenciamiento de autenticación multifactor Fortinet FortiToken Mobile (Este licenciamiento es necesaria para reforzar los mecanismos de autenticación de usuarios y reducir el riesgo de acceso no autorizados a sistemas críticos)
6. ORIGINAL: Expansión de Licencias FortiEDR(Esta ampliación es necesaria para extender la cobertura de protección de los endpoints, servidores y dispositivos IoT). MODIFICACION: **Renovación de Licencias FortiEDR (Esta renovación es necesaria para extender la cobertura de protección de los endpoints, servidores y dispositivos IoT).**
7. Ampliación Infraestructura Inalámbrica Puntos de Acceso Fortinet FortiAP 431F (Estos equipos son necesarios para ampliar y modernizar la infraestructura de conectividad inalámbrica existente de la DGCP)
8. Switches Core Alto Rendimiento. (Estos equipos son necesarios para fortalecer la capacidad de desempeño del núcleo de la red).
9. Switch de Accesso de Alto Rendimiento (Estos equipos son necesarios para ampliar y modernizar la infraestructura de conectividad LAN existente de la DGCP).
10. Equipo Gestión Centralizada Fortinet FortiManager FMG-410 (Estos equipos son necesarios para la centralización de la administración de la infraestructura Fortinet Existente).
11. Servicios Profesionales para Instalación, Configuración, Pruebas, Validación, integración y Puesta en producción.
12. Entrenamientos y Traspaso de Conocimiento.

* ***Lote 3: Servicio Protección Correo Electrónico y Concienciación.***

1. Servicio de protección de Correo Electrónico y Concienciación (este servicio es necesaria para fortalecer la seguridad del correo electrónico institucional, así como también para mejorar la cultura de ciberseguridad mediante programas de concienciación.)
2. Servicios Profesionales para Instalación, Configuración, Pruebas, Validación, integración, Puesta en producción y Traspaso de Conocimiento.

* ***Lote 4: Servidor Hiperconvergente.***

1. Servidor Hiperconvergente (este servidor es necesario para consolidar el cómputo, almacenamiento y conectividad en una plataforma unificada, que permita mejorar el rendimiento, la disponibilidad y la escalabilidad de los servicios críticos de ciberseguridad.)
2. Servicios Profesionales para Instalación, Configuración, Pruebas, Validación, integración, Puesta en producción y Traspaso de Conocimiento.

* ***Lote 5: Capacitaciones y Certificaciones***

1. Capacitaciones VMware
2. Voucher Certificación VMware
   * + 1. **Documentos técnicos entregables**

Para cada Lote, se detallan los siguientes documentos necesarios a ser entregados con la propuesta técnica:

**Lote 1: Sistemas de Respaldo y Recuperación de Datos**

**Item 1.1: Software Empresarial para Copias de Seguridad y Recuperación de Datos**

Carta del fabricante, dirigida a la institución y haciendo referencia al número de este proceso de adquisición en la que se indique lo siguiente:

**SE INCLUYE O ADICIONA**

**• El proveedor, en caso de no ser el fabricante, está autorizado por el fabricante para la venta del bien ofertado.**

• Artículo permite la regla de respaldo 3-2-1-1-0.

• Artículo alineado con el marco de trabajo de cibserseguridad del National Intitute of Standards and Technology.

• Artículo certificado para trabajar e integrarse con los sistemas de almacenamiento existentes en la DGCP (HPE Primera y HPE StoreOnce) y para utilizar el protocolo de comunicación propietario de HPE StoreOnce: Catalyst, como repositorio de respaldo a disco.

• Acuerdo de Nivel de Servicio (SLA por sus siglas en inglés) y la matriz de escalación que el fabricante de su oferta, en caso de no ser el mismo el fabricante, propone para la gestión de casos de soporte para cada uno de los bienes que conforman la propuesta.

• Al menos 2 representantes o distribuidores locales autorizados del artículo ofertado.

• Ciclo de vida certificado por el fabricante con al menos 5 años de vigencia a partir de la fecha de la propuesta.

**Item 1.2: Servidor para Software de Copias de Seguridad y Recuperación de Datos**

Carta del fabricante, dirigida a la institución y haciendo referencia al número de este proceso de adquisición en la que se indique lo siguiente:

**SE INCLUYE O ADICIONA**

**• El proveedor, en caso de no ser el fabricante, está autorizado por el fabricante para la venta del bien ofertado**

• Acuerdo de Nivel de Servicio (SLA por sus siglas en inglés) y la matriz de escalación que el fabricante de su oferta, en caso de no ser el mismo el fabricante, propone para la gestión de casos de soporte para cada uno de los bienes que conforman la propuesta.

• Al menos 2 representantes o distribuidores locales autorizados del artículo ofertado.

• Ciclo de vida certificado por el fabricante con al menos 5 años de vigencia a partir de la fecha de la propuesta.

**Item 1.3: Biblioteca de Cintas Magnéticas**

Carta del fabricante, dirigida a la institución y haciendo referencia al número de este proceso de adquisición en la que se indique lo siguiente:

• **SE INCLUYE O ADICIONA**

**• El proveedor, en caso de no ser el fabricante, está autorizado por el fabricante para la venta del bien ofertado**

• Acuerdo de Nivel de Servicio (SLA por sus siglas en inglés) y la matriz de escalación que el fabricante de su oferta, en caso de no ser el mismo el fabricante, propone para la gestión de casos de soporte para cada uno de los bienes que conforman la propuesta.

• Al menos 2 representantes o distribuidores locales autorizados del artículo ofertado.

• Ciclo de vida certificado por el fabricante con al menos 5 años de vigencia a partir de la fecha de la propuesta.

**Lote 2: Ampliación Infraestructura Ciberseguridad y Redes.**

**Items 2.1 - 2.10**

Carta del fabricante, dirigida a la institución y haciendo referencia al número de este proceso de adquisición en la que se indique lo siguiente:

• **SE INCLUYE O ADICIONA**

**• El proveedor, en caso de no ser el fabricante, está autorizado por el fabricante para la venta del bien ofertado**

• Acuerdo de Nivel de Servicio (SLA por sus siglas en inglés) y la matriz de escalación que el fabricante de su oferta, en caso de no ser el mismo el fabricante, propone para la gestión de casos de soporte para cada uno de los bienes que conforman la propuesta.

• Al menos 2 representantes o distribuidores locales autorizados del artículo ofertado.

• Ciclo de vida certificado por el fabricante con al menos 5 años de vigencia a partir de la fecha de la propuesta.

**Lote 3: Servicio de Protección Correo Electrónico y Concienciación.**

**Item 3.1 - Servicio de Protección Correo Electrónico y Concienciación.**

Carta del fabricante, dirigida a la institución y haciendo referencia al número de este proceso de adquisición en la que se indique lo siguiente:

**SE INCLUYE O ADICIONA**

**• El proveedor, en caso de no ser el fabricante, está autorizado por el fabricante para la venta del bien ofertado**

• Acuerdo de Nivel de Servicio (SLA por sus siglas en inglés) y la matriz de escalación que el fabricante de su oferta, en caso de no ser el mismo el fabricante, propone para la gestión de casos de soporte para cada uno de los bienes que conforman la propuesta.

• Al menos 2 representantes o distribuidores locales autorizados del artículo ofertado.

• Ciclo de vida certificado por el fabricante con al menos 3 años de vigencia a partir de la fecha de la propuesta.

**Lote 4: Servidor Hiperconvergente**

**Item 4.1 – Servidor Hiperconvergente**

Carta del fabricante, dirigida a la institución y haciendo referencia al número de este proceso de adquisición en la que se indique lo siguiente:

**SE INCLUYE O ADICIONA**

**• El proveedor, en caso de no ser el fabricante, está autorizado por el fabricante para la venta del bien ofertado**

• Acuerdo de Nivel de Servicio (SLA por sus siglas en inglés) y la matriz de escalación que el fabricante de su oferta, en caso de no ser el mismo el fabricante, propone para la gestión de casos de soporte para cada uno de los bienes que conforman la propuesta.

• Al menos 2 representantes o distribuidores locales autorizados del artículo ofertado.

• Ciclo de vida certificado por el fabricante con al menos 5 años de vigencia a partir de la fecha de la propuesta.

* + - 1. **Criterios para la ejecución y puesta en marcha del proyecto:**

La ejecución y puesta en marcha de los bienes y servicios propuestos en el actual proyecto se debe ejecutar de acuerdo con las siguientes fases en cada lote:

* **Lote 1:**
  + **Fase 1**: contempla la Reunión Kick-Off del proyecto para discutir su alcance.
  + **Fase 2:** contempla el Suministro/entrega de bienes detallados en las especificaciones técnicas.
  + **Fase 3:** contempla la prestación de Servicios Profesionales para Instalación, Configuración, Pruebas, Validación, Integración y Puesta en Producción de los bienes adquiridos.
  + **Fase 4:** contempla la prestación de servicios profesionales para instalación, configuración, pruebas, validación e integración con sistema de virtualización en producción.
  + **Fase 5:** contempla el entrenamiento contenido en la propuesta técnica.
  + **Fase 6:** entrega de informe final completo y aceptación del cierre de actividades para este lote.
* **Lote 2:**
  + **Fase 1**: contempla la Reunión Kick-Off del proyecto para discutir su alcance.
  + **Fase 2:** contempla el Suministro/entrega de bienes detallados en las especificaciones técnicas.
  + **Fase 3:** contempla la prestación de Servicios Profesionales para Instalación, Configuración, Pruebas, Validación, Integración y Puesta en Producción de los bienes adquiridos.
  + **Fase 4:** contempla el Entrenamiento contenido en la propuesta técnica.
  + **Fase 5:** Entrega de informe final completo y aceptación del cierre de actividades para este lote.
* **Lote 3:**
  + **Fase 1**: contempla la Reunión Kick-Off del proyecto para discutir su alcance.
  + **Fase 2:** contempla el Suministro/entrega de bienes detallados en las especificaciones técnicas.
  + **Fase 3:** contempla la prestación de Servicios Profesionales para Instalación, Configuración, Pruebas, Validación, Integración y Puesta en Producción de los bienes adquiridos.
  + **Fase 4:** Entrega de informe final completo y aceptación del cierre de actividades para este lote.
* **Lote 4:**
  + **Fase 1**: contempla la Reunión Kick-Off del proyecto para discutir su alcance.
  + **Fase 2:** contempla el Suministro/entrega de bienes detallados en las especificaciones técnicas.
  + **Fase 3:** contempla la prestación de Servicios Profesionales para Instalación, Configuración, Pruebas, Validación, Integración y Puesta en Producción de los bienes adquiridos.
  + **Fase 4:** Entrega de informe final completo y aceptación del cierre de actividades para este lote.
* **Lote 5:**
  + **Fase 1**: Contempla la Reunión Kick-Off del proyecto para discutir su alcance.
  + **Fase 2:** Contempla el Suministro/entrega de bienes detallados en las especificaciones técnicas.
  + **Fase 3:** Aceptación del cierre de actividades para este lote.

La entrega se considerará perfeccionada y cumplido el contrato una vez que se hayan ejecutado todas las actividades antes mencionadas y sean aceptadas por parte de la Dirección General de Contrataciones Públicas. Acontecida la entrega, se procederá a suscribir entre ambas partes el acta de Finalización del Servicio, indicando la culminación de este y el pleno cumplimiento de que se han completado las obligaciones de acuerdo con lo establecido en este documento.

