

### *MISIÓN: “Diseñar y Establecer Políticas Públicas, Programas e Instrumentos que apuntalen el desarrollo de la industria y aumente su participación en el Producto Interno Bruto, logre la facilitación del comercio legal, y permita la formalización de las MiPYMES…”*

**REPÚBLICA DEL PARAGUAY**

**PLIEGO DE BASES Y CONDICIONES**

**LICITACION PUBLICA NACIONAL Nº 03/2019**

**SUBASTA A LA BAJA ELECTRONICA**

**“ADECUACION DEL DATA CENTER DE LA DIRECCION GENERAL DE FIRMA DIGITAL Y COMERCIO ELECTRONICO”**

**ID XXX.XXX**



### VISIÓN: “Transformar al Ministerio de Industria y Comercio en la institución pública líder en tecnología y competitividad, que se constituya en el portal de acceso al país de las inversiones serias - locales y extranjeras...”

###### MIC - Sede Central; Av. Mcal. López 3333 c/ Dr. Weiss, Villa Morra Teléfono:+595 21 616 3185

**INDICE DE CONTENIDO**

**Sección I. DATOS DE LA SUBASTA (DDS)**

Esta sección contiene disposiciones específicas que complementan las Instrucciones a los Oferentes y Generalidades de la Subasta a la Baja Electrónica (IAO.SBE).

**Sección II. CRITERIOS DE EVALUACIÓN Y CALIFICACIÓN**

Esta sección detalla los criterios que se utilizarán para establecer la oferta evaluada como la más baja y las calificaciones que deberá poseer el Oferente para ejecutar el contrato.

**Sección III. SUMINISTROS REQUERIDOS**

Esta sección incluye el Plan de Entregas, las Especificaciones Técnicas y los Planos concernientes a los Bienes a ser adquiridos o Servicios a ser prestados.

###### Sección IV. CONDICIONES ESPECIALES DEL CONTRATO (CEC)

Esta sección incluye cláusulas específicas que son propias para cada contrato y que complementan las Condiciones Generales del Contrato de la SBE (CGC).

**Sección V. MODELO DE CONTRATO**

Esta sección incluye la pro-forma del Contrato que deberá ser perfeccionado entre la Contratante y el Oferente adjudicado.

###### Sección VI. FORMULARIOS

Esta sección contiene los Formularios de la Licitación que el Oferente deberá presentar con la oferta y además las que son requeridas para la firma del Contrato.

###### Sección VII. ANEXOS

Esta sección contiene la Lista de Documentos de carácter formal y sustancial a ser presentados por el oferente junto con su oferta, así como las requeridas para la firma del contrato, una vez notificada la adjudicación.

**SECCION I.**

**DATOS DE LA SUBASTA**

**Los Datos de la Licitación serán consignados en esta sección y en el SICP, los mismos forman parte de los Documentos de la presente Licitación.**

|  |  |  |
| --- | --- | --- |
| IAO 6 | Idioma de los documentos de la Oferta | La Convocante aceptará catálogos en idioma diferente al castellano: **Si.** **En idioma Ingles.**  En forma solo enunciativa y no limitativa, se podrán presentar los siguientes documentos en el idioma ingles los siguiente documentos:  a) Catálogos emitidos por el fabricante de los bienes que demuestren que los bienes ofertados cumplen con las especificaciones técnicas. |
| IAO 10.2 | Abastecimiento Simultaneo | No aplica. |
| IAO 19 (f) | Validez de la Oferta | 60 (sesenta) días contados a partir de la fecha y hora de apertura de la etapa competitiva. |
| IAO 19.(g) | Validez de la Garantía de Mantenimiento de Ofertas | 90 (noventa) días contados a partir de la fecha y hora de apertura de la etapa competitiva, debiendo ajustarse a lo establecido en la legislación vigente. |
| IAO 23.2 | Presentación de los documentos de la oferta | Una vez finalizada la Subasta a la Baja Electrónica y levantada el acta de sesión pública virtual en el portal, **TODOS LOS OFERENTES** deberán presentar sus respectivas documentaciones en **un 1 (un) ORIGINAL** en sobre cerrado con indicación del nombre del Oferente participante, a fin de realizar las evaluaciones pertinentes. El sobre deberá estar dirigido a la institución Convocante y/o Dirección de Contrataciones.  ***Observaciones:***   1. Los representantes de los oferentes que participen del acto de apertura de ofertas y que deseen hacer constar Observaciones en el Acta de Apertura de las ofertas deberán contar con autorización suficiente, bastando para ello la presentación de una autorización escrita del Representante Legal de la firma.      1. En caso de que existan oferentes que participen de la Subasta a la Baja Electrónica y que no presenten su oferta física en el plazo establecido se procederá conforme a lo establecido en el Art. 37 del Decreto 1107/14 y serán pasibles de las sanciones previstas en el Art. 72 de la Ley 2051/03 de acuerdo con el procedimiento establecido en el Art. 74 de la misma Ley. 2. Todas las páginas de la oferta deberán estar foliadas y firmadas por la persona debidamente autorizada para firmar en nombre del oferente. 3. En el llenado del formulario de lista de precios de la oferta física, cuando el resultado de la división del precio total del Grupo – ítem, que figura en el acta virtual de la subasta, con la cantidad del servicio solicitado en cada ítem arrojase una cifra con decimales, el oferente para la consignación de su precio, deberá realizar el redondeo del mismo hacia abajo sin que el nuevo resultado del precio total donde se realizó la operación supere al que figura en el Acta Virtual de la SBE como precio final. Será descalificada la oferta física cuyo monto total supere el último lance que figura en el Acta de Sesión Pública Virtual. 4. En caso de discrepancia entre los datos consignados en el Acta de sesión pública virtual y los presentados con la oferta física, se procederá a la descalificación de la oferta exceptuando la variación de los precios por efectos del redondeo hacia abajo. |
| IAO 27.3 | Notificación de la Adjudicación | La adjudicación quedará formalizada con la notificación escrita al adjudicatario y a los demás oferentes, dentro del plazo de cinco (5) días calendario siguiente a su emisión. Asimismo, deberá ser difundido en el Sistema de Información de Contrataciones Públicas (SICP). Las Notificaciones de Adjudicación serán remitidas vía Fax o Correo Electrónico. La Convocante respaldará la comunicación de las notificaciones Vía Correo Electrónico (email) con reporte de transmisión del correo electrónico de la Dirección de Contrataciones del MIC a la dirección de correo electrónico establecida por los oferentes en su oferta. Los oferentes serán totalmente responsables de la revisión de sus Teléfonos Fax y de los correos electrónicos asignados en la oferta. Este procedimiento sustituye a la notificación personal.  El oferente podrá solicitar una copia del Informe de Evaluación de ofertas a su costa de conformidad a lo establecido en el Art. 65 del Decreto 21.909/03. Dicha solicitud deberá realizarse por Nota e ingresarse por Mesa de Entrada de la Dirección de Contrataciones del MIC sito en Avda. Mcal Lopez Nª 3333 entre Salaskin y Dr. Weiss .La Dirección de Contrataciones informará por nota la disponibilidad de la copia del informe de evaluación de ofertas para su retiro. Dicha comunicación será remitida por las vías establecidas en este punto. |

**SECCION II**

**CRITERIOS DE EVALUACIÓN Y REQUISITOS DE CALIFICACIÓN**

Esta Sección complementa las Instrucciones a los Oferentes y Generalidades (IAO.SBE) y contiene los criterios que la Convocante utilizará para evaluar la oferta y determinar si el Oferente cuenta con las calificaciones requeridas de conformidad a las disposiciones de la Ley 2051/03; a la Sección VI del Decreto 21909/03; al Decreto 1107/14 y las reglamentaciones que la DNCP emitan al respecto.

**Criterios de Evaluación**

* + - * + Se verificará primeramente la presentación de los documentos de carácter sustancial:
* Formulario de Oferta y Lista de precios, generados electrónicamente a través del SICP, debidamente completado y firmado. Se descalificará la oferta que no cotice todos los ítems en la lista de precios.
* Garantía de Mantenimiento de Oferta debidamente extendida
* Documentos que acrediten la identidad del oferente y representación suficiente del firmante de la oferta.
  + - * + Una vez verificada la documentación y analizada la pertinencia de cada uno de los documentos sustanciales mencionados, en caso de que alguno de los oferentes omita la presentación de los mismos o la presente en forma irregular las ofertas serán descalificadas.
        + Se seleccionará provisoriamente al oferente o postor ganador del proceso de competencia de subasta determinado en el Acta de Sesión Pública Virtual, cuyas documentaciones serán analizadas en detalle para verificar el cumplimiento de los requisitos de calificación.
        + En caso de que la oferta más baja no cumpla con ellos se la desechará y se analizará la segunda oferta más baja y así hasta llegar a la oferta más solvente que cumpla con todos los requisitos y condiciones y se la propondrá para la adjudicación.
        + Posteriormente se verificará que se haya proveído la documentación que avale el cumplimiento de los criterios técnicos, legales y financieros conforme a los requisitos de calificación.
        + La Convocante a través de su Comité de Evaluación se reserva el derecho de solicitar los documentos formales que sean necesarios y de solicitar aclaraciones a los oferentes. La solicitud se realizará Vía Correo Electrónico (email). El reporte de transmisión del correo electrónico será considerado como prueba de recibido. Los oferentes serán totalmente responsables de la revisión de los correos electrónicos asignados en la oferta. Este procedimiento sustituye a la notificación personal.
        + El análisis de las ofertas se basará únicamente en la evidencia documentada requerida por el presente pliego de condiciones.
        + A fin de verificar el cumplimiento se utilizará el criterio “cumple” o “no cumple”.

**A) CALIFICACIÓN LEGAL**

El Comité de Evaluación confirmará que el oferente no se encuentra comprendido en las prohibiciones establecidas en el Art. 40, incisos a) y b) de la Ley 2051/03 en base al siguiente análisis:

En primer lugar, verificará que el oferente haya proporcionado en forma satisfactoria la Declaración Jurada de no hallarse comprendido en las prohibiciones y limitaciones establecidas en el Artículo 40 de la Ley N° 2051/03 que se incluye como parte del formulario de oferta.

**Inciso a)**

Verificará los registros del personal de la convocante para detectar si el oferente o sus representantes, se hallan comprendidos en el presupuesto del inciso “a” del Artículo 40.

**Inciso b)**

Verificará por los medios disponibles, si el Oferente y los demás sujetos individualizados en las prohibiciones contenidas en la Ley N° 1626/00 "De la Función Pública", aparecen en la base de datos del SINARH o bien de la Secretaría de la Función Pública.

Si se constata que alguna de las personas mencionadas en el párrafo anterior figura en la base de datos del SINARH, el Comité analizará acabadamente si tal situación le impedirá ejecutar el contrato de que se trate, exponiendo los motivos para aceptar o rechazar la oferta, según sea el caso.

El Comité podrá recurrir a fuentes públicas o privadas de información, para verificar los datos proporcionados por el Oferente.

Si el Comité confirma que el Oferente o sus integrantes, poseen impedimentos la oferta será rechazada, y se remitirán los antecedentes a la Dirección Nacional de Contrataciones Públicas (DNCP) para los fines pertinentes.

**B) ANÁLISIS DE LOS PRECIOS OFERTADOS**

Durante Ia evaluación de ofertas, luego de haber realizado la corrección de errores aritméticos y ordenar las ofertas de menor a mayor, conforme los precios ofertados, el Comité de Evaluación procederá a solicitar a los oferentes una explicación detallada de la composición del precio ofertado, conforme a la reglamentación dispuesta por la DNCP.

**C) MARGEN DE PREFERENCIA NACIONAL PARA PRODUCTOS NACIONALES**

Se aplicará el margen de preferencia nacional de conformidad a la legislación vigente. La acreditación de Origen Nacional del Producto, en el marco del proceso de contratación, será a través del Certificado de Origen Nacional, expedido por Autoridad competente. A fin de acogerse al beneficio, el certificado debe ser emitido como máximo a la fecha y hora de la etapa competitiva.

En caso de que los oferentes que se encuentren dentro del rango del porcentaje para beneficiarse del margen, no presentaren con su oferta el certificado o presentare la constancia en trámite del mismo, el Comité de Evaluación solicitará por escrito el certificado aquellas ofertas que hayan declarado ser nacionales. Si luego del requerimiento realizado por el Comité el oferente no presentare el documento, o la presentación sea deficiente o tardía, la oferta no será descalificada, pero no podrá acogerse al beneficio.

Durante la evaluación de la oferta, si la oferta evaluada como la más baja es una oferta de un bien importado o que no haya presentado el Certificado de Origen de Producto y Empleo Nacional, esta será comparada con la oferta más baja del bien nacional que ha presentado el aludido certificado, agregándole al precio total del bien que no cuenta con el Certificado de Origen de Producto y Empleo Nacional una suma equivalente al porcentaje establecido en la legislación vigente. Si en dicha comparación adicional, la oferta del bien producido del bien producido en el Paraguay que haya acreditado mediante la presentación del certificado, resultare ser la más baja se la seleccionará para la adjudicación; caso contrario se seleccionará la oferta del bien proveniente del extranjero o que no haya presentado el citado documento.

**D) CRITERIO DE DESEMPATE**

Siempre que el criterio de desempate establecido en las IAO de SBE no sean aplicables y en caso de que existan dos o más oferentes solventes que cumplan con todos los requisitos establecidos en el pliego de bases y condiciones del llamado, igualen en precio y sean sus ofertas las más bajas, el comité de Evaluación determinará cuál de ellas es la mejor calificada para ejecutar el contrato utilizando los criterios en el siguiente orden.

a) En primer lugar, la convocante tendrá en cuenta al oferente que tenga mayor cantidad de empleados inscriptos en el Instituto de Previsión Social – IPS, en promedio de los últimos seis meses anteriores al Acto de Apertura, para ello se requerirá la presentación de la “Declaración Jurada de Salarios” que el empleador utilizó para el pago del seguro social, en caso de que la documentación no esté contenida en la oferta o en el Sistema de Información de Proveedores del Estado (SIPE)

b) De persistir el empate, se analizará la capacidad financiera del Oferente, para cuyo efecto se verificará quien posea el mayor coeficiente en el Ratio de Liquidez (activo corriente / pasivo corriente) del último año.

c) Si aun aplicando este criterio de desempate, persistiera el mismo, la Convocante analizará la capacidad técnica de las ofertas evaluándose lo siguiente: El que posea la mayor cantidad de contratos ejecutados satisfactoriamente en el último año.

En caso de Consorcios;

Para los criterios a) y b), se sumarán los promedios y los coeficientes, respectivamente, de cada miembro, a los efectos de promediar los resultados; para el criterio c) se sumarán las cantidades de los contratos de todos los miembros.

De persistir el empate luego de la aplicación de los criterios precedentemente indicados, la Convocante determinará cuál es la oferta a ser adjudicada, exponiendo las razones de su elección en el Informe de Evaluación o en el acto administrativo de adjudicación.

**2. REQUISITOS PARA CALIFICACIÓN POSTERIOR**

La Convocante efectuará la calificación del Oferente, empleando únicamente los requisitos aquí estipulados. Los requisitos que no estén incluidos en el siguiente texto no podrán ser utilizados para evaluar las calificaciones del Oferente.

1. **Capacidad financiera**

Con el objetivo de calificar la situación financiera del Oferente, se considerarán los siguientes índices:

1. **Oferentes contribuyentes de IRACIS.**

Deberán cumplir con el siguiente parámetro:

a.  **Ratio de Liquidez:** activo corriente / pasivo corriente

Deberá ser igual o mayor que 1, en promedio, en los 3 años (2016, 2017 y 2018)

b**. Endeudamiento:** pasivo total / activo total

No deberá ser mayor a 0,80 en promedio, en los 3 años (2016, 2017 y 2018)

**c. Rentabilidad:** Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital.

El promedio en los en 3 (tres) años (2016, 2017 y 2018), no deberá ser negativo.

1. **Oferentes Contribuyentes de IRPC**

Deberán cumplir el siguiente parámetro:

**Eficiencia:** (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los 3 años (2016, 2017 y 2018).

1. **Oferentes contribuyentes de IRP**

Deberán cumplir el siguiente parámetro:

**Eficiencia:** (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los 3 años (2016, 2017 y 2018)

1. **Oferentes contribuyentes de exclusivamente IVA General**

Deberá cumplir el siguiente parámetro:

**Eficiencia:** (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los 3 últimos meses que serán verificados conforme al Calendario Perpetuo de vencimientos establecido por la SET.

Los oferentes al efecto de lo anteriormente señalado, deberán presentar los documentos que se indican en el Anexo I.

**Oferentes en Consorcio:** El análisis de la Capacidad financiera se realizará al Oferente Líder del Consorcio, el cual deberá cumplir con los parámetros establecidos de acuerdo al tipo de contribuyente.

1. **Experiencia y Capacidad Técnica**

El Oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de experiencia:

1. Los oferentes deberán presentar cartas de autorización del fabricante o de distribuidor debidamente autorizado para presentar oferta.

En caso de oferentes en consorcio las autorizaciones podrán ser de realizarás a cualesquiera de los miembros integrantes del consorcio.

1. Los oferentes deberán presentar copias de contratos de provisión de equipos informáticos de los tres últimos años (2016, 2017 y 2018). El promedio de la suma de los tres últimos años deberá ser de por lo menos el 50% del valor de la oferta.

Para oferentes en consorcio se considerará todos los contratos y/o facturaciones presentados de todos los miembros integrantes del consorcio.