Especificaciones Técnicas

(SE INCLUYE PARTES SOMBREADAS EN DOCUMENTOS TECNICOS ENTREGABLES)

| **ITEM** | **DENOMINACIÓN DEL EQUIPO:** | **ESPECIFICACIONES TÉCNICAS REQUERIDAS** | **ESPECIFICACIONES TECNICAS DEL BIEN OFERTADO** | **MODELO Y/O MARCA** | **PAÍS DE ORIGEN** |
| --- | --- | --- | --- | --- | --- |
| **Lote I: Sistemas de Respaldo y Recuperación de Datos** | | | | | |
| **1.1** | **Software Empresarial para Copias de Seguridad y Recuperación de Datos** | Un (1) software empresarial para copias de seguridad y recuperación de datos que cumpla con al menos las siguientes características:   * Licenciamiento para al menos 450 máquinas virtuales. * Licenciamiento, suscripción y soporte 24/7 por 3 años. * Respaldo de máquinas virtuales, bases de datos, sistema de correos Microsoft Exchange, file servers y Active Directory. |  |  |  |
| Implementado y en cumplimiento con la regla de respaldo 3-2-1-1-0. La regla 3-2-1-1-0 de respaldo debe ser:   * 3 copias de la data * 2 tipos de medios diferentes * 1 copia fuera de la localidad * 1 copia fuera de línea, aislada o inmutable * 0 (cero) errores en pruebas de recuperabilidad   Nota: Se debe demostrar mediante carta del fabricante que el software permite la regla de respaldo 3-2-1-1-0. |  |
| El fabricante del sistema debe estar incluido como líder en la versión más reciente del cuadrante mágico de Gartner para Soluciones de software empresarial para copias de seguridad y recuperación, con el fin de demostrar su tendencia y madurez en el mercado. |  |
| Debe estar alineado con el marco de trabajo de cibserseguridad del National Intitute of Standards and Technology.  Nota: Demostrable mediante carta del fabricante. |  |
| Debe licenciarse por carga de trabajo o instancia, donde cada instancia puede respaldar una máquina virtual o una máquina física. Se debe licenciar para 450 máquinas virtuales. No debe requerir licencia por capacidad.  Se debe incluir el licenciamiento, suscripción y soporte 24x7 por 3 años. |  |
|  |  | El software de copias de seguridad debe ofrecer licencias basadas en instancias sin restricciones sobre el tipo de almacenamiento protegido (compatibilidad con tecnologías heterogéneas), capacidad de producción en el entorno de origen o capacidad de destino para el respaldo en disco. |  |  |  |
|  |  | Debe permitir el análisis de tendencias para la planificación de capacidad en el entorno de respaldo, con alertas avanzadas e informes personalizables con formatos preconfigurados. Se debe incluir el licenciamiento necesario. |  |  |  |
|  |  | Debe proporcionar monitoreo en tiempo real (24x7) con vistas detalladas y de alto nivel sobre la salud, rendimiento y carga de trabajo de los servidores virtuales. |  |  |  |
|  |  | Debe contar con un panel de seguridad y cumplimiento integrado. |  |  |  |
|  |  | Debe soportar acciones automatizadas para alarmas críticas (automatizadas o semi-automatizadas) con vistas detalladas sobre la salud, rendimiento y carga de trabajo de los servidores virtuales. |  |  |  |
|  |  | Debe incluir una consola de administración centralizada que reporte todo tipo de estadísticas relativas a los jobs de respaldo configuradas, con generación de alertas. |  |  |  |
|  |  | Debe permitir restaurar máquinas virtuales (VMs) directamente en proveedores de nube como AWS, Azure o Google desde la copia de respaldo. |  |  |  |
|  |  | Debe ser capaz de extender el repositorio de respaldo a un servicio en la nube pública mediante la transferencia de archivos antiguos a almacenamiento S3 compatible o Azure BLOB. |  |  |  |
|  |  | Debe tener la capacidad de archivar datos en almacenamiento de bajo costo como Amazon Glacier o Azure Archive Tier y restaurarlos sin dependencia del proveedor de la nube. |  |  |  |
|  |  | Debe soportar respaldo sin agentes de aplicaciones dentro de máquinas virtuales, como Microsoft SQL, Exchange, SharePoint y Oracle, con recuperación granular sin necesidad de restauración intermedia. |  |  |  |
|  |  | Debe permitir la copia de seguridad de datos on-premises directamente en repositorios en la nube como AWS S3 o Microsoft Blob. |  |  |  |
|  |  | Debe aprovechar almacenamiento inmutable en la nube (S3-Immutable) para evitar la corrupción de copias de respaldo o ataques de ransomware. |  |  |  |
|  |  | El software de copias de seguridad debe contar con reglas YARA para la detección de amenazas. |  |  |  |
|  |  | Debe permitir análisis bajo demanda para la detección de malware. |  |  |  |
|  |  | Debe contar con detección en línea e indexación en invitado para detectar malware dentro de las máquinas virtuales respaldadas. |  |  |  |
|  |  | Debe implementar el esquema de aprobación de cuatro ojos para la eliminación de cualquier respaldo. |  |  |  |
|  |  | Debe ser un software agnóstico de hardware, con integración de snapshots para VMware, Hyper-V, Nutanix AHV y RHEV, y soportar de duplicación en cualquier destino de almacenamiento. |  |  |  |
|  |  | Debe permitir el respaldo a cintas LTO para retención a largo plazo. |  |  |  |
|  |  | Debe proporcionar recuperación instantánea para respaldos de VMware y Hyper-V, así como para cargas de trabajo en AHV. |  |  |  |
|  |  | Debe permitir la recuperación de archivos desde cualquier respaldo de una máquina virtual o servidor físico y proporcionar una recuperación completa del sistema en caso de fallo, ya sea en un entorno físico, virtual o como una instancia en la nube (AWS, Azure, Google). |  |  |  |
|  |  | Debe ofrecer integración con Syslog y ServiceNow. |  |  |  |
|  |  | Debe permitir la recuperación instantánea de bases de datos MS SQL y Oracle desde archivos de respaldo. |  |  |  |
|  |  | Debe ofrecer autenticación multifactor para el acceso a la consola de respaldo y contar con un sistema de cierre automático de sesión. |  |  |  |
|  |  | Debe contar con una función de validación de datos, permitiendo encender las máquinas virtuales respaldadas en un entorno de prueba para verificar su recuperabilidad. |  |  |  |
|  |  | Debe permitir la verificación automatizada de recuperación, donde el servidor arranca desde la copia de seguridad y se verifica la recuperación de la imagen de la máquina virtual, el sistema operativo invitado y la consistencia de las aplicaciones. Debe generar informes automáticos para auditorías de respaldo y recuperación. |  |  |  |
|  |  | Debe ofrecer capacidades de respaldo y replicación desde una única consola, integrándose con RBAC (Control de Acceso Basado en Roles) del hipervisor para que los usuarios puedan iniciar respaldo y restauración solo en las VMs a las que tienen acceso. |  |  |  |
|  |  | Debe soportar repositorios Linux endurecidos, protegiendo los respaldos contra ataques de ransomware. |  |  |  |
|  |  | Debe admitir Cuentas de Servicios Gestionadas en Grupo (GMSA), permitiendo a los usuarios establecer políticas de cambio de contraseña cada 30 días y cumplir con normas de contraseñas seguras. |  |  |  |
|  |  | Debe permitir el respaldo de almacenamiento de objetos. |  |  |  |
|  |  | Debe contar con restauraciones en etapas, permitiendo la eliminación selectiva de archivos para cumplir con normativas como GDPR. |  |  |  |
|  |  | Debe permitir la recuperación instantánea de archivos en almacenamiento NAS, asegurando el acceso rápido a los datos tras un desastre. |  |  |  |
|  |  | Debe permitir configurar los niveles máximos aceptables de latencia I/O en las unidades de producción, asegurando que las operaciones de respaldo y replicación no afecten la disponibilidad del almacenamiento de producción. |  |  |  |
|  |  | Debe soportar la recuperación de elementos individuales de aplicaciones, archivos, carpetas y máquinas virtuales completas desde copias de seguridad a nivel de imagen, con un RTO menor a 15 minutos. |  |  |  |
|  |  | Debe ser eficiente en red, con replicación segura de datos con cifrado de longitud variable en la fuente y compresión para optimizar la transmisión a través de redes WAN, sin requerir obligatoriamente un acelerador WAN de terceros. |  |  |  |
|  |  | Debe ofrecer replicación de máquinas virtuales a nivel de VM, con o sin respaldo previo en el sitio de origen. Debe soportar failover y failback automático, incluyendo la capacidad de adquisición automática de direcciones de red en el sitio de destino. |  |  |  |
|  |  | Debe soportar la replicación de cargas de trabajo entre sistemas heterogéneos (infraestructura hiperconvergente a servidores independientes o almacenamiento con hipervisores similares en diferentes sitios), permitiendo la creación de un entorno de recuperación ante desastres sin dependencia del hardware subyacente. |  |  |  |
|  |  | Debe permitir realizar respaldos en una plataforma y restaurarlos en otra, facilitando la recuperación ante desastres sin depender de un hardware específico. |  |  |  |
|  |  | Debe permitir el respaldo de máquinas virtuales en la nube (AWS/Azure) y su restauración en entornos VMware on-premises. |  |  |  |
|  |  | Certificado para trabajar e integrarse con los sistemas de almacenamiento existentes en la DGCP (HPE Primera y HPE StoreOnce) y para utilizar el protocolo de comunicación propietario de HPE StoreOnce: Catalyst, como repositorio de respaldo a disco  Nota: Demostrable mediante carta del fabricante. |  |  |  |
|  |  | Se debe incluir un (1) año de servicio de un Encargado Técnico de Cuenta, (Technical Account Manager, TAM). El servicio TAM debe incluir el equivalente de al menos un día hábil de servicio por semana durante un período de doce (12) meses.  El TAM debe ser proporcionado directamente por el fabricante del software empresarial de copias de seguridad propuesto, siendo empleado de este, y no del canal oferente.  El TAM debe ser un profesional experto en el software ofertado cuyo objetivo será proporcionar dirección técnica y estratégica, analizar la infraestructura tecnológica existente y los objetivos de la DGCP, recomendar configuraciones de implementación y garantizar que la infraestructura y políticas de la plataforma de respaldo cumplan con las mejores prácticas.  El TAM deberá apoyar en los siguientes procesos, sin ser estos limitativos:   * Alineación con el negocio. * Abordar necesidades y objetivos específicos. * Vistas ejecutivas y técnicas. * Informes de estado programados periódicamente. * Vistas de resumen. * Actualizaciones semanales del proyecto/estado. * Revisiones de mejores prácticas y comprobaciones del estado mediante la recopilación automatizada de datos de la infraestructura, el inventario, los datos de configuración y la utilización de la herramienta. |  |  |  |
|  |  | El proveedor deberá realizar la implementación del software de copias de seguridad siguiendo las mejores prácticas recomendadas por el fabricante y en acuerdo con los lineamientos establecidos por el equipo técnico de la DGCP, para lo cual, podrían establecerse al menos 2 instancias del software de copias de seguridad para respaldar ambientes de virtualización distintos. |  |  |  |
|  |  | El proveedor deberá realizar la implementación del software de copias de seguridad con los ítems 1.2, 1.3, 1.4 y la integración con los siguientes equipos existentes: almacenamiento HPE Primera, HPE StoreOnce. El alcance de la implementación e integración contempla lo siguiente en dos centros de datos distintos, sin ser esto limitativo:  **SE MODIFICA EN LO ADELANTE**  En el Sitio 1:   * RPO de 2 horas. * RTO para falla de VM, app, LUN: ≤ 1 hora * RTO para pérdida total de sitio sin infraestructura DR: ≥ 8 horas * Instalación y configuración del software de copias de seguridad en servidor provisto en el ítem 1.2 * Configuración de políticas de respaldo para 22 servidores virtuales de aplicativos y active directory (2TB), 3 servidores virtuales MS SQL (40TB) y 13 servidores virtuales de archivos (50TB). * Configuración de políticas de respaldo, restauración e inmutabilidad basado en las reglas 3-2-1-1-0 * Integración con HPE Primera existente en Sitio 1 para realización de Snapshots y guardar respaldos. * Integración con HPE StoreOnce existente en Sitio 1 para guardar respaldos. * Integración con HPE StoreOnce 5260 provisto en el ítem 1.4 para replicación de respaldo fuera de sitio. Este StoreOnce se instalará en el Sitio 2. * Integración con una de las dos bibliotecas de cintas magnéticas provistas en ítem 1.3 para respaldos en cintas LTO fuera de sitio. Esta biblioteca de cintas se instalará en el Sitio 2.   En el Sitio 2:   * RPO de 2 horas. * RTO para falla de VM, app, LUN: ≤ 1 hora * RTO para pérdida total de sitio sin infraestructura DR: ≥ 8 horas * Instalación y configuración del software de copias de seguridad en servidor existente provisto por la DGCP. * Configuración de políticas de respaldo para 65 servidores virtuales de aplicativos y active directory (12TB), 5 servidores virtuales MS SQL (10TB), 3 servidores virtuales MS Exchange (10TB) y 2 servidores virtuales de archivos (22TB). * Integración con HPE Primera existente en Sitio 2 para realización de Snapshots y guardar respaldos. * Integración con HPE StoreOnce existente en Sitio 2 para guardar respaldos. * Integración con la segunda biblioteca de cintas magnéticas provistas en ítem 1.3 para respaldos en cintas LTO.   **SE INCLUYE O ADICIONA**  **Notas:**   * **Se realizarán respaldos a ambientes 100% virtualizados con VMware vSsphere 8.0.3.** * Ya existe la infraestructura en fibra óptica y de comunicación para la replicación de datos entre el HPE StoreOnce del Sitio 1 y el HPE StoreOnce del Item 1.4, a instalar en el Sitio 2. * Los equipos HPE Primera y HPE StoreOnce existentes en los Sitios 1 y 2 ya están en funcionamiento. |  |  |  |
|  |  | El oferente deberá incluir en su oferta un Plan de Validación y Pruebas que contemple la verificación del cumplimiento de la regla de respaldo 3-2-1-1-0, el cual debe incluir como mínimo:   * Descripción detallada de la arquitectura de respaldo propuesta, indicando ubicación, tipo de medios, aislamiento/inmutabilidad, y frecuencia de respaldo. * Procedimientos y cronograma de pruebas de restauración, con al menos dos escenarios de recuperación en ambiente controlado. * Mecanismos para validar la integridad y éxito de las pruebas de restauración, asegurando 0 (cero) errores. * Roles y responsables durante el proceso de validación.   **SE INCLUYE O ADICIONA**  Nota: El Plan de Validación y Pruebas **DEBE** ser entregado con la oferta técnica.  La DGCP organizará una sesión técnica con los proveedores a fin de proporcionar la información necesaria para la elaboración del plan de validación y pruebas. |  |  |  |
|  | **Garantía:** | El oferente debe indicar el Acuerdo de Nivel de Servicio (SLA por sus siglas en inglés) y la matriz de escalación que el fabricante de su oferta, en caso de no ser el mismo el fabricante, propone para la gestión de casos de soporte para cada uno de los bienes que conforman la propuesta. Esta información debe venir en modalidad de carta liberada por el fabricante, dirigida a la institución y haciendo referencia al número de este proceso de adquisición. |  |  |  |
|  |  | La oferta debe incluir acceso al portal de Manejo de soporte y Averías en modalidad 24x7x365 (Descargas de actualizaciones, apertura de casos en línea directo al fabricante, otros servicios de soporte). |  |  |  |
|  |  | La oferta debe incluir tres (3) años de soporte y mantenimiento en modalidad 24x7, para todos los componentes del software. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. |  |  |  |
|  | **Requerimientos Generales:** | El oferente debe considerar que con la presentación de oferta se compromete a que en caso de resultar adjudicataria la marca del software ofertado tendrá al menos 2 representantes o distribuidores locales autorizados.  Nota: Demostrable mediante carta del fabricante. |  |  |  |
|  |  | El software ofertado debe tener un ciclo de vida certificado por el fabricante con al menos 5 años de vigencia a partir de la fecha de la propuesta.  Nota: Demostrable mediante carta del fabricante. |  |  |  |
|  |  | Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados. |  |  |  |
|  |  | El Proveedor se compromete a que, una vez vencido el periodo de garantía, las actualizaciones, nuevas versiones y/o mantenimiento del/los softwares provistos en el marco de este contrato serán provistos a tarifas razonables las que no podrán exceder las tarifas predominantes que el Proveedor cobre a otros compradores en el país del Contratista por servicios similares o a los precios vigentes en la Región. |  |  |  |
|  |  | El proveedor debe entregar el software instalado, configurado, funcionando e interconectado con la infraestructura tecnológica existente en la DGCP, para lo cual debe proveer todos los medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP. |  |  |  |
|  |  | El proveedor deberá incluir el entrenamiento oficial del fabricante, para 6 técnicos designados por la DGCP, en el uso, administración, mantenimiento y soporte de los bienes ofrecidos.  NOTA: Ver detalles en pie de página de la lista de servicios conexos y cronograma de cumplimiento del lote I. |  |  |  |
|  |  | Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. |  |  |  |
|  | | | | | |
| **1.2** | **Servidor para Software de Copias de Seguridad y Recuperación de Datos** | Un (1) servidor última generación, con 24 ranuras para DIMM de memoria RAM, escalable a 3 TB y 2 sockets de CPU, sin ser esto limitativo.  En este servidor se instalará el Software Empresarial para Copias de Seguridad y Recuperación de Datos ofrecido en el ítem 1.1. |  |  |  |
| Debe ser montable en rack y ocupar no más de 2U. |  |  |
| El servidor debe ser una plataforma densa que admita 24 discos LFF sin expansiones adicionales y que permita usos multipropósito como almacenamiento definido por software, bases de datos escalables, etc. |  |  |
| El servidor debe tener al menos 256 GB de memoria RAM DDR5 que funcione a un mínimo de 5600 MT/s.  Se deben dejar slots de memoria vacíos de manera que se pueda duplicar a futuro la memoria RAM sin necesidad de cambiar los DIMMS existentes. |  |  |
| El servidor debe tener 2 CPU físicos de arquitectura x86 última generación.  Cada CPU debe tener al menos 16 núcleos de procesamiento físico, con frecuencia mínima de 2.0 Ghz o más y al menos 30MB de cache.  La cantidad de núcleos de procesamiento físico no puede ser superior a 32 por CPU. |  |  |
|  |  | El servidor ofrecido debe tener al menos 6 unidades de disco SSD de 960GB intercambiables en caliente. |  |  |  |
|  |  | El servidor ofrecido debe incluir una controladora de almacenamiento con al menos 8GB de cache.  Debe ser una controladora PCI con un mínimo de 32 puertos o líneas, compatible con RAID y HBA y permitir formar RAID 0, 1, 5, 6, 10, 50, 60, RAID 1T y RAID 10T. |  |  |  |
|  |  | El servidor debe tener al menos 4 puertos 10/25 Gbps SFP28 y 2 puertos Fiber Channel 32Gbps. Se deben proveer y configurar todas las licencias y transceivers para todos los puertos que trae el servidor. |  |  |  |
|  |  | Debe contar con al menos un puerto USB 3.0 en el panel frontal y dos puertos USB 3.0 en el panel posterior. |  |  |  |
|  |  | Mínimo 8 ranuras PCI-Express Gen 5. Todas las ranuras deben ser al menos x16. |  |  |  |
|  |  | El servidor ofrecido debe incluir al menos 2 puertos OCP con ancho de banda de PCI-E x16 Gen5. |  |  |  |
|  |  | El servidor debe tener al menos doble fuente de energía redundante, cambiables en caliente.  Cada fuente de energía debe ser de al menos 1000W y 90% de eficiencia. |  |  |  |
|  |  | Debe ser compatible con los siguientes estándares o prácticas de la industria:   * ACPI 6.4 * PCIe 5.0 * WOL * Certificaciones del logotipo de Microsoft® * PXE * USB 3.2 Gen1 * SMBIOS 3.4 * Redfish API * IPMI 2.0 * Secure Digital 4.0 * Estándar de cifrado avanzado (AES) * Estándar de triple cifrado de datos (3DES) * SNMP v3 * TLS 1.2 * Arquitectura de administración de sistemas DMTF para línea de comandos de hardware de servidor (SMASH CLP) * Arranque seguro UEFI y Secure Start * Validación FIPS 140-2 * Configuración para cumplimiento de PCI DSS * Algoritmos de seguridad nacional comercial (CNSA) * Control granular de interfaces de acceso remoto * Actualizaciones sin manipulación: componentes firmados y verificados digitalmente * Recuperación del firmware crítico a un estado correcto conocido al detectar un firmware comprometido * Capacidad para revertir firmware * Borrado seguro de NAND * Opción TPM (Módulo de plataforma segura) 2.0 * Kit de bloqueo de bisel * Detección de intrusiones en el chasis |  |  |  |
|  |  | El servidor debe ser compatible con los siguientes sistemas operativos e hipervisores:   * Windows Server 2019 y superior * Red Hat Enterprise Linux (RHEL) 8.6 y superior * SUSE Linux Enterprise Server (SLES) 15 SP4 y superior * VMware 8.0 y superior * Canonical Ubuntu 20.04 y superior |  |  |  |
|  |  | El servidor debe permitir el cifrado de datos para el almacenamiento interno mediante cifrado basado en controlador. Se deben proporcionar las licencias necesarias. |  |  |  |
|  |  | El servidor debe ser compatible con el cifrado al menos para volúmenes RAID. |  |  |  |
|  |  | Puerto de administración para gestión remota. |  |  |  |
|  |  | La gestión remota del servidor debería admitir una consola remota gráfica basada en navegador, junto con un botón de encendido virtual y arranque remoto utilizando unidades USB/CD/DVD. Debería ser capaz de ofrecer actualizaciones de software y parches desde un cliente remoto mediante medios/imagen/carpeta; también debería admitir la limitación de energía del servidor.  Debe tener la funcionalidad de KVM remoto.  Se deben incluir en la oferta todas las licencias necesarias. |  |  |  |
|  |  | El servidor ofrecido deberá contar con un motor de monitoreo, gestión y análisis habilitado para la nube para la gestión proactiva. Se deben incluir en la oferta todas las licencias necesarias para ello. |  |  |  |
|  | **Garantía:** | El oferente debe indicar el Acuerdo de Nivel de Servicio (SLA por sus siglas en inglés) y la matriz de escalación que el fabricante de su oferta, en caso de no ser el mismo el fabricante, propone para la gestión de casos de soporte para cada uno de los bienes que conforman la propuesta.  NOTA: Esta información debe venir en modalidad de carta liberada por el fabricante, dirigida a la institución y haciendo referencia al número de este proceso de adquisición. |  |  |  |
|  |  | La oferta debe incluir acceso al portal de Manejo de soporte y Averías en modalidad 24x7x365 (Descargas de drivers, apertura de casos en línea directo al fabricante, otros servicios de soporte). |  |  |  |
|  |  | La oferta debe incluir cinco (5) años de Garantía en piezas y servicios en sitio, soporte y mantenimiento en modalidad 24x7, para todos los bienes propuestos. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. |  |  |  |
|  | **Requerimientos Generales:** | El oferente debe considerar que con la presentación de oferta se compromete a que en caso de resultar adjudicataria la marca de los dispositivos ofertados tendrá al menos 2 representantes o distribuidores locales autorizados.  Nota: Demostrable mediante carta del fabricante. |  |  |  |
|  |  | Los dispositivos ofertados deben tener un ciclo de vida certificado por el fabricante con al menos 5 años de vigencia a partir de la fecha de la propuesta.  Nota: Demostrable mediante carta del fabricante. |  |  |  |
|  |  | Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados. |  |  |  |
|  |  | El Proveedor se compromete a que, una vez vencido el periodo de garantía, las actualizaciones, nuevas versiones y/o mantenimiento del/los softwares provistos en el marco de este contrato serán provistos a tarifas razonables las que no podrán exceder las tarifas predominantes que el Proveedor cobre a otros compradores en el país del Contratista por servicios similares o a los precios vigentes en la Región. |  |  |  |
|  |  | El proveedor debe entregar todo el hardware y software instalado, configurado, funcionando e interconectado con la infraestructura tecnológica y eléctrica existente en la DGCP, para lo cual debe proveer todos los dispositivos, cables, conectores, transceivers, medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP.  A continuación, se detallan las especificaciones del datacenter donde se instalará el bien:  **Switches de Red Ethernet:**   * + Puertos 1Gbps RJ45.   + Puertos 10GBps SFP+ LC MM   + Distancia para cableado: al menos 5 metros.   **Switch SAN FC**:   * + Distancia para cableado: al menos 5 metros.   **PDU**:   * + 200-240VAC conector C13 y conector C19   + Distancia para Powercord: Al menos 6 pies.   **SE INCLUYE O ADICIONA**  Nota: Es responsabilidad de la DGCP la licencia e instalación del sistema operativo. |  |  |  |
|  |  | Todos los puertos de los equipos ofertados deben estar habilitados y licenciados para poder ser utilizados. Se deben incluir los adaptadores o transceivers para todos los puertos. |  |  |  |
|  |  | El proveedor deberá realizar un traspaso de conocimiento, para 6 técnicos designados por la DGCP, en el uso, administración, mantenimiento y soporte de los bienes ofrecidos.  NOTA: Ver detalles en pie de página de la lista de servicios conexos y cronograma de cumplimiento del lote I |  |  |  |
|  |  | Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. |  |  |  |
|  | | | | | |
| **1.3** | **Biblioteca de Cintas Magnéticas** | Dos (2) bibliotecas robotizadas de cintas magnéticas, de la misma marca y modelo, montables en Rack, cada una con al menos lo siguiente:  - 4 drives (unidades de lectura/escritura) LTO-9 Fibre Channel  - 80 ranuras de almacenamiento para cartuchos de cintas  - 200 unidades de cintas LTO-9 compatibles con cifrado. Estas deben tener etiquetas personalizadas.  - 10 unidades de cintas para limpieza de drives LTO-9. Estas deben tener etiquetas personalizadas. |  |  |  |
|  |  | Cada Biblioteca ofertada debe tener capacidad de hasta 6 drives, expandible hasta al menos 42 drives. |  |  |  |
|  |  | Las Bibliotecas deben permitir, cada una, una capacidad escalable hasta al menos 25 PB, utilizando cintas de tipo LTO-9 y compresión 2.5:1. |  |  |  |
|  |  | Los drives LTO-9 ofrecidos con las Bibliotecas deben cumplir con la técnica de coincidencia de velocidad (Data Rate Matching) de datos para mayor confiabilidad. |  |  |  |
|  |  | Los drives LTO-9 ofrecidos deben permitir velocidades de 360 MB/seg o superior en modo nativo. |  |  |  |
|  |  | Las Bibliotecas de cintas deben ser escalables, cada una, hasta al menos 560 cintas y 42 unidades LTO-9 dentro de la misma Biblioteca. |  |  |  |
|  |  | Las Bibliotecas de cintas ofrecidas deben proporcionar conectividad Fibre Channel nativa de al menos 8 Gbps a los conmutadores SAN. |  |  |  |
|  |  | Debe contar con monitoreo automatizado y predictivo del estado y rendimiento de unidades de cinta y cartuchos. Debe ofrecer pruebas automáticas de unidades y cintas con diagnóstico proactivo, generando alertas ante cualquier problema. Se deben incluir las licencias necesarias. |  |  |  |
|  |  | Las Bibliotecas de cintas ofrecidas deben ser compatible con particiones para que cada unidad pueda configurarse en una partición independiente. Debe ser compatible con al menos 20 particiones. |  |  |  |
|  |  | Las Bibliotecas de cintas deben proporcionar gestión remota basada en web. |  |  |  |
|  |  | Las bibliotecas ofrecidas deberán estar provistas de un dispositivo de hardware como una llave USB, un dispositivo separado, etc. para mantener todas las claves cifradas de forma redundante. |  |  |  |
|  |  | Cada biblioteca, de las 80 ranuras, deberán admitir un lector de código de barras y al menos 5 ranuras de correos, escalables a un mínimo de 30 ranuras de correo cuando estén completamente pobladas. |  |  |  |
|  |  | Las bibliotecas de cintas deberán contar con un panel de interfaz gráfica de usuario. |  |  |  |
|  |  | Fuente de alimentación redundante. |  |  |  |
|  |  | Las bibliotecas de cintas deberán contar con software que permita predecir y prevenir fallos mediante alertas tempranas y que también sugiera las acciones de servicio necesarias. |  |  |  |
|  |  | Las bibliotecas deberán realizar la apertura automática de un ticket de servicio con el fabricante, en caso de que se presente alguna anormalidad o falla en sus componentes. Se deben incluir las licencias necesarias. |  |  |  |
|  |  | El software ofrecido también deberá determinar cuándo retirar los cartuchos de cinta y qué relación de compresión se está logrando. |  |  |  |
|  |  | Las etiquetas de las unidades de cintas LTO-9, deben tener el siguiente formato:   * 200 cintas con formato SExxxx * 200 cintas con formato DGxxxx * 20 cintas de limpieza con formato CLxxxx   Siendo xxxx un número de secuencia. Ejemplo:   * SE0001 * DG0001 * CL0001 |  |  |  |
|  | **Garantía:** | El oferente debe indicar el Acuerdo de Nivel de Servicio (SLA por sus siglas en inglés) y la matriz de escalación que el fabricante de su oferta, en caso de no ser el mismo el fabricante, propone para la gestión de casos de soporte para cada uno de los bienes que conforman la propuesta.  NOTA: Esta información debe venir en modalidad de carta liberada por el fabricante, dirigida a la institución y haciendo referencia al número de este proceso de adquisición. |  |  |  |
|  |  | La oferta debe incluir acceso al portal de Manejo de soporte y Averías en modalidad 24x7x365 (Descargas de drivers, apertura de casos en línea directo al fabricante, otros servicios de soporte). |  |  |  |