1. El oferente o el subcontratista a ser contratado por el oferente para la realización de los servicios del ítem 10 – Readecuación del Data Center deberá presentar Fotocopia de contratos y/o Facturaciones que demuestre que cuenta con experiencia en Construcciones y/o readecuaciones y/o ampliaciones de Obras en General dentro de los últimos 2 (dos) años 2017 y 2018 cuya sumatoria de contratos sea al menos el 50 % del monto ofertado en el Ítem 10 – Readecuación del Data Center.

En el caso de oferentes en consorcio la experiencia deberá ser de cualesquiera de los miembros integrantes del consorcio.

1. En el caso de que el oferente designe a un subcontratista para la realización de los servicios del ítem 10 – Readecuación del Data Center deberá presentar:
2. Declaración Jurada del oferente en el cual se compromete a contratar una persona física o jurídica para la Realización del Servicio establecido en el Ítem 10 – Readecuación del Data Center en el cual se detalle los datos del subcontratista: Nombre o Razón Social, RUC, Teléfono, Dirección, correo electrónico, nombre del/los represente/s legal/es del subcontratista. El monto a ser subcontratado no deberá ser superior al 60 % del monto total de la oferta.
3. Documento que demuestre que el/los represente/s legal/es del Subcontratista a ser contratado por el oferente cuenta con la capacidad de comprometer a la firma ya sea estos (Fotocopia simple de Estatuto Social, Constitución de la Sociedad, Poderes Generales o especiales ante Escribanía Pública, Actas de Directorio o Actas de Asamblea. En el caso de personas físicas la fotocopia de cedula de identidad del propietario de la firma subcontratista. En el caso de que el subcontratista designe a otra persona la representación legal, deberá presentar el Poder ante Escribanía Pública).
4. Declaración Jurada del Art. 40 firmada por el/los represente/s legal/les del Subcontratista a ser designado para el desarrollo de los servicios.
5. Declaración Jurada del subcontratista a ser designado por el oferente en el cual manifieste contar con todas las herramientas, equipos, insumos, materiales y personales capacitados para la realización del servicios y se compromete a firmar un contrato de subcontratación con el oferente en el caso de ser adjudicado.
6. Planilla de cumplimiento mínimo declarando “si cumple o no cumple”.
7. 2 (dos) copias de contratos de provisiones de Sistema de Detección y Extinción de Incendios automática en Data Centers.

En el caso de oferentes en consorcio el contrato podrá ser de cualesquiera de los miembros integrantes del consorcio.

1. 2 (dos) copias de contratos de provisiones de UPS trifásicas de potencia igual o superior a las solicitadas en este llamado.

En el caso de oferentes en consorcio el contrato podrá ser de cualesquiera de los miembros integrantes del consorcio.

1. 3 (tres) copias de contratos de provisiones de storage SAN de la misma marca al ofertado en este llamado.

En el caso de oferentes en consorcio el contrato podrá ser de cualesquiera de los miembros integrantes del consorcio.

1. 4 (cuatro) copias de contratos de provisiones de Router de Borde de la misma marca al ofertado en este llamado

En el caso de oferentes en consorcio el contrato podrá ser de cualesquiera de los miembros integrantes del consorcio.

1. 2 (dos) copias de contratos de provisiones de Servidores de la misma marca y modelo al ofertado en este llamado.

En el caso de oferentes en consorcio el contrato podrá ser de cualesquiera de los miembros integrantes del consorcio.

1. 2 (dos) copias de contratos de provisiones de Monitores Profesionales de la misma marca a los ofertados en este llamado.

En el caso de oferentes en consorcio el contrato podrá ser de cualesquiera de los miembros integrantes del consorcio.

1. 1 (una) copia de contrato de provisión de UPS de la misma marca y potencia (igual o superior) al solicitado en este llamado.

En el caso de oferentes en consorcio el contrato podrá ser de cualesquiera de los miembros integrantes del consorcio

1. 2 (dos) copias de contrato de provisión de sistemas de detección y extinción de incendios automática con gas FM200, ECARO o Novec.

En el caso de oferentes en consorcio el contrato podrá ser de cualesquiera de los miembros integrantes del consorcio

1. 1 (una) copia de contrato de provisión de mantenimiento del Data Center.

En el caso de oferentes en consorcio el contrato podrá ser de cualesquiera de los miembros integrantes del consorcio

1. Certificado ISO 9001 o similar del oferente de modo a garantizar la calidad de los servicios ofrecidos.

En el caso de oferentes en consorcio el Certificado ISO 9001 o similar deberá ser del oferente Líder del Consorcio.

**(c) Solicitud de Muestras**

NO APLICA

**(d) Inspecciones y Pruebas en la etapa de evaluación**

NO APLICA

***Nota***: Conforme las disposiciones del Decreto 7781/06, para las Contrataciones con Organismos de la Administración Central, el Oferente que resulte adjudicado, deberá contar con una cuenta corriente y/o caja de ahorro habilitada en un Banco de plaza, o en su defecto, hallarse en condiciones de poder habilitar una cuenta corriente y/o caja de ahorro a su nombre, a fin de poder hacer efectivo el Pago Directo a Proveedores y Acreedores vía acreditación en cuenta bancaria.

**SECCION III**

**REQUISITOS DE LOS BIENES Y/O SERVICIOS REQUERIDOS**

**1. Lista de Bienes**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ítem** | **Descripción del Bien** | **Unidad de Medida** | **Cantidad** |
| 1 | Router de borde | Unidad | 2 |
| 2 | Servidor | Unidad | 3 |
| 3 | Storage | Unidad | 1 |
| 4 | UPS 40 KVA | Unidad | 1 |
| 5 | Sistema de CCTV | Global | 1 |
| 6 | Sistema de Control de Acceso | Global | 1 |
| 7 | Pantalla para NOC (2 x 2) | Unidad | 1 |
| 8 | Sistema de detección y extinción de incendios automática de incendios (Sala de Equipos) | Global | 1 |
| 9 | Sistema de detección y extinción de incendios automática de incendios (Sala de Energía) | Global | 1 |
| 10 | Readecuación Data Center | Global | 1 |
| 11 | Licencias de virtualización | Unidad | 3 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ítem** | **Descripción** | **Unidad de Medida** | **Cantidad Mínima** | **Cantidad Máxima** |
| 12 | Servicio Mantenimiento preventivo y correctivo | Hora | 200 | 200 |

**2. Especificaciones Técnicas**

**Objetivo**

Estas especificaciones tienen como objetivo ilustrar a todos los Oferentes sobre los criterios que deberán ser respetados para la cotización y posterior realización del proyecto de referencia, para el Ministerio de Industria y Comercio (MIC) – Dirección General de Firma Digital y Comercio Electrónico en lo que a **Infraestructura del Data Center** se refiere, las descripciones de las mismas y servicios necesarios para su implementación.

Los bienes y servicios ofertados deberán ser presupuestados atendiendo siempre a estas especificaciones técnicas y que cada oferente lo analizará entendiendo que será el marco mínimo a ser respetado tanto en la cotización como en la realización si fuere posteriormente adjudicado. Todo trabajo incluido en estas especificaciones deberá cumplir con los requisitos aquí mencionados, así como a las reglas del buen arte inherentes a la realización de los diversos trabajos.

**Ítem 1: Router de Borde**

|  |  |  |  |
| --- | --- | --- | --- |
| **ESPECIFICACIONES TÉCNICAS MÍNIMAS** | | | |
| **Nombre del Bien o Servicio Conexo** | **Descripción Técnica** | **Mínimo Exigido** | **El bien ofertado cumple con las especificaciones requeridas (SI/NO)** |
| **Marca:** | **Especificar** | |  |
| **Modelo:** | **Especificar** | |  |
| **Procedencia:** | **Especificar** | |  |
| **Cantidad:** | **02 (dos)** | **Exigido** |  |
| **Características Principales** | | | |
| **Definición:** | Sistema de Seguridad informática que sea del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés) | **Exigido** |  |
| **Funcionalidades y características del sistema** | | | |
| **Características de Desempeño:** | Numero de Interfaces Requeridas | **Como mínimo el dispositivo deberá contar con 20 interfaces de red (RJ-45 o SFP)** |  |
| Configuraciones de Alta Disponibilidad soportadas | **Activo-Activo/ Activo-Pasivo, Clúster** |  |
| Throughput de Firewall IPv4 e IPv6 (paquetes de 64 bytes) | **≥ 8 Gbps** |  |
| Latencia de Firewall | **≤ 4 µs** |  |
| Throughput de Antivirus | **≥ 1.200 Mbps** |  |
| Throughput de IPS | **≥ 2.000 Mbps** |  |
| Soporte de VPN | **SSL, IPSec** |  |
| Throughput de VPN IPSec | **≥ 8 Gbps** |  |
| Throughput VPN SSL | **≥ 800 Mbps** |  |
| Sesiones VPN IPSec Gateway -Gateway | **≥ 1.800** |  |
| Sesiones VPN IPSec Client-Gateway | **≥ 10.000** |  |
| Cantidad máxima de usuarios SSL-VPN concurrentes | **≥ 280** |  |
| Sesiones Concurrentes | **≥ 1.500.000** |  |
| Nuevas sesiones / segundo (TCP) | **≥ 130.000** |  |
| Políticas de Firewall | **≥ 10.000** |  |
| Dimensiones de Rack | **Altura máxima 1 RU** |  |
| Numero de Instancias virtuales (máximas) | **≥ 8** |  |
| AC Power | **220V AC** |  |
| Consumo de potencia promedio | **≤ 75 Watts** |  |
| **Características de Hardware:** | Interfaces GigaEthernet (switcheadas) 10/100/1000: | **≥ 14 GbE RJ-45** |  |
| Interfaces WAN del tipo RJ45 GE. Serán aceptados equipos que soporten interfaces WAN definidas lógicamente. | **Mínimo 2 unidades** |  |
| Interfaces de Administración: | **Mínimo 2 unidades (1x USB + 1 x Puerto de consola)** |  |
| Almacenamiento interno: | **1 x SSD de 400 GB o superior** |  |
| Interfaces SFP/SFP+: | **4 x SFP** |  |
| **Características del dispositivo:** | El dispositivo debe ser una appliance de propósito específico | **Exigido** |  |
| Capacidad de re-ensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC). | **Exigido** |  |
| El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red. | **Exigido** |  |
| En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP. | **Exigido** |  |
| **Características del Sistema operativo incluido:** | Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows | **Exigido** |  |
| **Firewall:** | Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs | **Exigido** |  |
| Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando | **Exigido** |  |
| Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos. | **Exigido** |  |
| Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI como por GUI | **Exigido** |  |
| La solución deberá tener la capacidad de balancear carga entre servidores. | **Exigido** |  |
| En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID | **Exigido** |  |
| **Conectividad y sistema de ruteo:** | Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP | **Exigido** |  |
| Soporte a etiquetas de VLAN (802.1q) | **Exigido** |  |
| Soporte a ruteo estático | **Exigido** |  |
| Soporte a políticas de ruteo (policy routing) | **Exigido** |  |
| Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS (opcional) | **Exigido** |  |
| Soporte a ruteo dinámico RIPng, OSPFv3, BGP4+ | **Exigido** |  |
| Soporte de ECMP (Equal Cost Multi-Path) | **Exigido** |  |
| Soporte a ruteo de multicast | **Exigido** |  |
| Soporta protocolo sFlow o NetFlow. | **Exigido** |  |
| **VPN IPsec/L2TP/PPTP:** | Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) | **Exigido** |  |
| Soporte para IKEv2 y IKE Configuration Method | **Exigido** |  |
| Debe soportar la configuración de túneles L2TP y PPTP | **Exigido** |  |
| Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES. | **Exigido** |  |
| Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits | **Exigido** |  |
| Posibilidad de crear VPN’s entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site. | **Exigido** |  |
| La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN) | **Exigido** |  |
| **VPN SSL:** | Capacidad de realizar SSL VPNs. | **Exigido** |  |
| Soporte de renovación de contraseñas para LDAP y RADIUS. | **Exigido** |  |
| Soporte a asignación de aplicaciones permitidas por grupo de usuarios | **Exigido** |  |
| Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet. | **Exigido** |  |
| Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL. | **Exigido** |  |
| La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS | **Exigido** |  |
| **Traffic Shapping / QoS:** | Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall | **Exigido** |  |
| Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente | **Exigido** |  |
| Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo | **Exigido** |  |
| Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia | **Exigido** |  |
| **Autenticación y Certificación Digital:** | Capacidad de integrarse con Servidores de Autenticación RADIUS. | **Exigido** |  |
| Capacidad nativa de integrarse con directorios LDAP | **Exigido** |  |
| Capacidad incluida, al integrarse con Microsoft Windows Active Directory | **Exigido** |  |
| **Antivirus:** | Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP. | **Exigido** |  |
| El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente. | **Exigido** |  |
| El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6. | **Exigido** |  |
| **Antispam:** | La capacidad antispam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje. | **Opcional** |  |
| La capacidad AntiSpam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). | **Opcional** |  |
| **Filtraje de URLs (URL Filtering):** | Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos. | **Exigido** |  |
| **IPS:** | El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror | **Exigido** |  |
| Capacidad de detección de más de 4000 ataques. | **Exigido** |  |
| El Detector y preventor de intrusos deberá de estar orientado para la protección de redes. | **Exigido** |  |
| **Filtraje de tráfico VoIP, Peer-to-Peer y Mensajería instantánea** | Soporte a aplicaciones multimedia tales como (incluyendo): SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP). | **Exigido** |  |
| El dispositivo deberá técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer), soportando al menos Yahoo! Messenger, MSN Messenger, ICQ y AOL Messenger para Messenger, y BitTorrent, eDonkey, GNUTella, KaZaa, Skype y WinNY para Peer-to-peer. | **Exigido** |  |
| **Licenciamiento y Actualizaciones** | El licenciamiento de todas las funcionalidades debe ser ilimitado en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URL Filtering debe proveerse por al menos 36 meses. | **Exigido** |  |
| **Garantía** | Se solicita garantía del equipo por el periodo de 36 meses, con soporte técnico en modalidad 24x7 | **Exigido** |  |
| **Certificados** | ISO 9001 | **Exigido** |  |
| **Autorización** | El oferente deberá contar con una autorización escrita del fabricante o el distribuidor en Paraguay para presentar la oferta. | **Exigido** |  |

**Ítem 2: Servidor**

|  |  |  |  |
| --- | --- | --- | --- |
| **ESPECIFICACIONES TÉCNICAS MÍNIMAS** | | | |
| **Nombre del Bien o Servicio Conexo** | **Descripción Técnica** | **Mínimo Exigido** | **El bien ofertado cumple con las especificaciones requeridas (SI/NO)** |
| **Marca:** | **Especificar** | |  |
| **Modelo:** | **Especificar** | |  |
| **Procedencia:** | **Especificar** | |  |
| **Cantidad:** | **03 (tres)** | **Exigido** |  |
| **Descripción** | **Servidor** | **Exigido** |  |
| **Factor de Forma** | Rackeable de 2U máximo. | **Exigido** |  |
| **Procesador** | Cantidad instalada en el equipo: 1 (uno) | **Exigido** |  |
| Cantidad máxima soportada por el equipo: 2 (dos) | **Exigido** |  |
| Características de cada procesador: 14 núcleos como mínimo, de 2.2 GHz como mínimo. | **Exigido** |  |
| **Memoria** | Cantidad instalada: 80 GB como mínimo (distribuidos en DIMMs de 16/32 GB cada uno). | **Exigido** |  |
| Tipo de memoria: DDR4 2.666 RDIMM | **Exigido** |  |
| Cant. Máx. de slots: 24 (veinticuatro) | **Exigido** |  |
| Capacidad máxima: 1.5 TB como mínimo. | **Exigido** |  |
| Tipos de Protección Soportadas: ECC, Memory Mirroring y Memory Sparing como mínimo | **Exigido** |  |
| **Almacenamiento** | 4 (cuatro) unidades de 600GB o superior, SAS de al menos 10.000 rpm, 12 Gbps hot swap. | **Exigido** |  |
| Capacidad de albergar hasta 8 discos SFF, y con capacidad de poder albergar a futuro 16 discos SFF como mínimo. | **Exigido** |  |
| El equipo debe poder soportar discos SAS, SATA y NVMe. | **Exigido** |  |
| **Controladora de discos** | 2 GB de cache tipo Flash o superior. | **Exigido** |  |
| Soporte para RAID 0, 1, 5, 6, 10, 50 y 60. | **Exigido** |  |
| **Ranuras de Expansión** | El equipo debe contar con cinco slots PCIe disponibles como mínimo. | **Exigido** |  |
| **Interfaces de periféricos** | Puertos USB: cuatro unidades (por lo menos dos de 3.0) | **Exigido** |  |
| Gráfico DB-15: una unidad posterior y una unidad frontal. | **Exigido** |  |
| Serial: con capacidad de poder agregar una unidad a futuro. | **Exigido** |  |
| El equipo debe contar con la capacidad de agregar a futuro dos discos SSD internos (en configuración espejada los mismos) para el S.O. o hypervisor. | **Exigido** |  |
| **Tarjeta Gráfica** | Puerto grafico de 16MB integrado con resolución máxima de 1920x1200, 16bpp, 60Hz. | **Exigido** |  |
| **Fuente de alimentación** | Fuentes de poder que no supere los 760 watts y sea cambiable en caliente, en configuración redundante. Certificación 80 PLUS Platinum o similar como mínimo. | **Exigido** |  |
| **Comunicaciones** | Cuatro puertos Gigabit Ethernet 10/100/1000 BASE-T. | **Exigido** |  |
| 1 x HBA 16 Gbps FC | **Exigido** |  |
| **Sistema Operativos Soportados** | Windows Server 2012 R2 o superior | **Exigido** |  |
| Red Hat Enterprise Linux 6.9 x64 o superior | **Exigido** |  |
| SUSE Enterprise Linux Server 11 x64 SP4 o superior | **Exigido** |  |
| VMware ESXi 6.0 U3 o superior | **Exigido** |  |
| Xenserver 7.1 o superior | **Exigido** |  |
| NeoKylin 6.9 o superior | **Exigido** |  |
| Oracle VM | **Exigido** |  |
| Oracle Linux | **Exigido** |  |
| **Características RAS** | Diagnóstico de fallas de hardware en el equipo mediante LEDs indicadores; y también debe contar con análisis predictivo de fallas que cubra los siguientes componentes del sistema: procesador, regulador de voltaje, memoria, discos, controladores de disco, fuente de poder y ventiladores. | **Exigido** |  |
| **Administración** | Puerto dedicado RJ-45 con soporte de Consola Remota opcional. | **Exigido** |  |
| Capacidad de poder administrar desde un smartphone con Android o iOS conectando el mismo al server a través de un puerto USB. | **Exigido** |  |
| **Kit de Montaje en Rack y Accesorios** | Proporcionar el kit completo de: cables, soportes, organizadores y demás accesorios requeridos para el montaje y funcionamiento correcto del servidor en el rack. | **Exigido** |  |
| **Servicio de Montaje** | El proveedor deberá montar y configurar apropiadamente el servidor en el rack en las oficinas del cliente | **Exigido** |  |
| **Certificado de Calidad** | La marca ofertada debe contar con certificación ISO 9001 y 14001 como mínimo. | **Exigido** |  |
| **Autorización del fabricante** | El oferente deberá contar con Autorización del Representante Local de la marca en Paraguay, quien a su vez deberá estar avalado por el Fabricante. | **Exigido** |  |
| **Garantía** | 3 (tres) años On Site. El servicio de garantía deberá ser realizado por técnicos certificados del CAS (Centro Autorizado de Servicios) avalado por el Fabricante. | **Exigido** |  |

**Ítem 3: Storage**

|  |  |  |  |
| --- | --- | --- | --- |
| **ESPECIFICACIONES TÉCNICAS MÍNIMAS** | | | |
| **Nombre del Bien o Servicio Conexo** | **Descripción Técnica** | **Mínimo Exigido** | **El bien ofertado cumple con las especificaciones requeridas (SI/NO)** |
| **Marca:** | **Especificar** | |  |
| **Modelo:** | **Especificar** | |  |
| **Procedencia:** | **Especificar** | |  |
| **Cantidad:** | **01 (uno)** | **Exigido** |  |
| **Descripción** | **Storage SAN** | **Exigido** |  |
| **Factor de forma** | Rackeable 19”, de dimensión 2U | **Exigido** |  |
| **Protocolos Front-End Soportados por el equipo.** | FC 16 Gbps | **Exigido** |  |
| FCoE 10 Gbps | **Exigido** |  |
| iSCSI 1 y 10Gbps | **Exigido** |  |
| SAS 12 Gbps | **Exigido** |  |
| **Detalles del sistema de almacenamiento** | El sistema de almacenamiento debe incluir dos controladoras activas y redundantes entre sí. | **Exigido** |  |
| Cada controladora debe contar con cuatro puertos FC 16 Gbps para conectividad Front-End. | **Exigido** |  |
| Cada controladora debe tener 8 GB de memoria caché. En caso de interrupción del fluido eléctrico, el equipo deberá contar con un mecanismo para realizar el destage (mover la información de caché a disco) con el fin de proteger la integridad de la información hasta que se re energice el equipo. | **Exigido** |  |
| No se aceptarán tecnologías de tarjetas PCI o discos de estado sólido como memoria caché. | **Exigido** |  |
| **Niveles de RAID** | El sistema de almacenamiento debe incluir la capacidad de definir arreglos de discos magnéticos de tipo RAID 0, 1, 5, 6, 10 y distribuido. | **Exigido** |  |
| **Discos magnéticos** | El equipo debe contar con 5 discos de 2 TB 7.2k rpm como mínimo. | **Exigido** |  |
| **Tipos de discos soportados.** | SSD SAS 12 Gbps | **Exigido** |  |
| SSD RI SAS 12 Gbps | **Exigido** |  |
| HDD 15k rpm SAS | **Exigido** |  |
| HDD 10k rpm SAS 12 | **Exigido** |  |
| HDD 7.2k rpm NL-SAS 12 | **Exigido** |  |
| **Escalabilidad** | El equipo debe tener la posibilidad de crecer hasta 350 discos a futuro. | **Exigido** |  |
| El sistema de almacenamiento debe ser capaz de poder soportar discos de 2.5” y 3.5” dentro de él. | **Exigido** |  |
| El sistema de almacenamiento debe ser capaz de poder agregar cajones de expansión, tanto de 2.5” como de 3.5” y puede mezclar ambos tipos de expansiones dentro de sí y con capacidad de soportar hasta 10 cajones de expansión dentro del mismo subsistema como mínimo. | **Exigido** |  |
| El sistema de almacenamiento debe ser capaz de poder agregar cajones de expansión de alta densidad de discos. | **Exigido** |  |
| **Software de Administración y Monitoreo del desempeño** | El sistema debe incluir la licencia de uso de la funcionalidad del software de administración del sistema. | **Exigido** |  |
| La licencia de uso debe tener cobertura para los sistemas operativos con los que es compatible el sistema de almacenamiento. | **Exigido** |  |
| **Software de copia y replicación.** | El sistema debe poder ser capaz de realizar copias de los volúmenes dentro del mismo sistema de almacenamiento (Snapshots y Clones). Dicha funcionalidad debe ser incluida en caso de ser una licencia adicional. | **Exigido** |  |
| El sistema debe poder ser capaz réplica remota sincrónica y asíncrona bidireccional vía FC. Dicha funcionalidad debe ser incluida en caso de ser una licencia adicional. | **Exigido** |  |
| **Software de Aprovisionamiento** | El sistema debe incluir el licenciamiento de software especializado que permita la provisión de capacidad física de almacenamiento en forma dinámica, la capacidad asignada no se deberá alojar en cuanto se cree el volumen, se deberá provisionar en cuanto la data sea efectivamente escrita en el volumen. (Thin- Provisioning) | **Exigido** |  |
| **Software de Tiering Automático** | El sistema debe poder soportar software que permita realizar tiering automático (movimiento de datos entre tecnologías distintas de disco) a nivel de sub lun. Dicha funcionalidad debe ser incluida en caso de ser una licencia adicional. | **Exigido** |  |
| **Disponibilidad de componentes** | Las controladoras, discos magnéticos, fuentes de poder y ventiladores deben ser hot-swap. | **Exigido** |  |
| Las controladoras, fuentes de poder y ventilación deben ser redundantes. | **Exigido** |  |
| **Sistemas operativos de hosts compatibles** | Microsoft Windows Server | **Exigido** |  |
| Red Hat Enterprise Linux | **Exigido** |  |
| VMware | **Exigido** |  |
| SUSE Enterprise Linux Server | **Exigido** |  |
| AIX | **Exigido** |  |
| **Certificado de Calidad** | La marca ofertada debe contar con certificación ISO 9001 y 14001 como mínimo. | **Exigido** |  |
| **Autorización del fabricante** | El oferente deberá contar con Autorización del Representante Local de la marca en Paraguay, quien a su vez deberá estar avalado por el Fabricante. | **Exigido** |  |
| **Garantía** | 3 (tres) años On Site. El servicio de garantía deberá ser realizado por técnicos certificados del CAS (Centro Autorizado de Servicios) avalado por el Fabricante. | **Exigido** |  |

**Ítem 4: UPS 40 KVA**

|  |  |  |  |
| --- | --- | --- | --- |
| **ESPECIFICACIONES TÉCNICAS MÍNIMAS** | | | |
| **Nombre del Bien o Servicio Conexo** | **Descripción Técnica** | **Mínimo Exigido** | **El bien ofertado cumple con las especificaciones requeridas (SI/NO)** |
| **Marca:** | **Especificar** | |  |
| **Modelo:** | **Especificar** | |  |
| **Procedencia:** | **Especificar** | |  |
| **Cantidad:** | **01 (uno)** | **Exigido** |  |
| **Descripción** | **UPS 40 KVA** | **Exigido** |  |
| **Configuración Base** | | |  |
| Potencia | 40.000 VA / 36.000 Watt | **Exigido** |  |
| Tecnología | On Line de doble conversión, con tecnología de doble control DSP de gran capacidad y completo control digital | **Exigido** |  |
| Formato | Torre | **Exigido** |  |
| **Entrada** | | |  |
| Tensión de entrada nominal | 380V | **Exigido** |  |
| Rango Frecuencia nominal | 40-70Hz | **Exigido** |  |
| Rango de tensión: | 204-520VAC (carga ≤50%); 242-520VAC (50% <carga ≤70%); 304-520VAC (70% <carga ≤100%) | **Exigido** |  |
| Fase | Trifásico + N+G | **Exigido** |  |
| Factor potencia | ≥0.99 | **Exigido** |  |
| **Salida** | | |  |
| Tensión | 380V | **Exigido** |  |
| Frecuencia | 50Hz/60Hz±5% | **Exigido** |  |
| Onda | Senoidal pura | **Exigido** |  |
| Distorsión de onda | ≤1% (Carga lineal); ≤4% (Carga no lineal) | **Exigido** |  |
| Factor de cresta | 3:1 | **Exigido** |  |
| Fase | Trifásico + N + G | **Exigido** |  |
| Factor de potencia | 0,9 | **Exigido** |  |
| **Batería** | | |  |
| Banco de batería | Externo | **Exigido** |  |
| Tipo de la batería | 12V 9Ah | **Exigido** |  |
| Tensión de la batería | ±384V | **Exigido** |  |
| Autonomía | 8 horas al 80% de la carga | **Exigido** |  |
| **Comunicación / Administración** | | |  |
| Software de comunicación | Software de monitoreo y comunicación Incluye CD | **Exigido** |  |
| Puerto de comunicación | RS232, USB. Incluir cable USB | **Exigido** |  |
| Monitoreo | Tarjeta de monitoreo SNMP | **Exigido** |  |
| **Otros** | | |  |
| Pantalla | LCD 5.7 pulgadas (con funciones táctil) | **Exigido** |  |
| Conexión en paralelo | Capacidad para soportar 4 conexiones | **Exigido** |  |
| Refrigeración | Refrigeración por aire forzado (ajustable para diferentes cargas) | **Exigido** |  |
| Indicadores de pantalla | Capacidad de Batería, Porcentaje de carga, Voltaje de salida, Voltaje y frecuencia de entrada, Alarma. Bypass. Inversor. | **Exigido** |  |
| Ruido | <60 (1metro) | **Exigido** |  |
| Temperatura | 0~40ºC | **Exigido** |  |
| Humedad | 0~90% (Sin condensación) | **Exigido** |  |
| Certificaciones | ISO 9001:2008 | **Exigido** |  |
| ISO 14001:2004 | **Exigido** |  |
| EN62040-2:2006 | **Exigido** |  |
| EN62040-1:2008 | **Exigido** |  |
| IEC 61000-4-2:2008 | **Exigido** |  |
| IEC 61000-4-3:2006+A1:2007+A2:2010 | **Exigido** |  |
| IEC 61000-4-4:2012 | **Exigido** |  |
| IEC 61000-4-5:2005 | **Exigido** |  |
| IEC 61000-4-6:2008 | **Exigido** |  |
| IEC 61000-4-8:2009 | **Exigido** |  |
| IEC 61000-4-11:2004 | **Exigido** |  |
| Garantía escrita | 24 meses sobre el equipo, ante desperfectos de fábrica y 12 meses sobre las baterías | **Exigido** |  |
| Servicio Técnico | Se deberá contar con un Centro de Servicios Autorizado (CAS) al cual se destine toda atención ante cualquier situación que presente el equipo. El CAS deberá poseer técnicos certificados por el fabricante de la marca de la UPS ofertada. | **Exigido** |  |
| Autorización | Carta de autorización del representante local autorizado. | **Exigido** |  |
| Manual | El contratista o adjudicatario deberá proveer el manual del usuario original de fábrica por cada equipo. | **Exigido** |  |
| Información del producto | Catálogo informativo del producto ofertado. | **Exigido** |  |