|  |  | La oferta debe incluir cinco (5) años de Garantía en piezas y servicios en sitio, soporte y mantenimiento en modalidad 24x7, para todos los bienes propuestos. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. |  |  |  |
|  | **Requerimientos Generales:** | El oferente debe considerar que con la presentación de oferta se compromete a que en caso de resultar adjudicataria la marca de los dispositivos ofertados tendrá al menos 2 representantes o distribuidores locales autorizados.  Nota: Demostrable mediante carta del fabricante. |  |  |  |
|  |  | Los dispositivos ofertados deben tener un ciclo de vida certificado por el fabricante con al menos 5 años de vigencia a partir de la fecha de la propuesta.  Nota: Demostrable mediante carta del fabricante. |  |  |  |
|  |  | Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados. |  |  |  |
|  |  | El Proveedor se compromete a que, una vez vencido el periodo de garantía, las actualizaciones, nuevas versiones y/o mantenimiento del/los softwares provistos en el marco de este contrato serán provistos a tarifas razonables las que no podrán exceder las tarifas predominantes que el Proveedor cobre a otros compradores en el país del Contratista por servicios similares o a los precios vigentes en la Región. |  |  |  |
|  |  | El proveedor debe entregar todo el hardware y software instalado, configurado, funcionando e interconectado con la infraestructura tecnológica y eléctrica existente en la DGCP, para lo cual debe proveer todos los dispositivos, cables, conectores, transceivers, medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP.  A continuación, se detallan las especificaciones del datacenter donde se instalará el bien:  **Switches de Red Ethernet:**   * + Puertos 1Gbps RJ45.   + Puertos 10GBps SFP+ LC MM   + Distancia para cableado: al menos 5 metros.   **Switch SAN FC**:  Distancia para cableado al menos 5 metros  **PDU**:   * + 200-240VAC conector C13 y conector C19   + Distancia para Powercord: Al menos 6 pies |  |  |  |
|  |  | Todos los puertos de los equipos ofertados deben estar habilitados y licenciados para poder ser utilizados. Se deben incluir los adaptadores o transceivers para todos los puertos. |  |  |  |
|  |  | El proveedor deberá configurar la integración de las bibliotecas ofertadas con el Software Empresarial para Copias de Seguridad y Recuperación de Datos ofertado en el Item 1.1, de manera que se puedan realizar duplicas a cintas magnéticas. |  |  |  |
|  |  | El proveedor deberá realizar un traspaso de conocimiento, para 6 técnicos designados por la DGCP, en el uso, administración, mantenimiento y soporte de los bienes ofrecidos.  NOTA: Ver detalles en pie de página de la lista de servicios conexos y cronograma de cumplimiento del lote I |  |  |  |
|  |  | Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. |  |  |  |
|  | | | | | |
| **1.4** | **Dispositivo Respaldo a Disco HPE StoreOnce 5260** | Un (1) dispositivo de respaldo a Disco HPE StoreOnce 5260, que tenga al menos 126 TB usables. Al menos 192 TB Raw de capacidad escalable a más de 700TB. |  |  |  |
| Debe tener discos separados dedicados al sistema operativo del dispositivo para respaldo a disco y estos no deben participar para el resguardo de datos. |  |  |  |
| Se deben configurar al menos 24TB de espacio en SSD para operaciones de almacenamiento de cache de datos. Este espacio debe ser adicional a la capacidad RAW especificada con anterioridad en este requerimiento. |  |  |  |
| El dispositivo debe venir configurado de fábrica con RAID 6 en hardware. |  |  |  |
| Debe tener al menos 2 puertos 10/25 Gbps SFP28. Se deben proveer y configurar todas las licencias y módulos SFP para todos los puertos. |  |  |  |
| Mínimo 4 puertos Fiber Channel 32Gbps. Se deben proveer y configurar todas las licencias y módulos SFP para todos los puertos. |  |  |  |
| Los puertos de fibra deberán admitir la conectividad de servidores ya sea directamente o a través de switches SAN, al tiempo que admiten la deduplicación basada en la fuente y en el destino. |  |  |  |
|  |  | Los dispositivos ofrecidos deben contar con una licencia integrada de deduplicación y una licencia de replicación de bajo ancho de banda, de modo que solo se transfieran bloques únicos no duplicados a la ubicación remota o de recuperación ante desastres (DR). |  |  |  |
|  |  | El dispositivo ofrecido deberá admitir la recepción de datos no duplicados desde ubicaciones remotas o sucursales directamente desde los servidores de aplicaciones / servidores de clientes en modo de bajo ancho de banda, sin utilizar ningún dispositivo de copia de seguridad o replicación en la ubicación remota / sucursal. |  |  |  |
|  |  | Deberá admitir la funcionalidad de cifrado. |  |  |  |
|  |  | Deberán admitir la autorización dual para prevenir operaciones disruptivas, de modo que los hackers no puedan ejecutar o completar todas las operaciones críticas, como la eliminación del almacenamiento de copia de seguridad, el cambio de la hora del sistema, etc. |  |  |  |
|  |  | La autorización dual deberá ser aprobada por dos cuentas o entidades separadas en lugar de una única cuenta o entidad responsable, para que todas las acciones maliciosas, como los ataques de ransomware, puedan prevenirse de manera efectiva. |  |  |  |
|  |  | La autorización dual deberá ser independiente del proveedor de software de copias de seguridad utilizado en el entorno. |  |  |  |
|  |  | Deben admitir la función de borrado seguro para proteger contra la recuperación no autorizada de datos eliminados. |  |  |  |
|  |  | Deben admitir el etiquetado de VLAN. Los puertos IP ofrecidos del mismo tipo también deberán admitir la agrupación de puertos (Port bonding) tanto en el equilibrio de carga adaptativo como en el modo de respaldo activo. |  |  |  |
|  | **Garantía:** | La oferta debe incluir acceso al portal de Manejo de soporte y Averías en modalidad 24x7x365 (Descargas de drivers, apertura de casos en línea directo al fabricante, otros servicios de soporte). |  |  |  |
|  |  | La oferta debe incluir cinco (5) años de Garantía en piezas y servicios en sitio, soporte y mantenimiento en modalidad 24x7, para todos los bienes propuestos. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. |  |  |  |
|  | **Requerimientos Generales:** | Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados. |  |  |  |
|  |  | El proveedor debe entregar todo el hardware y software instalado, configurado, funcionando e interconectado con la infraestructura tecnológica y eléctrica existente en la DGCP, para lo cual debe proveer todos los dispositivos, cables, conectores, transceivers, medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP.  A continuación, se detallan las especificaciones del datacenter donde se instalará el bien:  **Switches de Red Ethernet:**   * + Puertos 1Gbps RJ45.   + Puertos 10Gbps SFP+ LC MM   + Distancia para cableado: al menos 5 metros.   **Switch SAN FC**:  Distancia para cableado al menos 5 metros  **PDU**:   * + 200-240VAC conector C13.   + Distancia para Powercord: Al menos 6 pies |  |  |  |
|  |  | Se replicarán los respaldos entre el dispositivo ofertado y un StoreOnce 5260 existente, por lo que se deben proveer todas las capacidades y licencias necesarias para que se pueda realizar la replicación directa de copias de respaldo, sin necesidad de una herramienta de terceros. |  |  |  |
|  |  | El proveedor deberá configurar la replicación directa de copias de respaldo entre el dispositivo ofertado y un StoreOnce 5260 existente, sin necesidad de una herramienta de terceros. |  |  |  |
|  |  | El proveedor deberá configurar la integración del dispositivo ofertado con el sistema indicado en el Item 1.2 de manera que se realicen replicaciones de copias inmutables desde el HPE StoreOnce 5260 existente en la DGCP hasta este ofertado. |  |  |  |
|  |  | El proveedor deberá realizar un traspaso de conocimiento, para 6 técnicos designados por la DGCP, en el uso, administración, mantenimiento y soporte de los bienes ofrecidos.  NOTA: Ver detalles en pie de página de la lista de servicios conexos y cronograma de cumplimiento del lote I |  |  |  |
|  |  | Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. |  |  |  |
|  | | | | | |
| **1.5** | **Ampliación de licencias de uso de puertos para switches FC HPE SN6600B** | Una (1) ampliación para expandir las licencias y derechos de uso de puertos en cuatro (4) switches Fibre Channel HPE SN6600B, para que todos los switches queden habilitados para utilizar sus 48 puertos. |  |  |  |
|  |  | Cada switch actualmente tiene licenciado el uso de 24 puertos. Se requiere licenciar los 24 puertos adicionales de cada switch. |  |  |  |
|  |  | Se deben incluir los transceivers para los 24 puertos a licenciar de cada switch. Los transceivers deben soportar auto negociación de velocidad 32Gbps, 16Gbps y 8 Gbps. |  |  |  |
|  | **Garantía:** | La oferta debe incluir acceso al portal de Manejo de soporte y Averías en modalidad 24x7x365 (Descargas de drivers, apertura de casos en línea directo al fabricante, otros servicios de soporte). |  |  |  |
|  |  | La oferta debe incluir cinco (5) años de Garantía en piezas y servicios en sitio, soporte y mantenimiento en modalidad 24x7, para todos los bienes propuestos. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. |  |  |  |
|  |  | El proveedor deberá realizar en los switches existentes la instalación de las licencias y transceivers ofertados. |  |  |  |
|  |  | El proveedor deberá realizar un traspaso de conocimiento, para 6 técnicos designados por la DGCP, en la instalación y gestión de las licencias ofertadas.  NOTA: Ver detalles en pie de página de la lista de servicios conexos y cronograma de cumplimiento del lote I |  |  |  |
|  | | | | | |
| **1.6** | **Ampliación Blade HPE Synergy 12000** | Una (1) ampliación compuesta de:   * Cuatro (4) servidores HPE SY480 Gen11 (P39531-B21) para el Blade Synergy 12000   **NOTA: El Blade HPE Synergy 12000 a ser ampliado ya contiene 8 servidores HPE SY480 Gen11** |  |  |  |
|  |  | Cada servidor debe contener lo siguiente:   * 2 procesadores Intel Xeon Gold 5418Y 2.0GHz 24 cores (P49612-B21). En caso de no existir este modelo, se deben ofrecer 2 procesadores Intel Xeon de la misma generación del modelo solicitado, con al menos 24 núcleos de procesamiento físico y con frecuencia mínima de 2.0Ghz o más. * 1TB de memoria RAM distribuidos en 16 módulos 64GB Dual Rank x4 DDR5-4800 CAS-40-39-39 EC8 Registered Smart Memory Kit (P43331-B21). * 1 HPE Synergy 480 Gen11 without Drive Front Cage Kit (P39594-B21) * 2 HPE 480GB NVMe Gen3 Mainstream Performance Read Intensive M.2 Multi-Vendor SSD (P40513-B21) * 1 HPE Synergy NS204i-d Gen11 NVMe Boot Storage Device (P39568-B21) * 1 HPE Smart Storage Hybrid Capacitor with 260mm Cable Kit (P02381-B21) * 1 HPE Synergy 5330C 32Gb Fibre Channel Host Bus Adapter (870828-B21) * 1 HPE Synergy 4820C 10/20/25Gb Converged Network Adapter (876449-B21) * 1 HPE SR416ie-m Gen11 x16 Lanes 4GB Cache SPDM Mezzanine Storage Controller (P39959-B21) * 1 HPE Synergy 480 Gen11 CPU Front Heat Sink Kit (P39587-B21) * 1 HPE Synergy 480 Gen11 CPU Rear Heat Sink Kit (P39589-B21) |  |  |  |
|  |  | Se deben proveer todas las licencias VMware vSphere Standard para los 4 servidores Blade ofrecidos, de manera que se integre con el clúster de virtualización existente de 6 servidores.  **SE MODIFICA EN LO ADELANTE**  Las licencias ofrecidas deben ser con **soporte veinticuatro por siete (24x7) por un (1) año.**  Versión Actual instalada: 8.0.3 |  |  |  |
|  |  | El proveedor deberá realizar la instalación y configuración del VMware vSphere Standard en los 4 servidores, e integrarlos al clúster de virtualización existente. |  |  |  |
|  |  | Los servidores ofrecidos deberán contar con un motor de monitoreo y análisis habilitado para la nube para la gestión proactiva. Se deben incluir en la oferta todas las licencias necesarias para ello, con un tiempo de vigencia al menos 5 años. |  |  |  |
|  |  | El motor de monitoreo y análisis habilitado para la nube deberá tener la capacidad de proporcionar lo siguiente:   * Ofrecer recomendaciones proactivas para actualizaciones de firmware y parches. * Proporcionar el estado de la suscripción al soporte. * Recomendaciones para eliminar cuellos de botella de rendimiento y eventos críticos, basadas en la capacidad del motor de análisis de proporcionar recomendaciones proactivas para abordar problemas. * Creación automática de casos de soporte. * Detección de paquetes de actualizaciones para el servidor y notificaciones sobre cualquier hotfix disponible para la configuración específica. * Avisos al cliente basados en su relevancia para la configuración del servidor. * Deberá contar con monitoreo continuo y proactivo de la salud, registrando los parámetros del sistema necesarios y datos de telemetría diagnóstica las 24 horas, los 7 días de la semana. * Deberá tener una función de monitoreo y análisis para el servidor/chasis ofrecido junto con sus subcomponentes, con el objetivo de predecir, prevenir y resolver automáticamente problemas, y proporcionar la creación automática de casos y la presentación de archivos de registro para problemas que no puedan resolverse automáticamente. |  |  |  |
|  | **Garantía:** | La oferta debe incluir cinco (5) años de Garantía en piezas y servicios en sitio, soporte y mantenimiento en modalidad 24x7, para todos los bienes propuestos.  **SE INCLUYE O ADICIONA**  **con la excepción de las licencias de VMware vSphere Standard, las cuales deben ser por un periodo de (1) año**. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. |  |  |  |
|  | **Requerimientos Generales:** | Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados. |  |  |  |
|  |  | El proveedor debe entregar todo el hardware y software instalado, configurado, funcionando e interconectado con la infraestructura tecnológica y eléctrica existente en la DGCP, para lo cual debe proveer todos los dispositivos, cables, conectores, transceivers, medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP.  A continuación, se detallan las especificaciones del datacenter donde se instalará el bien:  **Switches de Red Ethernet:**   * + Puertos 1Gbps RJ45.   + Puertos 10GBps SFP+ LC MM   + Distancia para cableado: al menos 5 metros.   **Switch SAN FC**:   * + Distancia para cableado: al menos 5 metros.   **PDU**:   * + 200-240VAC conector C13 y conector C19.   + Distancia para Powercord: Al menos 6 pies |  |  |  |
|  |  | Todos los puertos de los servidores ofertados deben estar habilitados y licenciados para poder ser utilizados. Se deben incluir los adaptadores o transceivers para todos los puertos. |  |  |  |

| **ITEM** | **DENOMINACIÓN DEL EQUIPO:** | | **ESPECIFICACIONES TÉCNICAS REQUERIDAS** | **ESPECIFICACIONES TECNICAS DEL BIEN OFERTADO** | | **MODELO Y/O MARCA** | | **PAÍS DE ORIGEN** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lote II: Ampliación Infraestructura Ciberseguridad y Redes** | | | | | | | | |
| **2.1** | **Ampliación Seguridad Perimetral – Fortigate 601F** | | **SE MODIFICA EN LO ADELANTE**  **Dos (2) equipos Fortinet Fortigate 601F, cada uno con al menos lo siguiente:**  **- 16 interfaces GE RJ45**  **- 8 interfaces GE SFP**  **- 4 interfaces 10GE SFP+/SFP**  **- 4 interfaces 25/10GE SFP28**  **- 2 interfaces GE para gestión y HA**  **- 2 puertos USB**  **- 1 puerto consola RJ45**  **- 8 transceptores GE SFP-SR**  **- 4 transceptores 10GE SFP+-SR**  **- 4 transceptores 25/10GE SFP28-SR**  **- Forticare Premium 5 años**  **- Fortiguard UTP 5 años.** |  | |  | |  |
| Requerimientos Generales | | El equipo debe soportar hasta 139 Gbps de rendimiento para tráfico IPv4/IPv6. Latencia de 4.12 µs para paquetes de 64 bytes. Rendimiento NGFW de 11.5 Gbps y Threat Protection de 10.5 Gbps. |  | |  | |  |
| El equipo debe soportar hasta 55 Gbps de Throughput VPN (512 byte). |  | |  | |  |
| El dispositivo debe contar con capacidad de inspección SSL/TLS de hasta 9 Gbps incluyendo soporte para TLS 1.3. |  | |  | |  |
| El dispositivo debe soportar hasta 8 millones de sesiones TCP concurrentes y 550,000 nuevas sesiones por segundo. |  | |  | |  |
| El dispositivo debe contar con 16 puertos GE RJ45, 8 puertos GE SFP, 4 puertos 10GE SFP+/SFP, 4 puertos 25GE SFP28, 2 puertos GE para gestión y HA, 2 USB, 1 consola RJ45. |  | |  | |  |
| El dispositivo debe incluir x8 transceptores FN-TRAN-SX, x4 FN-TRAN-SFP+SR, x4 FN-TRAN-SFP28-SR. |  | |  | |  |
| El dispositivo debe contar con capacidad IPS con rendimiento de hasta 14 Gbps, protección contra amenazas con servicios UTP activados, control de aplicaciones, y soporte ZTNA. |  | |  | |  |
| El dispositivo debe utilizar sistema operativo FortiOS con integración en Fortinet Security Fabric. |  | |  | |  |
| El dispositivo debe contar con SPU y vSPU dedicados para descarga de funciones de seguridad. |  | |  | |  |
| El dispositivo debe contar con 2x SSD de 240 GB para logs y almacenamiento operativo. |  | |  | |  |
| El dispositivo debe incluir módulo TPM para gestión segura de claves criptográficas. |  | |  | |  |
| El dispositivo debe incluir Fuentes de alimentación duales, intercambiables en caliente. |  | |  | |  |
| El dispositivo debe soportar administración mediante FortiManager. |  | |  | |  |
| El dispositivo debe ser compatible con FortiAnalyzer para análisis avanzado de eventos. |  | |  | |  |
| El proveedor deberá realizar la implementación de los equipos siguiendo las mejores prácticas recomendadas por el fabricante y en acuerdo con los lineamientos establecidos por el equipo técnico de la DGCP. |  | |  | |  |
| El oferente debe considerar que con la presentación de oferta se compromete a que en caso de resultar adjudicataria la marca del equipo ofertado tendrá al menos 2 representantes o distribuidores locales autorizados.  Nota: Demostrable mediante carta del fabricante. |  | |  | |  |
| El equipo ofertado debe tener un ciclo de vida certificado por el fabricante con al menos 5 años de vigencia a partir de la fecha de la propuesta.  Nota: Demostrable mediante carta del fabricante. |  | |  | |  |
| Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados. |  | |  | |  |
| El proveedor debe entregar el equipo instalado, configurado, funcionando e interconectado con la infraestructura tecnológica existente en la DGCP, para lo cual debe proveer todos los medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP. |  | |  | |  |
| El oferente debe considerar que con la presentación de oferta se compromete a que en caso de resultar adjudicataria la marca del servicio ofertado tendrá al menos 2 representantes o distribuidores locales autorizados. Nota: Demostrable mediante carta del fabricante. |  | |  | |  |
| El equipo ofertado debe tener un ciclo de vida certificado por el fabricante con al menos 5 años de vigencia a partir de la fecha de la propuesta.  Nota: Demostrable mediante carta del fabricante. |  | |  | |  |
| Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados |  | |  | |  |
| El proveedor debe entregar el servicio instalado, configurado, funcionando e interconectado con la infraestructura tecnológica existente en la DGCP, para lo cual debe proveer todos los medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP. |  | |  | |  |
| Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. |  | |  | |  |
| **Entrenamiento** | | La oferta debe incluir entrenamiento (con instructor) y vouchers de certificación para 7 técnicos en los siguientes entrenamientos:FCP - Fortigate Administrator |  | |  | |  |
| **Garantía** | | La oferta deberá incluir garantía durante un periodo mínimo de cinco (5) años, el cual debe cubrir: - Asistencia técnica 24/7, - Acceso a actualizaciones y parches de firmware/seguridad, - Sustitución de hardware en caso de fallas cubiertas por la garantía, - Acceso a una base de conocimiento y centro de soporte en línea. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. |  | |  | |  |
|  | | | | | | | | |
| **2.2** | **Ampliación Seguridad Perimetral - Fortinet Fortigate 401F**  Requerimientos Generales | | **SE MODIFICA EN LO ADELANTE**  **Dos (2) equipos Fortinet Fortigate 401F, cada uno con al menos lo siguiente:**  **- 18 interfaces GE RJ45**  **- 8 interfaces GE SFP**  **- 8 interfaces 10GE SFP+/SFP**  **- 2 interfaces GE para gestión y HA**  **- 2 puertos USB**  **- 1 puerto consola RJ45**  **- 8 transceptores GE SFP-SR**  **-8 transceptores 10GE SFP+-SR**  **- Forticare Premium por 5 años**  **- Fortiguard UTP por 5 años.** | |  | |  |  |
| El equipo debe contar con una capacidad de procesamiento de firewall de al menos 79 Gbps para tráfico Ipv4, con una latencia inferior a 5 microsegundos. | |  | |  |  |
| El equipo debe soportar un rendimiento mínimo de 10Gbps en funciones de firewall con inspección avanzada (NGFW) y 9Gbps en protección contra amenaza, incluyendo IPS, control de aplicaciones, y filtrado de contenido. | |  | |  |  |
| El equipo debe contar con capacidad de inspección SSL/TLS de hasta 8 Gbps incluyendo soporte para TLS 1.3. | |  | |  |  |
| **SE MODIFICA EN LO ADELANTE**  El equipo debe soportar hasta 7.8 millones de sesiones TCP concurrentes y 500,000 nuevas sesiones por segundo. | |  | |  |  |
| El equipo debe contar con 18 puertos GE RJ45, 8 puertos GE SFP, 8 puertos 10GE SFP+/SFP, 2 puertos GE para gestión y HA, 2 USB, 1 consola RJ45. | |  | |  |  |
| El equipo debe incluir x8 transceptores FN-TRAN-SFP+SR. | |  | |  |  |
| El equipo debe contar con capacidad IPS con rendimiento de hasta 12 Gbps, protección contra amenazas con servicios UTP activados, control de aplicaciones, y soporte ZTNA. | |  | |  |  |
| El equipo debe utilizar sistema operativo FortiOS con integración en Fortinet Security Fabric. | |  | |  |  |
| El equipo debe contar con SPU y vSPU dedicados para descarga de funciones de seguridad. | |  | |  |  |
| El equipo debe contar con 2x SSD de 240 GB para logs y almacenamiento operativo. | |  | |  |  |
| El equipo debe incluir módulo TPM para gestión segura de claves criptográficas. | |  | |  |  |
| El equipo debe incluir Fuentes de alimentación duales, intercambiables en caliente. | |  | |  |  |
| El equipo debe soportar administración centralizada mediante FortiManager. | |  | |  |  |
| El equipo debe ser compatible con FortiAnalyzer para análisis avanzado de eventos. | |  | |  |  |
| El proveedor deberá realizar la implementación de los equipos siguiendo las mejores prácticas recomendadas por el fabricante y en acuerdo con los lineamientos establecidos por el equipo técnico de la DGCP. | |  | |  |  |
| El oferente debe considerar que con la presentación de oferta se compromete a que en caso de resultar adjudicataria la marca del equipo ofertado tendrá al menos 2 representantes o distribuidores locales autorizados.  Nota: Demostrable mediante carta del fabricante. | |  | |  |  |
| El equipo ofertado debe tener un ciclo de vida certificado por el fabricante con al menos 5 años de vigencia a partir de la fecha de la propuesta.  Nota: Demostrable mediante carta del fabricante. | |  | |  |  |
| Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados. | |  | |  |  |
| El proveedor debe entregar el equipo instalado, configurado, funcionando e interconectado con la infraestructura tecnológica existente en la DGCP, para lo cual debe proveer todos los medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP. | |  | |  |  |
| El oferente debe considerar que con la presentación de oferta se compromete a que en caso de resultar adjudicataria la marca del servicio ofertado tendrá al menos 2 representantes o distribuidores locales autorizados. Nota: Demostrable mediante carta del fabricante. | |  | |  |  |
| El equipo ofertado debe tener un ciclo de vida certificado por el fabricante con al menos 5 años de vigencia a partir de la fecha de la propuesta.  Nota: Demostrable mediante carta del fabricante. | |  | |  |  |
| Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados. | |  | |  |  |
| El proveedor debe entregar el servicio instalado, configurado, funcionando e interconectado con la infraestructura tecnológica existente en la DGCP, para lo cual debe proveer todos los medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP. | |  | |  |  |
| Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. | |  | |  |  |
|  | **Garantía** | | La oferta deberá incluir garantía durante un periodo mínimo de cinco (5) años, el cual debe cubrir: - Asistencia técnica 24/7, - Acceso a actualizaciones y parches de firmware/seguridad, - sustitución de hardware en caso de fallas cubiertas por la garantía, - Acceso a una base de conocimiento y centro de soporte en línea. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. | |  | |  |  |
|  | | | | | | | | |
| **2.3** | **Ampliación Infraestructura Seguridad Perimetral Servicio Gestión de Superficie de Ataque Externa (EASM) Fortinet FortiRecon**  Requerimientos Generales | | Un (1) servicio de gestión FortiRecon External Attack Surface Monitoring con vigencia de 5 años, para hasta 500 activos. Debe incluir servicio de eliminación (Takedown) con 10 créditos. | |  | |  |  |
| El servicio debe permitir la Identificación y catalogación de activos expuestos públicamente como dominios, subdominios, IPs y certificados. | |  | |  |  |
| El servicio debe permitir el análisis continuo para detectar configuraciones erróneas, vulnerabilidades conocidas y riesgos de seguridad. | |  | |  |  |
| El servicio debe permitir el Monitoreo de dominios similares, detección de phishing, vigilancia de redes sociales y tiendas de apps, y acciones de eliminación de contenido fraudulento (Protección de marca) | |  | |  |  |
| El servicio debe permitir la obtención de inteligencia desde fuentes OSINT, darknet y análisis de riesgos en la cadena de suministro. Supervisión de mercados clandestinos. | |  | |  |  |
| El servicio debe incluir 10 créditos de eliminación válidos por 3 años desde su activación, con activación dentro del primer año adquisición. | |  | |  |  |
| El servicio debe permitir generar informes periódicos con hallazgos clave, incidentes relevantes y recomendaciones estratégicas. | |  | |  |  |
| El servicio debe contar con acceso 24/7 a un portal de gestión con visualización de hallazgos, alertas y métricas en tiempo real. | |  | |  |  |
| El servicio debe permitir consultoría con analistas expertos para análisis detallados de incidentes. | |  | |  |  |
| El servicio debe soportar notificaciones inmediatas ante amenazas críticas o hallazgos sensibles. | |  | |  |  |
| El servicio debe soportar APIs abiertas, compatibilidad con SOAR y productos Fortinet como FortiGate y FortiDAST. | |  | |  |  |
| El proveedor deberá realizar la implementación del servicio siguiendo las mejores prácticas recomendadas por el fabricante y en acuerdo con los lineamientos establecidos por el equipo técnico de la DGCP. | |  | |  |  |
| Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. | |  | |  |  |
| Garantía: | | La oferta deberá incluir garantía durante un periodo mínimo de cinco (5) años, el cual debe cubrir: - Asistencia técnica 24/7, - Acceso a actualizaciones y parches de firmware/seguridad, - Sustitución de hardware en caso de fallas cubiertas por la garantiza, - Acceso a una base de conocimiento y centro de soporte en línea. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. | |  | |  |  |
|  | | | | | | | | |
| **2.4** | **Ampliación Infraestructura Monitoreo - Equipo de Análisis y Gestión de Registros – Fortinet FortiAnalyzer** | | Dos (2) equipos de análisis y gestión de registros FortiAnalyzer FAZ-300G con suscripción FortiCare Premium y FortiAnalyzer Enterprise Protection por 5 años. | |  | |  |  |
| Requerimientos Generales | | El equipo debe tener capacidad para manejar hasta 100 GB de registros por día. Análisis sostenido de hasta 2,000 logs por segundo y recolección de hasta 3,000 logs por segundo. | |  | |  |  |
| El equipo debe soportar hasta 180 dispositivos Fortinet o VDOMs para centralización de registros y análisis. | |  | |  |  |
| El equipo debe contar 8 TB de almacenamiento interno. Soporte para RAID 0/1, configurado por defecto en RAID 1. | |  | |  |  |
| El equipo debe contar con 4 puertos GE RJ45 para conectividad. | |  | |  |  |
| El equipo debe permitir la consolidación de registros desde múltiples dispositivos para visibilidad unificada de eventos de seguridad. | |  | |  |  |
| El equipo debe permitir correlación de eventos y análisis para detección de amenazas complejas. | |  | |  |  |
| El servicio debe permitir Integración con FortiGuard Labs para detección en tiempo real con IOCs actualizados. | |  | |  |  |
| El servicio debe permitir flujos de trabajo automatizados para alertas, generación de tickets, dashboards y reportes personalizables de cumplimiento. | |  | |  |  |
| El equipo debe incluir paquetes mensuales desde FortiGuard Labs con parsers, reglas de correlación, reportes, y playbooks automatizados. | |  | |  |  |
| Integración con infraestructura Fortinet y de terceros para gestión unificada de eventos de seguridad. | |  | |  |  |
| El proveedor deberá realizar la implementación de los equipos siguiendo las mejores prácticas recomendadas por el fabricante y en acuerdo con los lineamientos establecidos por el equipo técnico de la DGCP. | |  | |  |  |
| El oferente debe considerar que con la presentación de oferta se compromete a que en caso de resultar adjudicataria la marca del software ofertado tendrá al menos 2 representantes o distribuidores locales autorizados.  Nota: Demostrable mediante carta del fabricante. | |  | |  |  |
| Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados. | |  | |  |  |
| El proveedor debe entregar los equipos instalado, configurado, funcionando e interconectado con la infraestructura tecnológica existente en la DGCP, para lo cual debe proveer todos los medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP. | |  | |  |  |
| Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. | |  | |  |  |
| Entrenamientos | | La oferta debe incluir entrenamiento (con instructor) y vouchers de certificación para 7 técnicos en los siguientes entrenamientos:  FCP - FortiAnalyzer Analyst  FCP - FortiSIEM Analyst | |  | |  |  |
| Garantía | | La oferta deberá incluir garantía durante un periodo mínimo de cinco (5) años, el cual debe cubrir: - Asistencia técnica 24/7, - Acceso a actualizaciones y parches de firmware/seguridad, - Sustitución de hardware en caso de fallas cubiertas por la garantía, - Acceso a una base de conocimiento y centro de soporte en línea. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. | |  | |  |  |
| **2.5** | **Licenciamiento Token Autentication MultiFactor FortiToken** | Un (1) Licenciamiento TokenAutenticación Multifactor – Fortinet FortiToken Mobile – Paquete de 500 licencias electrónicas para autenticación multifactor (2FA) basada en software. SKU: FTM-ELIC-500. | |  | | |  |  |
| Requerimientos Generales | El licenciamiento debe incluir 500 Token de autenticación basado en aplicación móvil (software token). | |  | | |  |  |
| Debe ser compatible con fortigate, fortiauthenticator y soluciones externas que soporten tokens TOTP estándar RFC 6238. | |  | | |  |  |
| Debe permitir generación de contraseñas de un solo uso (OTP) con base en tiempo. | |  | | |  |  |
| Debe contar con almacenamiento seguro en el dispositivo móvil, resistente a ataques de clonación. | |  | | |  |  |
| Debe permitir distribución electrónica inmediata, sin requerimiento de hardware físico. | |  | | |  |  |
| Debe permitir la administración de tokens desde FortiGate o FortiAuthenticator. | |  | | |  |  |
| Garantia: | La oferta deberá incluir garantía durante un periodo mínimo de cinco (5) años, el cual debe cubrir: - Asistencia técnica 24/7, - Acceso a actualizaciones y parches de firmware/seguridad, - Sustitución de hardware en caso de fallas cubiertas por la garantía, - Acceso a una base de conocimiento y centro de soporte en línea. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. | |  | | |  |  |
|  | | | | | | | | |
| **2.6** | **Renovación Licenciamiento FortiEDR** | **SE MODIFICA EN LO ADELANTE**  Una (1) renovación del licenciamiento debe incluir 500 endpoints. | |  | | |  |  |
| Requerimientos Generales: | Protección avanzada de endpoints (EDR) con capacidades de detección y respuesta ante amenazas en tiempo real. | |  | | |  |  |
| El licenciamiento debe incluir 500 servidores, 500 workstations, 500 dispositivos IoT. | |  | | |  |  |
| El servicio debe incluir prevención de exploits, análisis de comportamiento, respuesta automatizada (MDR), protección de memoria y remediación forense. | |  | | |  |  |
| El servicio debe contar con capacidades de Threat hunting. | |  | | |  |  |
| El servicio debe ser compatible con Windows, Linux y dispositivos IoT que cumplan los requisitos mínimos del agente FortiEDR. | |  | | |  |  |
| El servicio debe contar con integración nativa con FortiGate, FortiAnalyzer y FortiSIEM para una protección coordinada en toda la red. | |  | | |  |  |
| El servicio debe permitir el despliegue de agente vía scripts, herramientas de gestión de endpoints t o GPO. | |  | | |  |  |
|  |  | **SE INCLUYE O ADICIONA**  **El oferente debe contar con acreditación MSSP.** | |  | | |  |  |
|  | Entrenamientos | La oferta debe incluir entrenamiento(instructor-led) y vouchers de certificación para 3 personas en los siguientes entrenamientos:  FCP - FortiEDR | |  | | |  |  |
|  | Garantía | La oferta deberá incluir garantía durante un periodo mínimo de cinco (5) años, el cual debe cubrir: - Asistencia técnica 24/7, - Acceso a actualizaciones y parches de firmware/seguridad, - Sustitución de hardware en caso de fallas cubiertas por la garantía, - Acceso a una base de conocimiento y centro de soporte en línea. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. | |  | | |  |  |
|  | | | | | | | | |
| **2.7** | **Puntos de Acceso Inalámbrico Fortinet FortiAP** | Veintitrés (23) Puntos de Acceso FortiAP FAP-431F-A con suscripción FortiCare Premium por 5 años. SKU: FAP-431F-A, FC-10-F431F-247-02-60. | |  | |  | |  |
| Requerimientos Generales | Debe Soportar el estándar IEEE 802.11ax (Wi-Fi 6) para mayor eficiencia y capacidad en entornos de alta densidad. | |  | | |  |  |
| Deben contar con tres radios: 2.4 GHz, 5 GHz y otro radio dedicado para escaneo o servicio adicional. Soporte 4x4 MU-MIMO en ambas bandas. | |  | | |  |  |
| Debe tener capacidad de hasta 1,147 Mbps en 2.4 GHz y hasta 2,402 Mbps en 5 GHz. | |  | | |  |  |
| Debe contar con Un puerto Ethernet de 2.5 Gbps con PoE y un puerto Ethernet adicional de 1 Gbps. | |  | | |  |  |
| Debe soportar integración con Fortinet Security Fabric, autenticación 802.1X y control de acceso basado en ACLs. | |  | | |  |  |
| Debe permitir la Administración autónoma o mediante FortiGate como controlador. | |  | | |  |  |
| Debe soportar monitoreo en tiempo real del rendimiento y estado de la red. | |  | | |  |  |
| Debe contar con radio BLE para aplicaciones de proximidad, escaneo de espectro para detección de interferencias y amenazas. | |  | | |  |  |
| Debe ser compatible con IEEE 802.3at (PoE+). Consumo máximo de 25.5 W. | |  | | |  |  |
| Debe permitir montaje en techo o pared. | |  | | |  |  |
| Debe permitir la operación en temperatura estándar de interiores y niveles normales de humedad sin condensación. | |  | | |  |  |
| Debe ser compatible con dispositivos 802.11a/b/g/n/ac y con infraestructura de red multivendedor. | |  | | |  |  |
| Garantía | La oferta deberá incluir garantía durante un periodo mínimo de cinco (5) años, el cual debe cubrir: - Asistencia técnica 24/7, - Acceso a actualizaciones y parches de firmware/seguridad, - Sustitución de hardware en caso de fallas cubiertas por la garantía, - Acceso a una base de Conocimiento y centro de soporte en línea. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. | |  | | |  |  |
| **2.8** | **Switch Core de Alto Rendimiento** | **SE MODIFICA EN LO ADELANTE**  Cuatro (4) Switch, montables en Rack, cada uno con al menos lo siguiente:  - 48 interfaces 10/25GE SFP28  - 8 interfaces 100GE QSFP28  - 2 interfaces 10GE SFP+  - 48 transceptores SFP28-SR (10/25GE)  - 8 transceptores QSFP28-SR (100GE)  - 48 cables de fibra multimodo OM4, conectores LC-LC  - 8 cables de fibra multimodo OM4 con conectores MPO-12 a MPO-12 | |  | | |  |  |
| Requerimientos Generales | El fabricante del sistema debe estar incluido como líder en la versión más reciente del cuadrante mágico de Gartner para Infraestructura LAN Empresarial por Cable e Inalámbrica. | |  | | |  |  |
| Debe contar con una capacidad de conmutación de hasta 880 Gbps en modo dúplex. | |  | | |  |  |
| Debe contar con una tasa de reenvío de hasta 1,309 millones de paquetes por segundo (Mpps) | |  | | |  |  |
| Debe presentar una latencia inferior a 1 microsegundo (<1 µs). | |  | | |  |  |
| **SE MODIFICA EN LO ADELANTE**  Debe soportar funcionalidades de capa 2 y capa 3, tales como VLANs, agregación de enlaces (MCLAG), STP, enrutamiento dinamico, PBR, etc. | |  | | |  |  |
| Debe permitir la integración con soluciones de red mediante autenticación 802.1X, listas de control de acceso (ACLs) y otras medidas de control de acceso. | |  | | |  |  |
| Debe contar con fuentes de alimentación redundantes e intercambiables en caliente (hot-swappable), y un consumo máximo de 1,660 W. | |  | |  | |  |
| Debe contar con un sistema de ventilación con flujo de aire frontal a posterior. | |  | | |  |  |
| Debe estar diseñado para montaje en rack de 1U, con dimensiones aproximadas de 44 x 440 x 410 mm y un peso de 7.5 kg (16.53 lbs). | |  | | |  |  |
| Debe operar en un rango de temperatura de 0°C a 45°C y soportar una humedad relativa de 10% a 95% sin condensación. | |  | | |  |  |
| Debe ser compatible con transceptores SFP28 y QSFP28 estándar del mercado, y permitir la integración con dispositivos de red de múltiples fabricantes. | |  | | |  |  |
| Debe incluir todos los transceptores requeridos. | |  | | |  |  |
| El proveedor deberá realizar la implementación de los equipos siguiendo las mejores prácticas recomendadas por el fabricante y en acuerdo con los lineamientos establecidos por el equipo técnico de la DGCP. | |  | | |  |  |
| El oferente debe considerar que con la presentación de oferta se compromete a que en caso de resultar adjudicataria la marca del equipo ofertado tendrá al menos 2 representantes o distribuidores locales autorizados.  Nota: Demostrable mediante carta del fabricante. | |  | | |  |  |
| El proveedor debe entregar los equipos instalados, configurados, funcionando e interconectados con la infraestructura tecnológica existente en la DGCP, para lo cual debe proveer todos los medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP. | |  | | |  |  |
| Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados. | |  | | |  |  |
| Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. | |  | | |  |  |
| Garantía: | La oferta deberá incluir garantía durante un periodo mínimo de cinco (5) años, el cual debe cubrir: - Asistencia técnica 24/7, - Acceso a actualizaciones y parches de firmware/seguridad, - Sustitución de hardware en caso de fallas cubiertas por la garantía, - Acceso a una base de conocimiento y centro de soporte en línea. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. | |  | | |  |  |
|  | | | | | | | | |
| **2.9** | **Switch de Acceso de alto rendimiento.** | **SE MODIFICA EN LO ADELANTE**  Veintitrés (23) Switch de acceso alto rendimiento, para distribución de red, montables en Rack, cada uno con al menos lo siguiente:  - 48 interfaces GE RJ45 (POE/POE+)  - 4 interfaces 10GE SFP+  - 4 transceptores SFP+ 10GE  - 4 cables de fibra multimodo OM4, conectores LC-LC  - Soporte y Mantenimiento por 5 años. | |  | |  | |  |
| Requerimientos Generales | El equipo debe soportar al menos 176Gbps en capacidad de conmutación. | |  | | |  |  |
| El equipo debe de contar con 48 puertos de red Ethernet 10/100/1000 Mbps (compatibles con PoE/PoE+ - IEEE 802.3af/at). Y 4 puertos SFP+ de 10 Gbps para enlaces ascendentes. | |  | | |  |  |
| EL equipo debe soportar una capacidad total de hasta 740W para dispositivos alimentados. | |  | | |  |  |
| El equipo debe contar con soporte para VLANs, agregación de enlaces (LAG), STP y otras funcionalidades de conmutación. | |  | | |  |  |
| El equipo debe contar con soporte para enrutamiento estático y dinámico. | |  | | |  |  |
| El equipo debe contar con soporte para operación autónomo o gestionado mediante un controlador externo. | |  | | |  |  |
| Debe contar con interfaces de administración: CLI, interfaz web y SNMP. | |  | |  | |  |
| El equipo debe soportar integración con herramientas de monitoreo en tiempo real, diagnóstico de red y recopilación de estadísticas. | |  | | |  |  |
| El equipo debe contar con soporte para autenticación 802.1X. | |  | | |  |  |
| El equipo debe contar con capacidad de Listas de control de acceso (ACLs). | |  | | |  |  |
| El equipo debe contar con fuentes de alimentación internas con soporte para POE. | |  | | |  |  |
| El equipo debe contar con sistema de ventilación lateral a posterior para eficiencia térmica. | |  | | |  |  |
| El equipo debe incluir x4 tranceptores FN-TRAN-SFP+SR. | |  | | |  |  |
| El proveedor deberá realizar la implementación del servicio siguiendo las mejores prácticas recomendadas por el fabricante y en acuerdo con los lineamientos establecidos por el equipo técnico de la DGCP. | |  | | |  |  |
| Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. | |  | | |  |  |
| **Garantía** | La oferta deberá incluir garantía durante un periodo mínimo de cinco (5) años, el cual debe cubrir: - Asistencia técnica 24/7, - Acceso a actualizaciones y parches de firmware/seguridad, - Sustitución de hardware en caso de fallas cubiertas por la garantía, - Acceso a una base de conocimiento y centro de soporte en línea. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. | |  | | |  |  |
| **2.10** | **Equipo Gestión Centralizada Fortinet FortiManager** | **SE MODIFICA EN LO ADELANTE**  Dos (2) equipos Fortinet FortiManager 410G, cada uno con al menos lo siguiente:  - 4 interfaces GE RJ45  - 2 interfaces GE SFP  - 2 transceptores SFP  - 2 cables de fibra multimodo OM4, conectores LC-LC  - Forticare Premium 5 años | |  | | |  |  |
| **Requerimientos Generales** | El equipo debe soportar hasta 150 dispositivos o instancias virtuales (VDOMS). | |  | | |  |  |
| El equipo debe soportar un mínimo sostenido de hasta 50 registros por segundo. | |  | | |  |  |
| El equipo debe soportar hasta 2Gb de eventos por día. | |  | | |  |  |
| El equipo debe contar con un almacenamiento interno mínimo de 32TB (8 discos 4TB). Almacenamiento utilizable de al menos 24 TB. | |  | | |  |  |
| El equipo debe soportar múltiples niveles RAID: 0/1/5/6/10/50/60. | |  | | |  |  |
| El equipo debe contar con fuente de alimentación redundante. | |  | | |  |  |
| El equipo debe contar con modulo TPM para almacenamiento seguro de claves criptográficas. | |  | | |  |  |
| El equipo debe contar con las siguientes interfaces de red: 4 puertos GE RJ45, 2 Puertos GE SFP, 1 Puerto consola RJ45 | |  | |  | |  |
| El equipo debe incluir x8 transceptores FN-TRAN-SFP+SR. | |  | | |  |  |
| El equipo debe operar como concentrador de gestión centralizada para políticas, configuraciones y despliegue masivo de actualizaciones. | |  | | |  |  |
| El equipo debe ofrecer integración nativa con FortiAnalyzer y FortiSIEM. | |  | | |  |  |
| El proveedor deberá realizar la implementación del servicio siguiendo las mejores prácticas recomendadas por el fabricante y en acuerdo con los lineamientos establecidos por el equipo técnico de la DGCP. | |  | | |  |  |
| Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. | |  | | |  |  |
| **Garantía:** | La oferta deberá incluir garantía durante un periodo mínimo de cinco (5) años, el cual debe cubrir: - Asistencia técnica 24/7, - Acceso a actualizaciones y parches de firmware/seguridad, - sustitución de hardware en caso de fallas cubiertas por la garantía, - Acceso a una base de conocimiento y centro de soporte en línea. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. | |  | | |  |  |