**Ítem 5: Sistema de CCTV**

|  |  |  |  |
| --- | --- | --- | --- |
| **ESPECIFICACIONES TÉCNICAS MÍNIMAS** | | | |
| **Nombre del Bien o Servicio Conexo** | **Descripción Técnica** | **Mínimo Exigido** | **El bien ofertado cumple con las especificaciones requeridas (SI/NO)** |
| **Marca:** | **Especificar** | |  |
| **Modelo:** | **Especificar** | |  |
| **Procedencia:** | **Especificar** | |  |
| **Cantidad:** | **01 (uno)** | **Exigido** |  |
| **Descripción** | **Sistema de CCTV** | **Exigido** |  |
| **NVR** | El hardware deberá estar basados sobre un sistema operativo confiable recomendado por el fabricante. | **Exigido** |  |
| Deberá ser un equipo diseñado y optimizado para las exigencias de aplicaciones de video vigilancia contando con redundancia en los principales componentes. | **Exigido** |  |
| Configuración de redundancia como mínimo en RAID 5 para permitir el funcionamiento aun cuando existan discos en falla. | **Exigido** |  |
| Los servidores a ser proporcionados deben corresponder a la misma marca de las cámaras que se están cotizando. Es permitido cotizar otras marcas de servidores, los mismos deben ir acompañados de la carta donde se garantice la compatibilidad por los fabricantes. | **Exigido** |  |
| Se deberá entregar la tabla de cálculo de almacenamiento especificada por el fabricante para poder validar la oferta. | **Exigido** |  |
| Discos rígidos SATA con capacidad de escritura para video vigilancia IP. | **Exigido** |  |
| Deberá permitir un ancho de banda máximo de grabación de 200 Mbps | **Exigido** |  |
| Deberá permitir un ancho de banda máximo de visualización de 100 Mbps, sin disminuir el ancho de banda de grabación. | **Exigido** |  |
| Deberá admitir a lo menos 16 canales de cámaras por cada servidor. | **Exigido** |  |
| Deberá ser compatible con las cámaras que ya se encuentran instaladas en el Data Center de la marca Hanwha Techwin, modelo SND-6011R (8 cámaras en total) | **Exigido** |  |
| Debe admitir hasta 30 imágenes por segundo por cada canal de cámara. | **Exigido** |  |
| Cada servidor de grabación debe permitir 6 TB de capacidad como mínimo | **Exigido** |  |
| Deberá contar con por lo menos 2 puertos Gigabit Ethernet. | **Exigido** |  |
| Deberá contar con por lo menos 1 puerto SFP combinado de 10/100/1000 Mbps | **Exigido** |  |
| Deberá contar en el mismo equipo un Switch administrable a través de web Browser de 16 puertos 10/100 (802.11at) | **Exigido** |  |
| Fuente de alimentación acorde y preparada para Sistemas de Grabación de Video Vigilancia. | **Exigido** |  |
| Deberá contar con chasis de montaje en bastidor. | **Exigido** |  |
| Deberá ser en formato 1U | **Exigido** |  |
| **Certificaciones** | **Exigido** |  |
| Seguridad: | **Exigido** |  |
| EN 60950-1:2006 + A11:2009; IEC 60950-1:2005 Ed2 o similar | **Exigido** |  |
| **Seguridad** | **Exigido** |  |
| Protección por contraseña, cifrado HTTPS, registro de acceso de usuario, autenticación basada en el puerto 802.1x en Switch administrable | **Exigido** |  |
| **Condiciones de Operación.** | **Exigido** |  |
| Temperatura de Operación: | **Exigido** |  |
| Menos 0 °C a 40 °C (0°C a 40°C) | **Exigido** |  |
| Humedad Relativa: 10 – 90 % sin condensación | **Exigido** |  |
| **Garantías** | **Exigido** |  |
| El oferente deberá presentar junto con su oferta carta de autorización firmada por un representante del fabricante con potestades sobre nuestra región, por la cual se autorice al oferente a proveer los equipos ofertados. | **Exigido** |  |
| Los técnicos de la empresa oferente deberán estar certificados por el fabricante. Los profesionales deberán residir en Paraguay, así como ser personal estable y formar parte de la nómina de la empresa oferente. | **Exigido** |  |
| Garantía escrita del fabricante de al menos 3(tres) años | **Exigido** |  |
| **Software de Gestión de Video en Red (NVMS)** | EL NVMS proporciona estaciones de trabajo con un diseño de pantalla simplificado, controles intuitivos y características personalizables, que mejoran las interacciones entre múltiples usuarios y que tiene las siguientes características: | **Exigido** |  |
| Inteligencia artificial (AI) y capacidades de análisis de video, incluyendo reconocimiento de apariencia y tecnología de detección de movimiento no usual. | **Exigido** |  |
| Capacidades de búsqueda con opciones de marcadores, eventos, alarmas y miniaturas. | **Exigido** |  |
| Fácil integración con las cámaras instaladas de la marca Hanwha Techwin, modelo SND-6011R | **Exigido** |  |
| Permite la supervisión de video en vivo y grabado a través de redes IP inalámbricas desde dispositivos móviles basados en tecnología Apple o Android. | **Exigido** |  |
| Análisis de reconocimiento de matrículas (LPR). | **Exigido** |  |
| Recibe y actúa basado en eventos de puertas de sistemas de control de acceso, eventos de entrada de hardware y concesiones de acceso. | **Exigido** |  |
| Al integrarse con un sistema de control de acceso permite el desbloqueo de puertas directamente desde una vista de cámara. | **Exigido** |  |
| La función de verificación de identidad permite que las credenciales presentadas en el sistema de control de acceso se muestren dinámicamente en las vistas de cámara del sistema NVMS | **Exigido** |  |
| GENERALIDADES: Proporcionar una aplicación de software NVMS que se pueda instalar en cualquier hardware de plataforma abierta y no requiera multiplexor de hardware o tecnología de división de tiempo para video o audio. | **Exigido** |  |
| Capacidad de almacenamiento de grabación: ampliable sin licencias adicionales. | **Exigido** |  |
| Descompresión de video: descomprime el video H.264 a través de la tarjeta gráfica del propietario y la unidad de procesamiento gráfico. | **Exigido** |  |
| Proporcionar una solución de software de nivel empresarial que sea escalable desde un cliente, servidor y cámara hasta al menos: | **Exigido** |  |
| a. 100 servidores por Locación. | **Exigido** |  |
| b. 300 cámaras por servidor. | **Exigido** |  |
| c. Hasta 10.000 cámaras por sitio. | **Exigido** |  |
| d. Número ilimitado de conexiones concurrentes de cliente a una locación. | **Exigido** |  |
| e. Los números expresados pueden superarse dependiendo de la capacidad de ancho de banda de la red y el servidor. | **Exigido** |  |
| El servidor NVMS y las aplicaciones de software cliente pueden instalarse y ejecutarse en la misma computadora o en computadoras separadas. | **Exigido** |  |
| Compatibilidad de aplicaciones: El software deberá ser compatible con las siguientes aplicaciones: | **Exigido** |  |
| a. Aplicaciones de software de servidor: | **Exigido** |  |
| 1) Servicio de Servidor (Grabación de Video y Gestor de Base de Datos). | **Exigido** |  |
| 2) Servicio de puerta de enlace. | **Exigido** |  |
| 3) Servicio de análisis de video. | **Exigido** |  |
| 4) Servicio Web Endpoint. | **Exigido** |  |
| b. Aplicaciones de software de cliente que no requieran licenciamiento adicional: | **Exigido** |  |
| 1) Software Cliente para monitoreo, gestión y configuración de la plataforma de video. | **Exigido** |  |
| 2) Reproductor de Video. | **Exigido** |  |
| 3) Matriz virtual | **Exigido** |  |
| 4) Monitoreo de video en vivo, grabado y alarmas desde un dispositivo móvil. | **Exigido** |  |
| 5) Cliente Web basado en HTML5 | **Exigido** |  |
| 6. Idiomas: El software deberá soportar al menos los siguientes idiomas: | **Exigido** |  |
| a. Español | **Exigido** |  |
| b. Ingles | **Exigido** |  |
| Transmisiones seguras: El software deberá enviar datos de audio y video de manera segura mediante la transmisión de comandos y datos de control a través de TCP / IP mediante claves criptográficas basadas en SSL / TLS para evitar escuchas o manipulaciones indebidas. | **Exigido** |  |
| Controladores: admite la grabación y administración de fuentes de video y audio a través del uso de controladores estándar de la industria o mediante controladores específicos para un fabricante particular, incluyendo como mínimo los siguientes controladores mas no limitado a estos: | **Exigido** |  |
| a. Perfil S ONVIF. | **Exigido** |  |
| b. Perfil T ONVIF. | **Exigido** |  |
| c. Dispositivos de Video Analítica ya sea que estos estén integrados en las cámaras o se manejen mediante un servidor centralizado. | **Exigido** |  |
| d. Cámaras ONVIF 1.00, 1.01 y 1.02. | **Exigido** |  |
| Soporte de funcionalidad De-wrapping eliminando distorsiones de video en vivo y grabado en cámaras compatibles y equipadas con un lente Immervision Panomorph | **Exigido** |  |
| B. DESCUBRIMIENTO E IDENTIFICACION DE DISPOSITIVOS: Debe detectar dispositivos y sistemas en red mediante los siguientes métodos como mínimo | **Exigido** |  |
| 1. Detección Automática: | **Exigido** |  |
| a. los servidores, las fuentes de video y audio que están conectados a la misma red que el cliente se descubren automáticamente. | **Exigido** |  |
| b. Debe permitir la búsqueda de los servidores, las fuentes de video y audio que se ejecutan en un segmento de red diferente al del cliente y que pueden descubrirse buscando la dirección IP o el nombre de host del dispositivo. | **Exigido** |  |
| c. De Locación padre a Locación hijo, al iniciar sesión en una locación principal (padre), se descubren automáticamente las locaciones secundarias (hijos) configurados. | **Exigido** |  |
| Detección manual: permite que las instancias del servidor, las fuentes de video y audio, y los dispositivos de control de acceso sean descubiertos manualmente y visibles para los usuarios de una única estación de trabajo cliente. | **Exigido** |  |
| ALARMAS y EVENTOS: proporciona la capacidad de configurar y gestionar alarmas y eventos. | **Exigido** |  |
| 1. Definir los disparadores de eventos que están configurados para dar como resultado una alarma. | **Exigido** |  |
| 2. Generar alarmas como resultado de los siguientes tipos de eventos como mínimo, pero no solo limitado a estos: | **Exigido** |  |
| a. Detectar eventos que ocurren dentro del campo de visión de una cámara. | **Exigido** |  |
| b. Detectar la presencia de personas y/o vehículos. | **Exigido** |  |
| c. Detectar si se pierde la señal de audio o video y alertar al administrador del sistema. | **Exigido** |  |
| d. Actividad de puertas detectada por aplicaciones de control de Acceso | **Exigido** |  |
| e. Notificar a los usuarios de los errores del sistema. | **Exigido** |  |
| f. Recibir alarmas de sistemas de terceros (control de acceso, LPR, etc) y permitir su configuración para ser monitoreadas | **Exigido** |  |
| g. Detectar la activación de entradas digitales, que permitan la activación de salidas digitales desde: | **Exigido** |  |
| 1) Una tarjeta de entrada / salida. | **Exigido** |  |
| 2) Cámara IP compatible, codificador o sensor. | **Exigido** |  |
| 3) Sistemas integrados, incluyendo POS. | **Exigido** |  |
| 3. Recibir eventos a través del controlador ONVIF. | **Exigido** |  |
| 4. Configurar las operaciones de video resultantes. | **Exigido** |  |
| 5. Admitir mensajes del Protocolo simple de administración de red (SNMP) de los servidores y alertar a los usuarios. | **Exigido** |  |
| 6. Personalizar y reenviar las notificaciones de alarmas y eventos como mínimo a lo siguiente: | **Exigido** |  |
| a. Usuarios registrados en la aplicación cliente. b. Usuarios registrados en la aplicación móvil. c. Direcciones de correo electrónico preconfiguradas d. Entidades externas y software de terceros, como estaciones centrales de monitoreo y centros de llamadas. | **Exigido** |  |
| 7. Escalar las alarmas de un usuario o grupo de usuarios a otro, si la alarma no es reconocida en un intervalo de tiempo predeterminado. | **Exigido** |  |
| 8. Configurar notificaciones de correo electrónico como mínimo a lo siguiente: | **Exigido** |  |
| a. Notificar a los usuarios y administradores del sistema cuando ocurra un evento o un error de funcionamiento del sistema. b. Programar cuando se envían las notificaciones por correo electrónico. c. Incluir imágenes de la cámara en las notificaciones por correo electrónico. | **Exigido** |  |
| 9. Configura las notificaciones a centrales de monitoreo de alarmas con mínimo lo siguiente: | **Exigido** |  |
| a. Notificar a un servicio de monitoreo de la estación central cuando ocurra un evento o un error de salud del sistema. b. Incluir videoclips y/o imágenes de cámara por eventos como movimiento de cámara, eventos analítica o entradas digitales. | **Exigido** |  |
| 10. Brinda la posibilidad de enviar mensajes de conexión periódicos a centrales de monitoreo, o una notificación regular para confirmar la conexión del sistema y que no hay eventos importantes. | **Exigido** |  |
| 11. Supervisar eventos y alarmas en base a un horario configurable por el usuario. | **Exigido** |  |
| D. DISPARADORES DE EVENTOS: | **Exigido** |  |
| 1. Asigna acciones en respuesta a desencadenadores de eventos específicos. Las acciones de respuesta deberán incluir como mínimo lo siguiente pero no estar limitado a | **Exigido** |  |
| a. Acciones de notificación de usuario: 1) Mostrar mensaje en pantalla. 2) Enviar un correo electrónico. 3) Enviar notificación a la estación central de monitoreo. 4) Reproducir un sonido. | **Exigido** |  |
| b. Acciones de seguimiento: 1) Iniciar video en vivo. 2) Crear marcador de video. 3) Abrir una vista guardada. 4) Iniciar la transmisión en vivo en un monitor de matriz virtual. 5) Abrir un mapa en un monitor de matriz virtual. 6) Abrir una página web en un monitor de matriz virtual. | **Exigido** |  |
| c. Acciones del dispositivo: 1) Reiniciar la cámara. 2) Activar salida digital. 3) Desactivar salida digital. | **Exigido** |  |
| d. Acciones PTZ: 1) Ir a Preset. 2) Ir a Home Preset. 3) Ejecutar un patrón. 4) Activación de auxiliares 5) Desactivación de auxiliares | **Exigido** |  |
| e. Acciones de Alarma: 1) Disparar una alarma 2) Reconocer una alarma | **Exigido** |  |
| 2. Admite activadores de eventos condicionales según el estado de la entrada digital seleccionada. | **Exigido** |  |
| 3. Autentica a los usuarios antes de conceder acceso al sistema. | **Exigido** |  |
| 4. Proporciona derechos de acceso que se pueden asignar a cada usuario mediante grupo de usuarios. Los derechos de acceso deberán mínimo incluir lo siguiente: | **Exigido** |  |
| a. Ver imágenes en vivo: 1) Utilice los controles de PTZ. 2) Bloquee los controles de PTZ. 3) Activación de grabación manual 4) Activar salidas digitales. 5) Activación de Altavoces. | **Exigido** |  |
| b. Ver imágenes grabadas: 1) Exportar imágenes. 2) Archivar imágenes. 3) Crear marcadores de enseñanza. | **Exigido** |  |
| c. Gestionar vistas guardadas. | **Exigido** |  |
| d. Gestionar mapas. | **Exigido** |  |
| e. Gestionar páginas web. | **Exigido** |  |
| f. Gestionar monitores matriciales virtuales. | **Exigido** |  |
| g. Iniciar sesiones de colaboración. | **Exigido** |  |
| h. Gestionar sesiones de usuario. | **Exigido** |  |
| i. Escuchar micrófonos. | **Exigido** |  |
| j. Configurar cámaras: | **Exigido** |  |
| 1) Configurar ajustes generales. 2) Configuración de la red. 3) Configuración de imagen y configuración de pantalla. 4) Configura los ajustes de compresión y velocidad de imagen. 5) Configurar la configuración de la dimensión de la imagen. 6) Configurar los ajustes de detección de movimiento. 7) Configuración de la zona de privacidad. 8) Configuración de los ajustes de grabación manual. 9) Configuración de entrada y salida digital. 10) Configuración de los ajustes del micrófono. 11) Configuración de los ajustes del altavoz. 12) Configuración de ajustes de analítica 13) Configuración de enseñanza por ejemplos. | **Exigido** |  |
| k. Configuración de Sitios: | **Exigido** |  |
| 1) Nombre del Sitio. 2) Administrar el sitio. 3) Configuración de la vista del sitio. 4) Configuración de usuario y configuración de grupo. 5) Configuración de la sincronización de Active Directory. 6) Configurar la jerarquía corporativa. 7) Configurar los ajustes de gestión de alarmas. 8) Configuración de la configuración de transacciones POS. 9) Configurar los ajustes LPR. 10) Configuración de la configuración de correo electrónico. 11) Configurar la configuración del motor de reglas. 12) Ver los registros del sitio. 13) Conectar y desconectar dispositivos. 14) Ver la salud del sitio. | **Exigido** |  |
| l. Configurar servidores: | **Exigido** |  |
| 1) Administrar el servidor. 2) Configuración de los horarios de configuración. 3) Configuración de grabación y ajustes de ancho de banda. 4) Configuración de la gestión de almacenamiento. 5) Configuración de copia de seguridad. 6) Configuración del análisis del servidor. | **Exigido** |  |
| 5. Proporciona la capacidad de clasificar los derechos de acceso según la posición de un usuario dentro de una jerarquía configurada. | **Exigido** |  |
| a. Los usuarios clasificados solo pueden administrar cambios a los usuarios y grupos que están subordinados en la clasificación. b. La jerarquía corporativa se puede usar para imponer la autoridad de un sitio principal sobre la configuración de usuarios y grupos de uno o más sitios secundarios. | **Exigido** |  |
| 6. Crea familias de sitio. | **Exigido** |  |
| a. Un sitio secundario se puede conectar a un sitio principal con licencia apropiada. b. El sitio principal tendrá control sobre el permiso del usuario y la información de un sitio secundario. c. Si un usuario tiene acceso al sitio principal, los sitios secundarios se descubren automáticamente. | **Exigido** |  |
| 7. Admite múltiples credenciales para obtener acceso al sistema, que incluyen, entre otras: | **Exigido** |  |
| a. Importa miembros de grupos de Active Directory como usuarios en NVMS. 1) Sincroniza automáticamente los cambios realizados a los miembros en Active Directory con NVMS. 2) Agrega directamente a los usuarios importados de Active Directory a los grupos de permisos existentes. | **Exigido** |  |
| b. Permitir Importar roles desde la aplicación de Control de Acceso 1) Sincroniza automáticamente los cambios realizados a los roles de usuario en la aplicación de control de Acceso con NVMS. 2) Agrega directamente a los usuarios importados del control de acceso a los grupos de permisos existentes. 3) Los usuarios importados podrán controlar puertas dentro de NVMS. | **Exigido** |  |
| c. Utiliza las credenciales de Windows para autenticar a los usuarios. | **Exigido** |  |
| d. Acepta credenciales de usuario ingresadas en la base de datos de usuarios de NVMS. | **Exigido** |  |
| 1) Las credenciales cumplen con un requisito de complejidad de contraseña que es configurable. | **Exigido** |  |
| 8. Activar manualmente la salida digital como mínimo a través de lo siguiente: a. Un control de software preconfigurado. b. Un disparador físico que está conectado a un dispositivo de entrada / salida compatible. | **Exigido** |  |