| **ITEM** | **DENOMINACIÓN DEL EQUIPO:** | **ESPECIFICACIONES TÉCNICAS REQUERIDAS** | **ESPECIFICACIONES TECNICAS DEL BIEN OFERTADO** | **MODELO Y/O MARCA** | **PAÍS DE ORIGEN** |
| --- | --- | --- | --- | --- | --- |
| **Lote III: Servicio Protección Correo Electrónico y Concienciación** | | | | | |
| **3.1** | **Requerimientos Generales**  Requerimientos Generales | **SE MODIFICA EN LO ADELANTE**  Un (1) Servicio de Protección Correo Electrónico y Concienciación para **400 buzones.** |  |  |  |
| El fabricante del sistema debe estar incluido como líder en la versión más reciente del cuadrante mágico de Gartner para Plataformas de Seguridad de Correo Electrónico. |  |  |  |
| El servicio debe estar basadop en modalidad SaaS (Software como Servicio). |  |  |  |
| Debe incluir licenciamiento por un período mínimo de tres (3) años. |  |  |  |
| Debe contar con mecanismos de detección y bloqueo de amenazas usando técnicas de inteligencia artificial (IA) y aprendizaje automático (ML). |  |  |  |
| **SE INCLUYE O ADICIONA**  **Debe ser compatible con entorno hibrido Exchange /MS365.** |  |  |  |
| Debe ofrecer protección contra: Phishing,Compromiso de correo electrónico empresarial (BEC), Ransomware y amenazas avanzadas. |  |  |  |
| Debe incluir capacidad de: - Reescritura de URLs y análisis en tiempo de clic, Análisis de archivos adjuntos con sandboxing. |  |  |  |
| Debe contar con paneles de control que proporcionen visibilidad sobre usuarios más atacados y tácticas utilizadas. |  |  |  |
| Debe permitir la automatización de respuestas a incidentes, incluyendo la remoción automática de correos maliciosos de las bandejas de entrada. |  |  |  |
| **SE MODIFICA EN LO ADELANTE**  Debe incluir capacidad en Concienciación sobre Seguridad (Security Awareness) para 400 usuarios. |  |  |  |
| El módulo de Concienciación sobre Seguridad debe incluir simulaciones periódicas de phishing configurables, módulos de capacitación interactivos, herramientas de evaluación del conocimiento del personal, reportes de progreso y efectividad del programa de concienciación. |  |  |  |
| El contenido del módulo de Concienciación sobre Seguridad debe estar disponible en múltiples idiomas, incluyendo español. |  |  |  |
| Debe contar con una consola centralizada de administración para la gestión unificada de políticas, usuarios, eventos y capacitación. |  |  |  |
| Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. |  |  |  |
| El proveedor deberá realizar la implementación del servicio siguiendo las mejores prácticas recomendadas por el fabricante y en acuerdo con los lineamientos establecidos por el equipo técnico de la DGCP. |  |  |  |
| El oferente debe considerar que con la presentación de oferta se compromete a que en caso de resultar adjudicataria la marca del servicio ofertado tendrá al menos 2 representantes o distribuidores locales autorizados.  Nota: Demostrable mediante carta del fabricante. |  |  |  |
| Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados. |  |  |  |
| El proveedor debe entregar el servicio instalado, configurado, funcionando e interconectado con la infraestructura tecnológica existente en la DGCP, para lo cual debe proveer todos los medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP. |  |  |  |
| Garantía | **SE MODIFICA EN LO ADELANTE**  La oferta deberá incluir garantía durante un periodo mínimo de cinco (3) años, el cual debe cubrir: - Asistencia técnica 24/7, - Acceso a actualizaciones y parches de firmware/seguridad, - Sustitución de hardware en caso de fallas cubiertas por la garantía, - Acceso a una base de conocimiento y centro de soporte en línea. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. |  |  |  |

| **ITEM** | **DENOMINACIÓN DEL EQUIPO:** | **ESPECIFICACIONES TÉCNICAS REQUERIDAS** | **ESPECIFICACIONES TECNICAS DEL BIEN OFERTADO** | **MODELO Y/O MARCA** | **PAÍS DE ORIGEN** |
| --- | --- | --- | --- | --- | --- |
| **Lote IV: Servidor Hiperconvergente** | | | | | |
| **4.1** | **Servidor hiperconvergente** | Un (1) Servidor hiperconvergente compuesto por tres (3) nodos integrados en un solo chasis con soporte y mantenimiento por 5 años. |  |  |  |
| **Requerimientos Generales** | El servidor debe contar con 3 nodos en chassis de 2U. |  |  |  |
| Cada nodo debe contar con 2 procesadores de 8 núcleos físicos, con frecuencia base mínima de 2.9 Ghz (total de 16 núcleos por nodo / 48 núcleos físicos en total). |  |  |  |
| Cada nodo debe contar con al menos 768 GB de memoria RAM (12 módulos de 64 GB) para un total de 2.3TB. |  |  |  |
| Cada nodo debe incluir al menos: 1 unidad SSD de 3.84TB y 2 unidades HDD de 12TB. |  |  |  |
| **SE MODIFICA EN LO ADELANTE**  Cada nodo debe contar con al menos 2 interfaces SFP28 de 25/10 Gbps y los transceptores SFP28-SR correspondientes para cada interfaz. |  |  |  |
| **SE MODIFICA EN LO ADELANTE**  El servidor debe incluir servicio de Soporte 24/7 durante un periodo mínimo de 5 años. |  |  |  |
| **SE MODIFICA EN LO ADELANTE**  El servidor debera utilizar el hipervisor Acropolis AHV como plataforma de virtualizacion. |  |  |  |
| El soporte del servidor debe cubrir: atención con SLA de 4 horas para reemplazo de partes y respuesta tecnica, acceso a actualizaciones de software y firmware durante la vigencia del soporte. |  |  |  |
| Al finalizar la instalación, configuración e interconexión, el proveedor deberá entregar la documentación de todo el trabajo realizado, detallando licenciamientos, inventario, configuraciones, diseños, diagramas de interconexión, explicativo del producto ofrecido, el modo de licenciamiento, las fechas de vencimiento, el costo estimado y formas de renovación para períodos de un año, sin ser estos limitativos. |  |  |  |
| El proveedor deberá realizar la implementación del servicio siguiendo las mejores prácticas recomendadas por el fabricante y en acuerdo con los lineamientos establecidos por el equipo técnico de la DGCP. |  |  |  |
| El oferente debe considerar que con la presentación de oferta se compromete a que en caso de resultar adjudicataria la marca del servicio ofertado tendrá al menos 2 representantes o distribuidores locales autorizados.  Nota: Demostrable mediante carta del fabricante. |  |  |  |
| Durante la vigencia de la garantía se deben proveer e instalar, sin costo alguno, las actualizaciones de software, firmware y manuales respectivos que sean publicados. |  |  |  |
| El proveedor debe entregar el servicio instalado, configurado, funcionando e interconectado con la infraestructura tecnológica existente en la DGCP, para lo cual debe proveer todos los medios de instalación, programas, licencias y cualquier otro elemento necesario. Este proceso debe realizarse con la participación de los técnicos designados por la DGCP. |  |  |  |
| **Garantía** | La oferta deberá incluir garantía durante un periodo mínimo de cinco (5) años, el cual debe cubrir: - Asistencia técnica 24/7, - Acceso a actualizaciones y parches de firmware/seguridad, - sustitución de hardware en caso de fallas cubiertas por la garantía, - Acceso a una base de conocimiento y centro de soporte en línea. La garantía debe iniciar a partir de la aceptación conforme, por parte de la DGCP, de la entrega e implementación de los bienes y servicios ofertados acorde a los Requerimientos Técnicos. |  |  |  |