| **SEGURIDAD:** | **Exigido** |  |
| Administrar y personalizar el acceso de los usuarios mínimo de la siguiente manera: | **Exigido** |  |
| 1. Permite a los administradores anular el acceso de los usuarios a un NVR si no hay suficientes licencias. 2. Configura el software del cliente para iniciar sesión automáticamente en varios sitios. 3. Configura el software del cliente para que cierre la sesión automáticamente de todos los sitios cuando la aplicación se deja inactiva. 4. Configura el software del cliente para guardar y restaurar automáticamente el diseño de la última ventana de visualización que uso el operador. 5. Establece el ancho de banda máximo de los datos de video transmitidos desde el servidor a la aplicación cliente. | **Exigido** |  |
| **PROCESAMIENTO Y COMPRESION DE VIDEO/AUDIO:** | **Exigido** |  |
| Admitir el almacenamiento y procesamiento de video y audio mínimo de la siguiente manera: 1. Grabar de forma nativa el audio y el video de la cámara sin transcodificación. 2. Sincronizar audio y video independientemente de la velocidad de fotogramas, la resolución o la tasa de bits. 3. Admitir los formatos de compresión de video estándar de la industria, que incluyen, como mínimo entre otros, los siguientes: a. JPEG2000. b. MJPEG. c. MPEG-4. d. H.264. | **Exigido** |  |
| **ADMINISTRACION DINAMICA DE FLUJOS DE VIDEO** |  |  |
| Realizar la administración dinámica de flujos de video mínimo de la siguiente manera: 1. Proporcionar un mecanismo de gestión de flujos de video de Alta definición. 2. Reduce el ancho de banda del sistema y el uso de almacenamiento al transmitir solo el video al cliente según lo requiera el Propietario. 3. El cliente debe comunicar la resolución máxima del monitor al servidor y el servidor actúa como un proxy de video y transmite la resolución de video requerida. 4. Organizar secuencias de videos de múltiples megapíxeles y solo transmitir la parte solicitada del flujo de video al cliente. 5. Extender el almacenamiento de video grabado al reducir dinámicamente la calidad del video grabado a lo largo del tiempo para que el video aún sea viable, pero use menos almacenamiento. a. Reduce la velocidad de imagen de video JPEG y JPEG2000 a la mitad o un cuarto de la velocidad de imagen original. b. Grabe un flujo de alta calidad y un flujo de baja calidad. 1) Capacidad de eliminar el flujo de alta calidad después de un período de tiempo determinado por el propietario. 6. Hacer que la gestión dinámica de video esté disponible para usuarios locales, usuarios remotos y dispositivos móviles. | **Exigido** |  |
| **REGISTRO DE EVENTOS:** |  |  |
| Mantener un registro de eventos y permitir a los usuarios utilizar eventos de registro como activadores para acciones de específicos. Los eventos registrados incluyen como mínimo lo siguiente: | **Exigido** |  |
| 1. Eventos del servidor: a. Aplicación del servidor iniciando. b. La aplicación del servidor se apaga. c. La aplicación del servidor terminó inesperadamente. d. Aplicación de servidor con pocos recursos. e. Error de instalación de la aplicación del servidor. f. La licencia expira pronto. g. Licencia expirada. h. Error de la base de datos. i. Error de inicialización de datos. j. Volumen de datos en falla k. Volumen de datos recuperado. l. Tamaño del volumen de datos reducido. m. Error de escritura de datos. n. Actualización de datos iniciada. o. Actualización de datos completada. p. Actualización de datos fallida. q. La recuperación de datos comenzó. r. Recuperación de datos se completado. s. Recuperación de datos fallida. t. Marcador guardado fallido. u. Conexión de red establecida. v. Conexión de red perdida. w. Correo electrónico enviar error. x. Evento de hardware del servidor. y. Archivado iniciado. z. Archivado completado. aa. Archivado interrumpido. bb. Conexión del servidor perdida. cc. Cola del servidor de Analítica llena. dd. Se perdió la conexión del servidor de análisis. | **Exigido** |  |
| 2. Eventos del dispositivo: | **Exigido** |  |
| a. Conexión creada. b. Conexión eliminada. c. Conexión creada al servidor en espera. d. Conexión eliminada del servidor en espera. e. Fallo de conexión. f. Conexión restaurada. g. Pérdida de paquetes de red inaceptable. h. Pérdida de paquetes de red aceptable. i. La detección de movimiento comenzó. j. La detección de movimiento terminó. k. Se inició el evento de análisis de video. l. Evento de analítica de video finalizado. | **Exigido** |  |
| m. Manipulación detectada. | **Exigido** |  |
| n. Grabación iniciada. | **Exigido** |  |
| o. Grabación finalizada. | **Exigido** |  |
| p. Grabación interrumpida. | **Exigido** |  |
| q. Se reanudó la grabación. | **Exigido** |  |
| r. Entrada digital activada. | **Exigido** |  |
| s. Entrada digital desactivada. | **Exigido** |  |
| t. Actualización de firmware iniciada. | **Exigido** |  |
| u. Actualización de firmware completada. | **Exigido** |  |
| v. Falló la actualización del firmware. | **Exigido** |  |
| w. Se ha detectado un firmware obsoleto. | **Exigido** |  |
| x. Evento definido por el usuario iniciado. | **Exigido** |  |
| y. Evento definido por el usuario finalizado. | **Exigido** |  |
| z. Presencia detectada. | **Exigido** |  |
| aa. La presencia terminó. | **Exigido** |  |
| bb. Tiempo de permanencia en presencia excedido. | **Exigido** |  |
| cc. El tiempo de permanencia de la presencia terminó. | **Exigido** |  |
| 3. Eventos del usuario: | **Exigido** |  |
| a. Inicio de sesión de usuario. b. Cierre de sesión del usuario. c. Se cambió la configuración del servidor. d. Se ha cambiado la configuración del sitio. e. Se ha cambiado la configuración del dispositivo. f. Dispositivo conectado. g. Dispositivo desconectado. h. Salida digital activada. i. Marcador de video añadido. j. Marcador de video actualizado. k. Marcador de video eliminado l. PTZ se movió. m. PTZ inactivo. n. Exportación realizada. o. Altavoz activado. p. Altavoz desactivado. q. Monitor de matriz virtual abierto. r. Mapa agregado. s. Mapa actualizado. | **Exigido** |  |
| t. Mapa eliminado. u. Vista añadida. v. Vista actualizada. w. Ver borrado. x. Página web añadida. y. Página web actualizada. z. Página web eliminada. aa. Vista del sitio actualizada. bb. Comando del teclado personalizado activado. | **Exigido** |  |
| 4. Eventos de alarma: | **Exigido** |  |
| a. Alarma reconocida. b. Alarma auto reconocida. c. Alarma activada. d. Alarma asignada. e. Alarma sin asignar. f. Alarma purgada. | **Exigido** |  |
| 5. Eventos de transacciones POS: | **Exigido** |  |
| a. Se inició la transacción POS. b. Transacción POS finalizada. c. Excepción de transacción POS. | **Exigido** |  |
| 6. Eventos de reconocimiento de matrículas: | **Exigido** |  |
| a. Se inició la detección de matrículas. b. Finalizó la detección de matrículas. c. Matrícula coincidente en lista de seguimiento. | **Exigido** |  |
| 7. Eventos de Control de Acceso: | **Exigido** |  |
| a. Acceso a la puerta denegado. b. Acceso a la puerta concedido. c. Puerta cerrada. d. Puerta forzada. e. Puerta forzada cerrada. f. Puerta abierta. g. Puerta cerrada. h. Puerta abierta. i. Coacción de la puerta j. Solicitud para salir en una puerta. k. La validación del certificado falló. | **Exigido** |  |
| I. GESTION DE ALMACENAMIENTO DE VIDEO: | **Exigido** |  |
| 1. Proporcionar como mínimo los siguientes niveles de administración de almacenamiento de video: a. Nivel 1: Video grabado directamente en el servidor local. b. Nivel 2: Video grabado mediante proceso de archivado para almacenamiento a largo plazo, en intervalos de mínimo 1 hora. c. Ad hoc: el video grabado en el servidor local, se puede archivar en una ubicación de almacenamiento definida por el usuario a demanda. | **Exigido** |  |
| 2. Admitir como mínimo las siguientes opciones de grabación de video y audio: | **Exigido** |  |
| a. Activar manualmente la grabación. b. Proporcionar la opción de grabación pre-evento y post-evento. c. Proporcionar la opción de grabación de cuadros de referencia en ausencia de eventos (grabación en tiempo lapsado). d. Crear agendas de grabación que se pueden definir individualmente para cada fuente de video. Incluye, pero no limitado a, las siguientes opciones de grabación: 1) Grabación continua. | **Exigido** |  |
| e. Grabación basada en eventos que se desencadena por lo siguiente: 1) Pixel o movimiento de objeto clasificados por analítica. 2) Entradas digitales. 3) Alarmas. 4) Transacciones POS. 5) Reconocimiento de matrículas. f. Horario diario y semanal personalizado. | **Exigido** |  |
| COPIA DE SEGURIDAD Y ARCHIVADO: | **Exigido** |  |
| 1. Programar el archivado de video grabado con eventos asociados a una carpeta local o unidad de red asignada. 2. Configuraciones de respaldo y configuración para cada servidor, incluyendo como mínimo lo siguiente: a. Configuración del sitio; Como usuarios / grupos, mapas y páginas web. b. Configuración del servidor, incluidas las conexiones de dispositivos. c. Capacidad de encriptar la copia de seguridad para mantener la seguridad de la información. 3. Restaurar la configuración de copia de seguridad y las configuraciones a un servidor nuevo o de reemplazo en un sitio. Admitir archivos de copia de seguridad de versiones anteriores a la actual. | **Exigido** |  |
| VIDEO ANALITICA: | **Exigido** |  |
| 1. Proporcionar detección de objetos clasificados configurables para cada dispositivo con capacidades de análisis de video de autoaprendizaje. | **Exigido** |  |
| a. Permite a los usuarios conectar fuentes de video individuales a canales de dispositivos de análisis. b. Permite a los usuarios configurar eventos basados en la detección de movimiento de objetos clasificados. c. Permite que los eventos de análisis de video configurados se usen como activadores de alarma y regla. d. Permite a los usuarios marcar objetos clasificados como una detección verdadera o falsa. 1) Transmite los datos recopilados a la fuente de video para mejorar la precisión del dispositivo de análisis de video. | **Exigido** |  |
| 2. Admite los siguientes tipos de eventos analíticos de video cuando son capturados por cámaras compatibles: | **Exigido** |  |
| a. Objetos en zona. b. Objeto merodeando. c. Objetos que cruzan la línea definida. d. Aparece el objeto o entra en el área. e. Objeto no presente en el área. f. Los objetos entran en el área. g. Los objetos salen del área. h. El objeto se detiene en el área. i. Se viola la dirección de viaje prevista. j. La escena cambia dramáticamente de una manera inesperada. | **Exigido** |  |
| L. RECONOCIMIENTO DE MATRICULAS AUTOMATICO (ALPR): es compatible con la operación de un sistema de reconocimiento de matrículas que incluye: | **Exigido** |  |
| 1. Definir la región de una imagen donde se realiza la detección de matrículas. 2. Almacenar las matrículas detectadas con datos de video. 3. Crear una lista de observación que se utiliza para crear eventos cuando se detectan placas específicas 4. Crear un número ilimitado de listas de observación. Cada lista de observación deberá soportar como mínimo 2 millones de matrículas. | **Exigido** |  |
| M. INTEGRACION CON EL SISTEMA DE CONTROL DE ACCESO | **Exigido** |  |
| 1. Aplicación de Control de Acceso: a. Admitir la conexión de red configurable a un dispositivo tipo servidor de control de acceso. b. Crear enlaces entre cámaras y puertas. c. Crear reglas activadas por acciones de puerta que dan como resultado acciones realizadas por el NVMS. d. Sincronizar a los usuarios del control de acceso para proporcionar acceso a las puertas. e. Proporcionar acceso de concesión para una puerta mientras monitorea el video. | **Exigido** |  |
| 2. Requisitos de integración de terceros: admite la integración a nivel de software con aplicaciones de terceros que utilizan el kit de desarrollo de software (SDK) o Servicio Web (Web Endpoint) del NVMS y proporciona como mínimo las siguientes características al software de terceros: | **Exigido** |  |
| a. Conexión: Autodescubrimiento de servidores, login y autenticación. b. Transmisión de video: descubra automáticamente cámaras conectadas, video en vivo y grabado (formato RAW o MJPEG; H.264 solo para aplicaciones de ventana). c. Superposiciones de video: muestre superposiciones sobre transmisión de video (cuadros de delimitación de objetos clasificados, detección de movimiento, nombre / ubicación de la cámara, marca de tiempo). d. re. Control PTZ: controle las cámaras PTZ (pan / tilt, zoom, presets, patrones, iris y bloqueo PTZ). e. Transmisión de audio: transmitir audio desde un sistema de terceros a una cámara NVMS (cámara a un sistema de terceros solo en aplicaciones con ventanas). | **Exigido** |  |
| f. Gestión de alarmas: enumerar, consultar, activar, asignar, reconocer y purgar alarmas. g. Gestión de eventos: enumerar, consultar, suscribirse para recibir notificaciones sobre eventos (cámara, servidor, administración, E / S digital, análisis de video, reconocimiento de matrículas, puntos de venta). h. Gestión de marcadores: Lista, consulta, crear, eliminar. i. Salida digital: Disparar salidas digitales. j. Archivar / Exportar: activar el archivado o exportar en formato de video nativo al NVMS o formatos de video / imagen genéricos, que incluyan como mínimo AVI, PNG, TIFF, JPEG. | **Exigido** |  |
| CONFIGURACION Y CONTROL PTZ: activa y configura el control PTZ en la interfaz RS-485 de una fuente de video. | **Exigido** |  |
| 1. Soportar mínimo los siguientes protocolos PTZ: a. American Dynamics Sensormatic. b. AXSYS. c. AXSYS DCU. d. Ernitec ERNA. e. Honeywell Diamond. f. JVC JCBP. g. Kalatel ASCII. h. Pelco D. i. Pelco p. j. TEB Ligne. k. Vicon extendió. l. Vicon normal. m. Videotec Legacy. n. Videotec MACRO. | **Exigido** |  |
| 2. Admitir cámaras con PTZ y proporcionar mínimo lo siguiente: a. Admite el control de PTZ mecánico, el iris y el enfoque, así como la configuración de presets y patrones. b. Proporciona la capacidad de nombrar presets PTZ. c. Admite la capacidad de crear recorridos de PTZ combinando un número establecido de ajustes preestablecidos que se ejecutan en orden o secuencia aleatoria. | **Exigido** |  |
| d. Admite la capacidad de centrar el campo de visión de una cámara PTZ haciendo clic en cualquier lugar de la imagen de video. e. Admite la capacidad de hacer clic y arrastrar para definir un área para que la cámara PTZ haga zoom y se centre mecánicamente. f. Admite el control de la visualización de la cámara PTZ mecánica y los controles auxiliares. g. Soporta bloqueo de controles PTZ. h. Permite a un usuario con un rango más alto anular un bloqueo de control PTZ. i. Admite el uso de un joystick USB para controlar las funciones PTZ. | **Exigido** |  |
| CAMBIAR PARAMETROS DE CALIDAD DE IMAGEN Y VELOCIDAD DE LA FUENTE DE VIDEO: | **Exigido** |  |
| 1. Brindar la posibilidad de cambiar los siguientes parámetros de calidad de imagen y velocidad de imagen para cada fuente de video de manera individual: a. Formato de transmisión de video. b. Sistema optimizado de registro de perfil o configuración manual. c. Intervalo de fotogramas clave. d. Transmisión secundaria para visualización en vivo. e. Configure la transmisión de video a una velocidad de imagen inferior cuando la escena está inactiva. f. Personalice el flujo primario y secundario en las cámaras compatibles. | **Exigido** |  |
| OPCIONES DE CONFIGURACION EN CLIENTES Y CAMARAS: | **Exigido** |  |
| 1. Brinda la posibilidad de cambiar mínimo las siguientes opciones de video admitidas en el cliente o la fuente de video: a. Cifrar los datos de configuración de la cámara si esta es compatible con dicha función b. Cambiar contraseñas de cámara desde la aplicación cliente. c. Cambiar configuración de exposición, iris, filtro IR, compensación de contraluz, ganancia, prioridad, nitidez, saturación, enfoque y balance de blancos para una fuente de video. | **Exigido** |  |
| d. Dimensiones de la imagen para una fuente de video. e. Permitir girar la imagen 90 °, 180 ° o 270 ° para una fuente de video. f. Agregar múltiples zonas de privacidad a una fuente de video para evitar que se vean y graben áreas en el campo de visión de la imagen. g. Establecer una duración máxima de grabación para la grabación activada manualmente para una fuente de video. | **Exigido** |  |
| **CARACTERISTICAS DE AUDIO:** | **Exigido** |  |
| 1. Proporcionar la capacidad de cambiar la entrada, salida, ganancia y volumen para una fuente de audio. 2. Soportar el uso de audio unidireccional y bidireccional. 3. Proporcionar la capacidad de vincular cualquier fuente de audio a cualquier fuente de video. a. Capacidad de vincular múltiples fuentes de audio a una única fuente de video. b. Capacidad de vincular múltiples fuentes de video a una única fuente de audio. 4. Proporcionar la capacidad de sincronizar audio y video en la reproducción. 5. Admite la capacidad de desviar el video visualizado a una velocidad de cuadros más baja o una resolución de imagen más baja si no hay suficiente ancho de banda de red o potencia de procesamiento. a. Esta acción no afectará la grabación de video. b. Esta acción no afectará las exportaciones de video. | **Exigido** |  |
| **INTERFAZ DE USUARIO:** | **Exigido** |  |
| 1. Admitir la posibilidad de compartir la visualización de la ventana de la aplicación en una sesión conjunta con otros usuarios para realizar investigaciones colaborativas. 2. Proporcionar un árbol del sistema que incluya mínimo fuentes de video, mapas, vistas guardadas y páginas web en la pestaña de monitoreo de video. a. La pantalla del árbol del sistema se puede configurar. b. El árbol del sistema se puede organizar en carpetas virtuales que se representan como sucursales dentro del sitio. c. Los usuarios pueden tener acceso a elementos individuales o a carpetas completas dentro del árbol del sistema. | **Exigido** |  |
| 3. Admitir una cantidad ilimitada de monitores utilizados para monitorear secuencias de audio y video conectadas a una sola estación de trabajo. a. Muestra todas las fuentes de video conectadas al sistema. b. Admite la capacidad de arrastrar y soltar elementos del árbol del sistema en el área de monitoreo de video. c. Admite la supervisión de secuencias de audio y video en vivo y grabadas simultáneamente en el mismo monitor. d. Permite ver la misma transmisión de video en vivo o grabada en diferentes niveles de zoom y áreas de interés. e. Admite la capacidad de cambiar de video en vivo a video bajo demanda para una reproducción instantánea de video grabado recientemente. | **Exigido** |  |
| f. Admite la creación de vistas ilimitadas con diseños únicos de secuencias de video. g. Admite la capacidad de alternar entre vista de mosaico y pantalla completa. h. Admite la capacidad de guardar la configuración de pantalla. i. Admite la capacidad de desplazarse por las vistas (recorrido de guardia) en función de un intervalo específico configurable. j. Admite el monitoreo de video en vivo o grabado de 1 a 64 transmisiones de video simultáneamente en un solo monitor. | **Exigido** |  |