| **ITEM** | **DENOMINACIÓN DEL EQUIPO:** | **ESPECIFICACIONES TÉCNICAS REQUERIDAS** | **ESPECIFICACIONES TECNICAS DEL BIEN OFERTADO** | **MODELO Y/O MARCA** | **PAÍS DE ORIGEN** |
| --- | --- | --- | --- | --- | --- |
| **Lote V:** **Capacitaciones y Certificaciones** | | | | | |
| **5.1** | **Capacitación VMware** | Un (1) Entrenamiento Oficial del fabricante para 8 técnicos designados por la DGCP en el curso VMware vSphere: Advanced Administration [V8]  El curso debe ser en español y provisto en modalidad virtual.  El proveedor debe realizar todos los arreglos logísticos para la realización del entrenamiento requerido por la institución: material de apoyo (manuales, guías) e instructores con el conocimiento que sea requerido. |  |  |  |
| **5.2** | **Voucher Certificación VMware** | Cinco (5) vouchers para Certificación Vmware Certified Professional Data Center Virtualization. |  |  |  |
| Los vouchers serán utilizados por 5 técnicos designados de la DGCP, los cuales ya han recibido las capacitaciones necesarias para optar por la certificación. |  |  |  |
| Los vouchers deben tener una duración de 1 año a partir de la fecha de entrega. |  |  |  |