| k. Admite la visualización de secuencias de videos mínimo en los siguientes diseños estándar: Pantalla completa. 1) 2 x 2. 2) 3 x 3. 3) 4 x 4. 4) 5 x 5. 5) 6 x 6. 6) 8 x 8. 7) 1 + 5. 8) 1 + 7. 9) 1+ 12. 10) 2 + 8. l. Proporciona herramientas para construir diseños personalizados de monitoreo de video. | **Exigido** |  |
| 4. Proporcionar un módulo de aplicación de Virtual Matrix: a. Admite el control remoto de múltiples pantallas de monitor, conectadas a la red b. Muestra transmisiones de video simultáneas en pantallas de monitores conectados desde múltiples sitios. | **Exigido** |  |
| 5. Muestra superposiciones sobre imágenes de video. a. Se superponen automáticamente las opciones funcionales que cambian según el modo de transmisión de video y la compatibilidad del dispositivo. Las superposiciones funcionales deben incluir mínimo, las siguientes: | **Exigido** |  |
| 1) Botón para activar manualmente la grabación de video / indicador de grabación de video. 2) Botón para activar la salida digital. 3) Botón para capturar instantáneas de video. 4) Botón para cerrar el flujo de video. 5) Botón para reservar una porción de la pantalla para el video de alarma. 6) Botón para habilitar el audio. 7) Botón para visualizar transacciones POS. 8) Botón para maximizar la visualización de video. 9) Botón para activar la búsqueda de una sola cámara. 10) Botón para otorgar acceso en una puerta vinculada. 11) Permitir hacer clic en el cuadro delimitador de un objeto clasificados para iniciar la búsqueda de apariencia. 12) Controles de PTZ. | **Exigido** |  |
| b. Superposiciones de información que incluyen, entre otras, las siguientes: 1) Nombre de la cámara. 2) Ubicación de la cámara. 3) Marca de tiempo de reproducción con la opción de mostrar la hora del dispositivo o la hora local. 4) Marca de tiempo en vivo con la opción de mostrar la hora del dispositivo o la hora local. 5) Indicador de grabación. 6) Actividad de movimiento. 7) Actividad de análisis de video con cuadros delimitadores codificados por colores alrededor de objetos en movimiento clasificando como mínimo humanos y/o vehículos. 8) Matrícula detectada. | **Exigido** |  |
| 6. Apoyar las operaciones de gestión de alarmas a través de la interfaz de monitoreo de video. Incluyendo, pero no limitado a: a. Pestaña designada para revisar alarmas. b. La interfaz admite la visualización secuencial de alarmas. c. La interfaz admite la clasificación de alarmas por: 1) Prioridad. 2) Tiempo de activación. 3) Estado. | **Exigido** |  |
| d. La interfaz admite el filtrado de alarmas por estado en la siguiente prioridad: 1) Asignado a mí. 2) Alarmas activas (sin asignar). 3) Alarmas asignadas a otros. 4) Alarmas reconocidas. | **Exigido** |  |
| e. Admite la capacidad de asignar alarmas al usuario. f. Apoya la capacidad de reconocer alarmas. g. Soporta la capacidad de marcar las alarmas. h. Designar una o más regiones en el área de visualización de video para mostrar el video directamente vinculado a las alarmas o reglas activadas. 1) Admite la capacidad de reconocer alarmas del área de visualización de video designada. | **Exigido** |  |
| 7. Admite la capacidad de crear un mapa que represente la ubicación física de las cámaras y otros dispositivos en todo el sistema de vigilancia. a. Permitir crear mapas como mínimo a partir de imágenes en los siguientes formatos: 1) JPEG. 2) BMP. 3) PNG. 4) GIF. | **Exigido** |  |
| b. Tamaño mínimo de la imagen del mapa: 3000 por 3000 o 9 MP c. Proporcionar mapas con la capacidad de hacer lo siguiente: 1) Crear una jerarquía de mapas interconectados. 2) Arrastrar y soltar los objetos en el árbol del sistema durante la configuración del mapa. 3) Haga clic y visualice los objetos del mapa. 4) Arrastrar y soltar una fuente de video del mapa en el área de visualización de video. 5) Mostrar un área preestablecida de la fuente de video seleccionada. d. Las cámaras en un mapa se resaltan cuando se activa una alarma vinculada a la cámara. e. Proporcionar iconos de mapa configurables. | **Exigido** |  |
| **REPRODUCCION DE AUDIO Y AUDIO/VIDEO GRABADO:** | **Exigido** |  |
| 1. Soporta la reproducción de video y audio grabados. a. Reproducción hacia adelante y hacia atrás de video y audio grabados a velocidades variables. b. El video y el audio se reproducen de manera sincrónica cuando las fuentes de video y audio están vinculadas. c. La reproducción del video grabado incluye el video archivado para el almacenamiento a largo plazo. | **Exigido** |  |
| 2. Brinda la posibilidad de solicitar una autenticación de segundo usuario antes de que se muestre el video grabado. | **Exigido** |  |
| 3. Proporcionar los siguientes métodos para navegar el video grabado: a. Calendario seleccionable. b. Línea de tiempo horizontal, desplazable: 1) La línea de tiempo enumera todas las fuentes de video mostradas. 2) La línea de tiempo resalta el movimiento y los eventos en el video grabado. | **Exigido** |  |
| 3) El video archivado para almacenamiento a largo plazo se identificará en la línea de tiempo. 4) Admite una línea de tiempo que puede mostrarse en incrementos de un cuarto de segundo. 5) Admite una línea de tiempo que puede sincronizar el video que se muestra en varias pestañas en el mismo punto en el tiempo. c. Buscar. | **Exigido** |  |
| 4. Admite la búsqueda de videos grabados con los siguientes parámetros seleccionables: a. Hora. b. Fecha. c. Fuente de vídeo. d. Alarma. e. Tipo de evento. | **Exigido** |  |
| f. Búsqueda visual basada en un área de imagen predefinida, o miniatura de una imagen: 1) Las miniaturas pueden basarse en una región de imagen completa o en un área preseleccionada. 2) Las miniaturas se pueden apilar para admitir una búsqueda secundaria automática cuando se mira un gran intervalo de tiempo de video. | **Exigido** |  |
| g. Movimiento de píxeles en áreas definidas por el usuario. h. Detección de movimiento de objetos clasificados en fuentes de análisis de video compatibles. i. Transacciones en puntos de venta. j. Eventos de detección de matrículas. k. Marcadores | **Exigido** |  |
| 5. Debe Soportar búsquedas de personas basadas en su apariencia a. Capaz de buscar una persona o vehículo de interés en el video grabado de varias cámaras en un sitio y devolver posibles coincidencias. | **Exigido** |  |
| 1) Mejore automáticamente la búsqueda de personas utilizando caras detectadas en escenas de cámaras compatibles. 2) Las cámaras compatibles con capacidades de análisis de video de autoaprendizaje que están conectadas a un NVR deberán poder devolver posibles coincidencias para la búsqueda. | **Exigido** |  |
| b. Capaz de iniciar la búsqueda desde el video grabado en la aplicación Cliente. c. Admite la revisión de resultados de búsqueda y la confirmación de coincidencias correctas. | **Exigido** |  |
| d. Soporta la edición de parámetros de búsqueda incluyendo: 1) Cámaras incluidas en la búsqueda. 2) Rango de tiempo para la búsqueda. e. Admite la reproducción de resultados de búsqueda, incluyendo: 1) Video grabado asociado a resultados individuales. 2) Reproducción secuencial del video grabado asociado con coincidencias confirmadas como correctas. f. Soporta la exportación de video asociado a resultados, incluyendo: 1) Video grabado asociado con uno o más resultados seleccionados. 2) El video grabado asociado con las coincidencias confirmadas como correctas. g. Admite la creación de marcadores para resultados, que incluyen: 1) Uno o más resultados seleccionados. 2) Confirmado para ser los partidos correctos. | **Exigido** |  |
| **MARCADORES:** | **Exigido** |  |
| 1. Proporciona un registro de mantenimiento y un registro de auditoría de todos los errores y eventos del sistema. | **Exigido** |  |
| 2. Admite la creación de marcadores para video y audio grabados. Los marcadores pueden ser: a. Aplicable a múltiples fuentes de video. b. Se muestra en la línea de tiempo durante la reproducción. c. Se utiliza como criterio de búsqueda para video y audio grabados. Los criterios de búsqueda pueden incluir, pero no se limitan a: 1) Nombre. 2) Descripción. 3) creador de marcadores. d. Admite la protección de un marcador para que los datos de audio y video asociados nunca se sobrescriban. e. Admite marcadores privados que solo son visibles para el usuario que los designó como privado y para el administrador del sistema. | **Exigido** |  |
| EXPORTACION DE VIDEO: admite la capacidad de exportar video y proporciona las siguientes opciones: | **Exigido** |  |
| 1. Exporta video grabado en los siguientes formatos: a. Nativo. b. JPEG c. PNG. d. TIFF. e. AVI. f. Impresión. | **Exigido** |  |
| 2. Exporta audio grabado en los siguientes formatos: a. WAV. b. Nativo. c. AVI. | **Exigido** |  |
| 3. Exporta un fotograma fijo de video como se muestra en el área de vista previa de video: a. Nativo. b. JPEG. c. PNG. d. TIFF. | **Exigido** |  |
| 4. Formato nativo exportado de la siguiente manera: a. Firma digital en el video y el audio grabados con cifrado de 256 bits para que el video pueda ser autenticado con fines probatorios. b. Capaz de exportar video desde una o varias transmisiones de cámara simultáneamente. c. Soporta la exportación de múltiples segmentos de video de diferentes períodos de tiempo. d. Admite la revisión de audio y video exportados o respaldados en un reproductor dedicado. e. Admite la reproducción de clips exportados en tiempo secuencial sincronizado. f. Admite la reproducción de varios clips en orden continuo y secuencial. | **Exigido** |  |
| g. Admite la exportación de video en tasas de cuadros más bajas que las grabadas originalmente. h. Admite la exportación de un área designada desde el campo de visión grabado de la cámara. i. Admite la reexportación a formatos nativos u otros formatos compatibles. j. Proporciona un registro de la fuente de video con los siguientes metadatos: 1) Modelo de cámara. 2) Versión de firmware. 3) Ubicación. 4) dirección MAC. 5) Número de serie. 6) Resolución. | **Exigido** |  |
| **PROCESO DE ACTUALIZACION DE LA VERSION DEL NVMS:** proporcionar un proceso para actualizar las versiones del VMS | **Exigido** |  |
| 1. La actualización del software del servidor no requerirá acceso físico a los servidores. a. Iniciar actualizaciones desde la interfaz del cliente. b. Todos los servidores y clientes conectados recibirán una distribución de la actualización de la nueva versión. 1) El administrador puede activar manualmente la actualización de cada servidor. c. El usuario podrá monitorear el progreso de la actualización desde la interfaz del cliente. | **Exigido** |  |
| 2. La actualización del número de dispositivos conectados o la actualización a la versión empresarial solo requiere un cambio en la clave de licencia. | **Exigido** |  |
| 3. Durante el proceso de actualización, El NVMS continuará registrando y pasando las alarmas, el video y los datos operativos a los usuarios, monitores y aplicaciones de terceros. | **Exigido** |  |
| 4. La actualización de una versión a otra ocurre sin tener que desinstalar la aplicación y la versión anterior. | **Exigido** |  |
| 5. Actualice automáticamente la fuente de audio o video conectado. | **Exigido** |  |
| 6. Solicitar automáticamente al usuario que actualice la aplicación del cliente si está desactualizada con respecto al software del servidor. | **Exigido** |  |
| 7. Las actualizaciones de una misma versión y edición no tendrán un costo adicional sin importar cuantos reléase se liberen de esta. | **Exigido** |  |
| 8. Se deberá contar con una figura de soporte 7x24 por parte del fabricante de la solución. Proporcionando como mínimo los siguientes medios de comunicación: a. Chat b. Correo Electrónico para la creación automática de un caso de soporte c. Vía Telefónica | **Exigido** |  |
| **CONSIDERACIONES GENERALES DE HARDWARE:** | **Exigido** |  |
| 1. El NVMS deberá permitir ser configurado para que se ejecute como un servicio que se inicie automáticamente cuando se encienda el servidor o la estación de trabajo. | **Exigido** |  |
| 2. El NVMS deberá permitir a los usuarios monitorear y administrar el sistema desde: a. Una aplicación de cliente único para monitorear video y audio en vivo y grabado. b. Una sola ventana para administrar todas las conexiones del sistema. c. Una sola pestaña para monitorear el estado general del sistema y los sitios conectados en las relaciones entre sitios padre y sitios hijo. d. Cada cliente con acceso a una red local o distribuida. | **Exigido** |  |
| 3. El NVMS deberá proporcionar múltiples niveles de redundancia del sistema: a. Agrupar y sincronizar hasta 100 servidores en un sitio unificado. 1) En el caso que se produzca una falla en el servidor, el sistema puede continuar ejecutándose y permitir que otros servidores asuman las tareas fallidas del servidor. b. Administración centralizada del sistema: 1) Los detalles de la configuración del sitio y del servidor se replican en cada servidor del sitio, no se aceptarán sistemas con esquemas de bases de datos centralizados. 2) Los sitios pueden organizarse en una relación jerárquica entre padres e hijos, donde los padres siempre pueden controlar la configuración del sitio secundario. 3) Conecte una fuente de video o audio a múltiples servidores para lograr una grabación redundante. 4) Permitir crear una conexión de conmutación por error (failover) para una fuente de video o audio entre servidores en un sitio. Se deberá soportar configuraciones de failover N:1 y N:M | **Exigido** |  |
| 4. El NVMS proporciona la capacidad de cambiar el nombre de todos los sitios, servidores y fuentes de audio y video. | **Exigido** |  |
| 5. Software NVMS debe proporcionar soporte para los siguientes sistemas operativos como mínimo a. Windows 7. b. Windows 8.1. c. Windows 10. d. Windows Server 2012/2012 R2. | **Exigido** |  |
| **Cámara IP Tipo domo** | **Cantidad: 08 (ocho)** | **Exigido** |  |
| Estas cámaras serán del tipo mini domo para ambientes internos con IR automático y con lente adecuado en función del área de visualización. | **Exigido** |  |
| Las cámaras admitirán rango de resoluciones de vídeo de 1920 (H) x 1080 (V) o superior, independientemente de la complejidad de la escena. | **Exigido** |  |
| La cámara deberá ser capaz de proporcionar secuencias de video en H.264 y Motion JPEG simultáneas, independientemente configuradas (multi-streams) 30 fps como mínimo. | **Exigido** |  |
| Es necesario que las cámaras manejen tecnología de transmisión de video eficiente preservando la integridad total de la imagen mediante la compresión sin pérdida de calidad, al tiempo que administra de forma eficiente el ancho de banda y el almacenamiento. | **Exigido** |  |
| La cámara deberá contar con la funcionalidad de detección de movimiento con umbral y sensibilidad seleccionables. | **Exigido** |  |
| La cámara podrá contar con alimentación PoE (Power Over Ethernet) o entrada de alimentación auxiliar según corresponda. | **Exigido** |  |
| La cámara deberá está preparada y contar con los accesorios para su correcto montaje en los distintos entornos en el interior o exterior según corresponda. | **Exigido** |  |
| **Capacidades** | **Exigido** |  |
| Sensor de imagen CMOS de barrido progresivo 1/ 2,8” o inferior. | **Exigido** |  |
| La cámara deberá contar con un rango dinámico amplio (WDR) de al menos 100 dB con 30 fps. | **Exigido** |  |
| La cámara deberá ser del tipo lente fijo 2,8 mm, F/1.2, IR corregida. | **Exigido** |  |
| La cámara deberá proporcionar iluminación uniforme en la oscuridad a 0,00 lux o inferior (F 1.2) en modo monocromo y 0,01 lux o inferior (F 1.2) en modo color. | **Exigido** |  |
| La cámara deberá contar con control de parpadeo seleccionable entre 50/60 Hz, compensación de contraluz ajustable, control de día/noche manual y automático. | **Exigido** |  |
| Compatible con ONVIF perfil S. | **Exigido** |  |
| IR con cobertura mínima de 10 metros. | **Exigido** |  |
| Streaming de video: Varios flujos H.264 y Motion JPEG. | **Exigido** |  |
| Detección de movimiento: Objetos de píxeles. | **Exigido** |  |
| Control electrónico del obturado: Automático, manual | **Exigido** |  |
| Control del diafragma: Automático, Manual. | **Exigido** |  |
| Control de día/noche: Automático, Manual. | **Exigido** |  |
| Balance de blancos: Automático, Manual. | **Exigido** |  |
| Compensación de contraluz: ajustable. | **Exigido** |  |
| **Seguridad** | **Exigido** |  |
| Protección por contraseña, cifrado HTTPS, registro de acceso de usuario, autenticación basada en el puerto 802.1x. | **Exigido** |  |
| **Protocolos Compatibles** | **Exigido** |  |
| La cámara incorporará soporte de al menos IPv4, HTTP, HTTPS, DNS, NTP, RTSP, RTCP, RTP, TCP, UDP, IGMP, ICMP, DHCP, entre otros. | **Exigido** |  |
| **Protocolos de transferencia** | **Exigido** |  |
| RTP/UDP, multidifusión RTP/UDP, RTP/RTSP/TCP, RTP/RTSP/HTTP/TCP, RTP/RTSP/HTTPS/TCP, HTTP | **Exigido** |  |
| **Interface de Red** | **Exigido** |  |
| La cámara estará equipada con un puerto Ethernet 100BASE-TX | **Exigido** |  |
| **Protocolos de administración de dispositivos** | **Exigido** |  |
| SNMP v2c, SNMP v3 | **Exigido** |  |
| **Almacenamiento interno** | **Exigido** |  |
| Ranura SD/SDHC/SDXC | **Exigido** |  |
| **Certificaciones** | **Exigido** |  |
| Seguridad UL 60950-1 - Evaluación de impacto IK10 o similar | **Exigido** |  |
| Emisiones electromagnéticas FCC Sección 15 Subsección B Clase B o similar | **Exigido** |  |
| Inmunidad electromagnética EN 55024 o similar | **Exigido** |  |
| **Condiciones de Operación.** | **Exigido** |  |
| Temperatura de funcionamiento; | **Exigido** |  |
| 0°C a 50°C (0 °C +50 °C) | **Exigido** |  |
| Temperatura de almacenamiento; | **Exigido** |  |
| Menos 20°C a más 65°C (-20 °C a +65 °C) | **Exigido** |  |
| Humedad Relativa: 0 -95 % sin condensación | **Exigido** |  |
| **Protocolos de administración de dispositivos** | **Exigido** |  |
| SNMP v2c, SNMP v3 | **Exigido** |  |
| **Zonas de privacidad** | **Exigido** |  |
| Hasta 24 zonas como mínimo. | **Exigido** |  |
| **Garantías** | **Exigido** |  |
| El oferente deberá presentar junto con su oferta carta de autorización firmada por un representante del fabricante con potestades sobre nuestra región, por la cual se autorice al oferente a proveer los equipos ofertados. | **Exigido** |  |
| Los técnicos de la empresa oferente deberán estar certificados por el fabricante. Los profesionales deberán residir en Paraguay, así como ser personal estable y formar parte de la nómina de la empresa oferente. | **Exigido** |  |
| Garantía escrita del fabricante de al menos 3(tres) años | **Exigido** |  |

**Ítem 6: Sistema de Control de Acceso**

|  |  |  |  |
| --- | --- | --- | --- |
| **ESPECIFICACIONES TÉCNICAS MÍNIMAS** | | | |
| **Nombre del Bien o Servicio Conexo** | **Descripción Técnica** | **Mínimo Exigido** | **El bien ofertado cumple con las especificaciones requeridas (SI/NO)** |
| **Marca:** | **Especificar** | |  |
| **Modelo:** | **Especificar** | |  |
| **Procedencia:** | **Especificar** | |  |
| **Cantidad:** | **01 (uno)** | **Exigido** |  |
| **Descripción** | **Sistema de control de acceso** | **Exigido** |  |
| **Control de Acceso** | 1. El sistema de control de acceso físico (PACS) deberá estar disponible en las siguientes presentaciones: | **Exigido** |  |
| a. Dispositivo tipo appliance de control de acceso físico que combina hardware más software de tipo empresarial, el cual estará preinstalado y habilitado para que el sistema pueda implementarse de manera inmediata con la mínima configuración. | **Exigido** |  |
| b. Dispositivo tipo appliance de control de acceso físico virtualizado componente de solo software. El cual podrá ser instalado en un ambiente virtualizado que posea el cliente y deberá estar como mínimo certificado para funcionar sobre plataformas VMWare. | **Exigido** |  |
| 2. El PACS deberá cumplir con los estándares de IT y así mismo tener las funcionalidades completas de una solución de control de acceso convencional. | **Exigido** |  |
| 3. El dispositivo tipo appliance del PACS tendrá basado su sistema operativo en Linux y una estructura de directorio compatible con LDAP. | **Exigido** |  |
| 4. El dispositivo tipo appliance del PACS deberá soportar: a. Paquetes de actualización y mantenimiento del sistema operativo. b. Actualización de claves de licenciamiento. | **Exigido** |  |
| 5. El dispositivo tipo appliance del PACS deberá utilizar infraestructura de una red TCP/IP estándar para comunicaciones entre: a. Todos los dispositivos de control de acceso físico en un ambiente de múltiples dispositivos (appliance). b. Hardware de controladores empresariales Inteligentes para instalación en campo. c. Estaciones de trabajo basadas en navegador Web. | **Exigido** |  |
| 6. El dispositivo tipo appliance del PACS deberá tener como mínimo los siguientes componentes preinstalados: a. Sistema operativo Linux b. Estructura de directorio (base de datos) OpenLDAP para el almacenamiento de información relacionada con los titulares de credenciales (identidades o cardholders). c. Estructura de directorio (base de datos) PostgreSQL para el almacenamiento de las transacciones del sistema. d. Servidor Web integrado. e. Aplicación de software del sistema de control de acceso físico (PACS). | **Exigido** |  |
| 7. Todas las configuraciones, mantenimiento e interacción con el sistema serán llevadas a cabo sin la directa intervención del usuario con el sistema operativo o la estructura de directorio (Base de Datos). | **Exigido** |  |
| 8. Todos los dispositivos tipo appliance del PACS deberán actuar como un repositorio centralizado para todas las configuraciones y actividad del sistema. a. La interfaz de trabajo y configuración del dispositivo tipo appliance del PACS deberá ser únicamente vía navegador web. b. El uso de servidores de bases de datos separados no será aceptado. | **Exigido** |  |
| 9. El dispositivo tipo appliance del PACS deberá proveer acceso basado en navegador web, sin la necesidad de requerir una estación de trabajo dedicada. Como mínimo deberá el sistema ser capaz de soportar los siguientes navegadores web: a. Mozilla Firefox b. Google Chrome c. Apple Safari d. Internet Explorer | **Exigido** |  |
| 11. El dispositivo tipo appliance del PACS deberá soportar medidas de seguridad para todas las comunicaciones e información de la solución soportando como mínimo: a. Las comunicaciones de red hacia o desde el dispositivo tipo appliance, así como también de las estaciones de trabajo basadas en navegador web deberán soportar SSL 128 bit de encripción o superior. b. Las copias de seguridad de la configuración del sistema deberán estar encriptadas usando AES como mínimo. c. Las copias de seguridad deberán poderse almacenar como mínimo en las siguientes opciones: i. Dispositivo de almacenamiento USB. ii. Un directorio compartido de Windows o un directorio compartido sobre la red. iii. A servidores seguros SCP (Secure Copy Protocol). d. Todas las contraseñas requeridas, para registrarse en el PACS deberán estar encriptadas dentro de la estructura de base de datos OpenLDAP que soporta el sistema. | **Exigido** |  |
| La arquitectura del PACS deberá tener un esquema de toma de decisiones distribuida mediante el uso de los controladores empresariales inteligentes de campo. a. La arquitectura del PACS deberá mantener funcionalidades completas durante los periodos de tiempo en el cual se presenten perdidas de comunicación entre el dispositivo tipo appliance y el dominio de controladores inteligentes de hardware del sistema. b. Durante la falla de comunicación los controladores empresariales inteligentes (hardware control de acceso) del sistema deberán llevar un registro completo de eventos correspondientes de actividad del sistema, así como un registro de auditoria los cuales deberán ser transmitidos al dispositivo tipo appliance del PACS una vez las comunicaciones sean restauradas y estén funcionando de manera normal. | **Exigido** |  |
| 13. La arquitectura del sistema de control de acceso físico (PACS) deberá soportar la adición de: a. Al menos 2048 lectores por dispositivo tipo appliance. b. Al menos 5060 entradas y 5060 salidas digitales. c. Al menos 512 controladores empresariales inteligentes por dispositivo tipo appliance. d. Dispositivos tipo appliance adicionales. | **Exigido** |  |
| 14. Cuando múltiples dispositivos tipo appliance del PACS, sean implementados el sistema deberá soportar la replicación automática de la información de la base de datos, además de: a. Soportar una configuración uno a uno. b. No requerir de un servidor central de bases de datos dedicado. c. Habilitar la replicación de configuración y titulares de tarjeta de manera automática a todos los dispositivos tipo appliance del sistema. | **Exigido** |  |
| El PACS deberá soportar una arquitectura de failover tipo hot standby. Donde frente a la falla de funcionamiento de un dispositivo tipo appliance del PACS un segundo appliance este en capacidad de actuar como respaldo del primero detectando la falla de este y asumiendo el control del sistema de manera automática. | **Exigido** |  |
| 16. El PACS deberá soportar la integración con sistemas de terceros mediante el uso de interfaces de software. Dentro de estos sistemas deberán estar como mínimo, pero no solo limitados a estos: a. Integración con bases de datos Oracle RDBMS b. Integración con bases de datos Windows SQL c. Integración con bases de datos LDAP. d. El sistema deberá estar en capacidad de extraer información de estas bases de datos y enviar eventos a sistemas externos en tiempo real en formato XML. | **Exigido** |  |
| 17. El PACS deberá proveer un esquema de licenciamiento basado en una clave de software que reside en cada dispositivo tipo appliance y esta clave controlara las características y/o componentes que hacen parte del sistema. | **Exigido** |  |
| 18. El PACS deberá soportar como mínimo la conexión de hasta 50 conexiones concurrentes de estaciones cliente. Esquemas de licenciamiento individual por cada conexión concurrente de un cliente no serán aceptadas. | **Exigido** |  |
| El PACS deberá soportar como mínimo los siguientes idiomas en su interfaz gráfica a. Ingles b. Español | **Exigido** |  |
| **B. Hardware** |  |  |
| 1. Plataforma tipo appliance hardware y software en uno. a. CPU: Mínimo Intel Quad Core 3.0GHz con 8 MB de cache b. RAM: Mínimo 6 GB a 1600M c. NIC: Mínimo dos interfaces 1 Gbps d. OS: Linux e. HDD: Mínimo 1 TB @ 7200rpm f. Capacidades mínimas requeridas por appliance: i. Puertas / Lectoras: 2048 ii. Entradas de Alarma: 5060 iii. Salidas de relevo: 5060 iv. Tarjetas habientes: 500.000 v. Conexiones concurrentes de clientes Web: 50 vi. Histórico de eventos en línea 150.000.000 | **Exigido** |  |
| **C. Software** | **Exigido** |  |
| **Funcionalidad para Control de Alarmas** | **Exigido** |  |
| 1. Atributos de Eventos y Alarmas, el PACS deberá permitir a los administradores configurar cada alarma y evento para que sea comunicado a un visor de alarmas. a. La ventana de Lista de eventos deberá listar todas las alarmas y eventos junto con el tipo de evento asociado y la fuente del objeto que es el responsable por la generación de la alarma o evento b. Una vez un operador se registre y acceda el visor de alarmas toda la cola de alarmas y eventos deberá ser reportada. | **Exigido** |  |
| 2. Por cada alarma y evento del sistema, el administrador deberá tener la opción de: | **Exigido** |  |
| a. Renombrar la alarma o evento de sus parámetros de fábrica. b. Renombrar, cuando aplique, el nombre del retorno a un estado normal de la alarma o evento. c. Asignar un tipo de evento que del configurado de fabrica a una alarma o evento. d. Mostrar la alarma o evento en el visor de alarmas. | **Exigido** |  |
| e. Enmascarar la alarma o evento que se esté visualizando en el monitor de alarmas. f. Mostrar instrucciones en texto que permitan guiar al operador de cómo debe responder a una determinada alarma. g. Automáticamente, enviar un correo electrónico a un recipiente de correo especifico. h. Tener la visualización de alarmas basado en un orden de prioridad como también de los eventos de retorno a estado normal. Un mínimo de 99 prioridades deberá ser soportadas. | **Exigido** |  |
| i. Configurar una prioridad de una alarma o evento, así como al evento de retorno a normal. j. Poder relacionar video a alarmas o eventos, para que automáticamente sea mostrado el video en vivo suministrado por la cámara asociada con el dispositivo que genero la alarma o evento. k. Deberá almacenar la información de las alarmas o eventos para posteriores revisiones. l. Crear diferentes agendas que permitan habilitar y ser asignadas a diferentes tipos de alarmas. m. Crear una agenda para habilitar/deshabilitar eventos de manera global, los cuales deben incluir, pero no estar limitados a: i. Derivación o no de puertas. ii. Denegación de credenciales masivas (aseguramiento de emergencia). | **Exigido** |  |
| 3. Registro de Eventos y Alarmas, todas las alarmas y eventos en el PACS deberá registrarse de fabrica en el almacenamiento interno del dispositivo tipo appliance en una estructura de registro preestablecida. | **Exigido** |  |
| 4. Tipos de Alarmas y Eventos, el sistema de control de acceso físico deberá permitir la creación de alarmas y eventos. Estos tipos deberán contener como mínimo los siguientes parámetros de configuración, pero no estar limitados a estos. a. Prioridad b. Instrucciones en Texto c. Agenda para enmascaramiento y desenmascaramiento d. Almacenamiento en la estructura de registro. e. Reporte f. Notificaciones a correo electrónico | **Exigido** |  |
| 5. Sincronización de Alarmas y Eventos, el PACS deberá soportar la sincronización de alarmas y eventos que se reporten en múltiples visores de alarma. De tal forma que cuando una alarma o evento es reconocido por un operador este sea reportado de la misma forma en todos los visores de alarmas del sistema. | **Exigido** |  |
| 6. Reporte de Alarmas basado en Agendas, cada alarma del sistema deberá tener la opción de asociarle su propia agenda que le permita reportar la misma en un horario especifico. | **Exigido** |  |
| 7. Instrucciones de Texto para Alarmas y Eventos, el sistema de control de acceso físico deberá permitir a cada alarma y evento asociarle un mensaje de texto el cual deberá contener como mínimo 240 caracteres. | **Exigido** |  |
| **Funcionalidad para Control de Accesos** | **Exigido** |  |
| 1. Grupos de Acceso: estos deberán consistir en la combinación de lectoras de tarjeta con horarios. Cada grupo de acceso se compondrá del número necesario de lectoras que existan en el sistema y a este se le podrá asignar una única agenda. Una lectora de tarjetas deberá tener la habilidad de pertenecer a múltiples grupos de acceso de ser necesario. El PACS permitirá a un titular de tarjeta acceder a áreas seguras basado en: | **Exigido** |  |
| a. Lector de tarjeta donde se presenta la credencial de acceso. b. Hora c. Dia d. El PACS deberá soportar como mínimo de: i. 16 grupos de acceso por cada controlador inteligente de hardware del sistema. ii. Los grupos de acceso deberán soportar nombres convencionales de 50 caracteres alfanuméricos. iii. Los grupos de acceso se podrán asignar de forma individual a un titular de tarjeta por cada controlador inteligente de hardware del sistema y se podrán seleccionar hasta un mínimo de 8 en total. | **Exigido** |  |
| 2. Agendas: el PACS deberá soportar la creación de agendas y estas servirán como plantillas para la aplicación de parámetros incluyendo como mínimo los siguientes, pero no solo limitados a estos: | **Exigido** |  |
| 1. Grupos de Acceso 2. Enmascaramiento de Dispositivos 3. Modos de dispositivo. | **Exigido** |  |
| a. El sistema de control de acceso físico deberá soportar como mínimo 255 agendas y cada agenda deberá estar en capacidad de asignarle uno de al menos tres modos de operación | **Exigido** |  |
| i. Encendido, la agenda estará activa 7x24 todos los días de la semana. ii. Apagado, la agenda nunca estará activa iii. Escaneo, La agenda estar activa durante los intervalos de tiempo asignados. | **Exigido** |  |
| b. Cada agenda deberá tener la opción de asignarle un intervalo predeterminado. Cada intervalo permitirá asignarle un día de la semana especifico y se le podrán asignar hasta 8 tipos de festivos diferentes como mínimo. El mínimo de intervalos soportados por agenda deberá ser de 10. | **Exigido** |  |
| c. Estas agendas deberán poderse descargar a los controladores inteligentes de hardware para que estos realicen un procesamiento local y toma de decisiones. | **Exigido** |  |
| d. Las agendas deberán soportar nombres convencionales de mínimo 50 caracteres alfanuméricos. | **Exigido** |  |
| 3. Festivos: El sistema de control de acceso físico (PACS) deberá permitir especificar fechas o rango de fechas para ser definidas como festivos. a. El sistema de control de acceso físico (PACS) deberá soportar como mínimo 255 festivos. b. Un festivo deberá estar habilitado para que se le asignen hasta 8 diferentes tipos de festivos diferentes. c. Los siguientes parámetros del sistema podrán ser afectados de forma temporal, aunque no deberán estar limitados a solo estos: i. Modos de Operación de un Lector de tarjetas. ii. Derechos de acceso de un titular de tarjeta. iii. Enmascaramiento de agendas. d. El sistema de control de acceso físico deberá soportar un calendario embebido que asista en la configuración de los festivos. e. Los festivos deberán soportar nombres convencionales de hasta 50 caracteres alfanuméricos como mínimo. | **Exigido** |  |
| 4. Opciones de Puerta: El sistema de control de acceso físico (PACS) deberá permitir como mínimo las siguientes opciones para ser definidas en las puertas del sistema durante su configuración: | **Exigido** |  |
| a. Especificar que la puerta es una puerta activa. | **Exigido** |  |
| b. Especificar la operación en modo fuera de línea en caso de que la puerta pierda comunicación con el controlador inteligente de hardware. | **Exigido** |  |
| c. Especificar un filtro de puerta forzada que reduzca las falsas alarmas para las puertas cuando se cierran y existe un rebote de está brindando un tiempo de espera de al menos 3 segundos para el cierre de la puerta de tal forma que no se genere un evento de alarma por puerta forzada. | **Exigido** |  |
| d. El sistema deberá permitir un tiempo de apertura extendido independiente al normal para facilitar el acceso a personas con algún tipo de discapacidad en su movilidad y así evitar la generación de una falsa alarma por puerta abierta en el sistema. | **Exigido** |  |
| e. El tiempo de apertura extendido para una puerta deberá poderse definir en segundos y hasta un intervalo configurable de al menos 32.767 segundos | **Exigido** |  |
| f. La funcionalidad de tiempo de apertura extendido para una puerta deberá poderse asignar a: i. Puertas ii. Tarjeta Habiente | **Exigido** |  |
| g. El sistema deberá soportar el acceso a puerta basado en un código de Amenaza (Duress Code), de tal forma que el titular de la tarjeta digite su número de PIN habitual más un digito adicional que permita la apertura de la puerta de manera normal, pero reportando esa acción específica como una alarma. | **Exigido** |  |
| h. Este código de amenaza (Duress Code), debe poderse habilitar para que funcione en los modos: i. Tarjeta y PIN. ii. Tarjeta o PIN. iii. Solo PIN. | **Exigido** |  |
| i. El sistema frente al reporte de un evento de código de amenaza (Duress Code) debe estar en capacidad de denegar el acceso a un nuevo titular de tarjeta que intente ingresar y generar una alarma que reporte la solicitud de acceso y su denegación en el visor de alarmas. | **Exigido** |  |
| j. El sistema debe permitir definir el modo de operación del mecanismo de retención (strike) de la puerta en al menos los siguientes: i. El mecanismo de retención de la puerta permanece activo durante todo el tiempo. ii. El mecanismo de retención se apaga después que la puerta ha sido cerrada. iii. El mecanismo de retención se desactiva tan pronto la puerta está abierta. iv. El mecanismo de retención es deshabilitado durante una solicitud de salida (REX) | **Exigido** |  |
| k. El tiempo extendido de activación del mecanismo de retención de puerta (Strike) debe ser de mínimo 255 segundos. | **Exigido** |  |
| l. El sistema de control de acceso físico (PACS) debe permitir la opción de acceso a una puerta mediante la modalidad de presentar dos tarjetas validas en el lector, en un intervalo no menor a 10 segundos para que un acceso sea autorizado. | **Exigido** |  |
| m. En el caso que por algún motivo la puerta no posea un sensor de apertura, que monitoree si la puerta fue abierta o no durante un acceso valido. El sistema de control de acceso físico (PACS) debe permitir un modo de operación que registre la puerta como usada frente a un acceso autorizado y este evento deberá ser reportado como un evento al visor de alarmas. | **Exigido** |  |
| n. El sistema debe poseer un mecanismo de configuración de pre-alarma por puerta abierta, de tal forma que este permita definir un tiempo que permita activar una alarma audible que avise que la puerta está abierta para que el titular de tarjeta la cierre, antes que sea generada y visualizada una alarma por puerta abierta en el visor de alarma. El tiempo de pre-alarma debe ser configurable en segundos hasta un mínimo de 65534 segundos. | **Exigido** |  |
| o. El sistema de control de acceso físico (PACS) debe permitir establecer como mínimo los siguientes modos de operación de una puerta: i. Solo Tarjeta. ii. Tarjeta y PIN iii. Tarjeta o PIN iv. Asegurada v. Desasegurada i. Código de Sitio ii. Al final de una agenda de anulación, la puerta deberá regresar a su modo de operación estándar. | **Exigido** |  |
| p. El sistema de control de acceso físico deberá permitir asignar el atributo a una puerta para trabajar en modo cifrado en el cual un titular de tarjeta puede intentar acceder a un área digitando el número de su credencial en un lector de tipo teclado (keypad). | **Exigido** |  |
| q. El PACS deberá brindar la posibilidad de establecer un umbral máximo de intentos permitidos al digitar un PIN erróneo en un lector de teclado (keypad). Una vez este umbral sea superado deberá existir un evento que reporte dicha anomalía mediante una alarma en el visor de alarmas. | **Exigido** |  |
| r. La interfaz gráfica del PACS debe incluir botones que permitan controlar el estado operacional de una puerta y deberá incluir como mínimo los siguientes: i. Deshabilitar ii. Asegurar iii. Desasegurar iv. Permitir un acceso v. Restaurar vi. Enmascarar un evento de puerta abierta vii. Desenmascarar un evento de puerta abierta viii. Enmascarar un evento de puerta forzada ix. Desenmascarar un evento de puerta forzada. | **Exigido** |  |
| s. El PACS deberá suministrar una interfaz gráfica que permita ver el resumen y estado de todas las puertas del sistema de la tal forma que por cada puerta del sistema se muestre como mínimo la siguiente información: i. Nombre de la puerta ii. Modo de operación actual de la puerta iii. El estado actual de la puerta incluyendo estados como puerta abierta, puerta forzada, estados de enmascaramiento. | **Exigido** |  |
| t. La interfaz gráfica de resumen y estado de puertas deberá permitir el filtrar puertas o grupos de puertas como un criterio de búsqueda para facilitar la visualización de la información por parte del operador. | **Exigido** |  |
| u. El PACS deberá soportar múltiples formatos de tarjetas y a nivel de los controladores inteligentes de hardware estos deberán soportar como mínimo 8 formatos de tarjeta incluidos, pero no limitados a: i. Wiegand. ii. Banda Magnética. | **Exigido** |  |
| v. El PACS soportara cualquier formato estándar de la industria que use: i. Un número de tarjeta. ii. Un código de sitio. iii. Una combinación de códigos de emisión. iv. Tarjetas con un número máximo de 19 dígitos | **Exigido** |  |
| 5. Cerraduras Inalámbricas: El PACS deberá soportar y como mínimo, pero no limitado a los siguientes modelos: a. ASSA ABLOY Aperio b. Schlage AD400 | **Exigido** |  |
| 6. Resistencias de Final de Línea: El PACS debe permitir establecer una configuración de resistencias de final de línea a las entradas de alarma. Estas configuraciones de final de línea deben incluir como mínimo: | **Exigido** |  |
| a. Estados de Normalmente abierto y normalmente cerrado definibles de manera independiente para botones de egreso y contactos magnéticos. | **Exigido** |  |
| b. Estados de supervisión o no supervisión, definibles de manera independiente para botones de egreso y contactos magnéticos. | **Exigido** |  |
| c. 4 configuraciones de resistencias de final de línea (EOL) totalmente personalizables. | **Exigido** |  |
| d. Las opciones de configuración de resistencias de final de línea deberán permitir umbrales altos y bajos de resistencia y soportar como mínimo los siguientes estados: i. Inactivo ii. Activo iii. Falla a tierra iv. Abierto v. En corto circuito | **Exigido** |  |
| 8. Antipassback: el sistema de control de acceso físico deberá soportar características de control de áreas incluyendo, pero no limitadas a: | **Exigido** |  |
| a. Política Dura de Antipassback, esta requiere que cada credencial sea usada para salir o entrar a un área específica. Por tanto, cada puerta debe necesariamente tener tanto lector de entrada como de salida. En caso de que una credencial reporte una violación de antipassback el sistema no permitirá el acceso al titular de la tarjeta y será reportado como un evento al visor de alarmas. | **Exigido** |  |
| b. Política Suave de Antipassback, esta requiere que cada credencial sea usada para salir o entrar a un área específica. Por tanto, cada puerta debe necesariamente tener tanto lector de entrada como de salida. En caso de que una credencial reporte una violación de antipassback el sistema permitirá el acceso al titular de la tarjeta y será reportado como un evento al visor de alarmas. | **Exigido** |  |
| c. Antipassback temporizado, esta funcionalidad permitirá definir un límite de tiempo el cual una vez expire dejará de comportarse como un área controlada con una política de antipassback duro a un área controlada con una política de antipassback suave. | **Exigido** |  |
| d. Control de Dos personas, esta funcionalidad restringe a que dos credenciales autorizadas sean presentadas en un intervalo menos a 10 segundos mínimo para poder entrar o salir. | **Exigido** |  |
| e. Antipassback temporizado basado en Puerta, esta funcionalidad permite la configuración de antipassback en una puerta que solo posee un solo lector, de tal forma que la puerta mantiene un seguimiento de cada credencial que entra al área y no permite que esa misma credencial ingrese dos veces a menos que ya se haya cumplido el tiempo de Antipassback previamente configurado. | **Exigido** |  |
| f. Antipassback temporizado basado en Credencial, esta funcionalidad permite rastrear una credencial y las puertas por las cuales ha tenido acceso. Después que una credencial ha ganado el acceso a una puerta especifica esta deberá acceder una segunda puerta o esperara hasta que el tiempo de Antipassback se cumpla para nuevamente tener acceso a esa primera puerta. | **Exigido** |  |
| g. El sistema deberá soportar como mínimo 127 áreas de antipassback por cada dispositivo tipo appliance del PACS. | **Exigido** |  |
| h. El sistema deberá permitir anidamiento de áreas, el cual estará definido por un mínimo de 64 lectores de tarjetas de entrada y salida. Sin perder la capacidad de tener áreas independientes todo esto combinado con una política de antipassback duro. | **Exigido** |  |
| i. Las áreas deberán poderse definir de manera lógica simplemente definiendo en cada lector a que área da acceso y de cual área da salida. | **Exigido** |  |
| j. Funcionalidad de un solo paso libre a una credencial especifica. | **Exigido** |  |
| k. Característica de “Perdón” que le permitirá dar a una credencial un solo acceso libre permitiendo al PACS mover esa credencial de un área a otra sin importar su actual estatus de antipassback. | **Exigido** |  |
| 9. Control y Conteo de Ocupación: Esta funcionalidad deberá permitir al sistema restringir el número de credenciales que pueden estar presentes en un área en un momento especifico. Dentro de las características mínimas a soportar por esta funcionalidad están: | **Exigido** |  |
| a. Debe poderse definir como mínimo hasta 250.000 credenciales que pueden estar en área específica. | **Exigido** |  |
| b. Una vez se haya alcanzado un límite de ocupación para aceptar una nueva credencial en el área será necesario que al menos una de las credenciales que están reportadas como ocupando el área salgan de la misma. | **Exigido** |  |
| c. A cada a la cual se le desee aplicar el control de ocupación podrá ser definida hasta por 64 lectores de entrada / salida. | **Exigido** |  |
| d. Múltiples áreas con control de ocupación podrán ser definidas en el sistema. | **Exigido** |  |
| 10. Retardo de Entrada y Salida: Esta funcionalidad le deberá permitir al sistema configurar retardos de tiempo a cualquier entrada del sistema, de tal forma que se evite reportar la activación de una entrada siempre que no se alcance el límite de tiempo establecido. Los modos de operación mínimos soportados para esta funcionalidad serán: | **Exigido** |  |
| a. Entrada sin enclavamiento, cuando una entrada es activada, esta alarma no será reportada hasta que el retardo de ingreso no expire. Si la entrada permanece activa una vez expire el tiempo de retardo de entrada la alarma será reportada. Si expirado el tiempo la entrada no está activa la alarma no será reportada. | **Exigido** |  |
| b. Entrada con enclavamiento, cuando una entrada es activada esta no será reportada hasta que el retardo de ingreso no expire. En caso de que la entrada no se haya colocado en un estado de enmascarada para el momento en el que el retardo de ingreso expire la alarma será reportada. Si la entrada es enmascarada para cuando expire el retardo de ingreso la alarma no será reportada. | **Exigido** |  |
| c. Retardo de salida, aplica para entradas de alarma que han sido previamente enmascaradas, de tal forma que si la entrada se activa y se cumple el tiempo límite de salida la alarma será reportada. En caso contrario de no estar activa la entrada y expirado el tiempo de retardo de salida la alarma no será reportada. | **Exigido** |  |
| d. El PACS deberá soportar como mínimo un retardo en la entrada o salida de 65.535 segundos. | **Exigido** |  |
| Enlaces de Entradas/ Salidas / Eventos: esta funcionalidad permitirá al sistema de control de acceso físico que mediante una entrada, salida o evento el controlador inteligente de hardware pueda localmente disparar múltiples grupos de acciones de manera autónoma sin tener que depender del dispositivo tipo appliance del PACS. Cada controlador inteligente de hardware deberá soportar como mínimo 100 grupos de acciones y cada grupo deberá como mínimo soportar 30 acciones. Estas acciones deberán incluir, mas no estar limitadas a: a. Activar una salida de relevo. b. Enmascarar / Desenmascarar una entrada de alarma. c. Establecer el modo de operación de un lector de tarjetas. d. Activar o desactivar una agenda. | **Exigido** |  |
| 12. Funcionalidad de gestión de identidad: El PACS ofrecerá una funcionalidad integrada de gestión e inscripción de la identidad como parte de la funcionalidad del sistema central. | **Exigido** |  |
| a. El módulo de Gestión de Identidad e Inscripción de la aplicación no debe ser escrito por una fuente de terceros. | **Exigido** |  |
| b. Importación de datos: el PACS deberá tener la capacidad de importar registros de identidad y su imagen asociada en un formato JPEG estándar. | **Exigido** |  |
| c. Los registros de identidad deben poder precargarse antes de la implementación o agregarse en cualquier momento después de la implementación. | **Exigido** |  |
| d. El PACS proporcionará una utilidad de importación única preconfigurada, utilizando archivos estándar de valores separados por comas (.csv) que permitirán la importación de información de identidad basada en los campos de datos enviados de fábrica. | **Exigido** |  |
| e. Inscripción de identidad: el PACS permitirá la inscripción individual de identidades. Cada Identidad permitirá el ingreso de campos obligatorios y opcionales. | **Exigido** |  |
| f. Para las identidades que tienen acceso a la aplicación PACS, se deben definir los siguientes parámetros de seguridad durante el proceso de inscripción: i. Cuenta de usuario ii. Contraseña de la cuenta iii. Tiempo de espera de no actividad | **Exigido** |  |
| g. El PACS utilizará permisos de basado en roles. | **Exigido** |  |
| h. Los roles serán asignados durante la inscripción. El rol de la identidad determinará sus grupos de acceso: i. A qué lectores de tarjetas tienen acceso ii. Qué horarios de acceso a esos lectores de tarjetas está permitido | **Exigido** |  |
| i. Se creará una credencial y se asignará durante la inscripción. Cada credencial debe incluir, pero no limitarse a: i. Una identificación de placa ii. Se admitirá un mínimo de una identificación de identificación de 19 dígitos. iii. Número en relieve según sea necesario iv. El código PIN se asignará según sea necesario v. Fecha de activación y desactivación. vi. Configuración asociada para Antipassback según sea necesario | **Exigido** |  |
| j. Los parámetros de credenciales opcionales incluirán, pero no se limitarán a: i. Agregar un token a un grupo durante la inscripción. ii. Un grupo puede tener una configuración predefinida de roles y políticas que impulsará la configuración de la información de identidad. | **Exigido** |  |
| k. Caducidad de la credencial por no uso. La credencial se puede configurar para que caduque si no se utiliza dentro de un determinado período de tiempo. Los parámetros incluirán, pero no se limitarán a: | **Exigido** |  |
| i. En todo el sistema para cada credencial ii. Parámetros variables por individuo iii. Las personas físicas pueden quedar exentas del vencimiento. | **Exigido** |  |
| l. Durante la inscripción, la imagen de la identidad se capturará o cargará desde un formato de archivo JPEG y se asignará una plantilla de distintivo. | **Exigido** |  |
| n. Deberá admitir la importación de la fotografía y la huella dactilar biométrica de la tarjeta inteligente emitida por el gobierno que cumple con FIPS-201. | **Exigido** |  |
| o. El PACS permitirá la suspensión de credenciales si el número de serie del certificado de la tarjeta se encuentra en una lista designada, que incluye, entre otros: i. Lista de revocación de certificados (CRL) ii. Si el FASC-N está en la lista de tarjetas canceladas por la TSA (CCL). | **Exigido** |  |
| p. El PACS admitirá las credenciales PIV, TWIC, CAC y FRAC. | **Exigido** |  |
| 13. Re-emisión de credenciales: El Operador podrá desactivar la credencial existente marcándola como: i. Perdida ii. Robado | **Exigido** |  |
| a. El PACS podrá utilizar la información de identidad y la foto existentes para la nueva credencial. b. El proceso no requerirá la reinscripción del titular de la credencial. c. El proceso de reemisión deberá automáticamente: i. Eliminar los derechos de acceso del token desactivado. ii. Habilite esos mismos derechos en el nuevo token. iii. Enviar automáticamente los cambios apropiados a los controladores empresariales inteligentes. | **Exigido** |  |
| 14. Base de datos de identidad: cada identidad tendrá un registro único en la estructura de directorios de Open LDAP. a. La estructura del directorio LDAP debe incluir el uso y la definición de campos y formularios definidos por el usuario. b. Los campos definidos por el usuario se pueden usar con todas las búsquedas de identidad en todo el PACS | **Exigido** |  |
| 15. Eliminación de identidades: A los administradores de niveles más altos se les debe dar la capacidad de: a. Eliminar identidades b. Eliminar Identidades de forma masivas, capacidad de eliminar un grupo de identidades, basado en un conjunto de búsqueda definido por el usuario. | **Exigido** |  |
| 16. Asignar grupos de acceso: el PACS permitirá a los administradores asignar grupos de acceso a los roles. a. A continuación, se asignará un rol a una identidad durante la inscripción. b. Cada Identidad puede tener hasta 8 grupos de acceso asignados a su registro por controlador empresarial inteligente a través de la asignación de uno o más Roles a su registro. | **Exigido** |  |
| 17. Las modificaciones o asignaciones de grupos de acceso: se descargarán automáticamente a los controladores empresariales inteligentes adecuados: a. Sin intervención del operador. b. Se completa como una comunicación push inmediatamente después de que se guarda un registro del titular de la tarjeta. Programados, no se aceptan lotes actualizados. | **Exigido** |  |
| 18. El PACS debe admitir un formulario de Vista de grupo de acceso que permita a los operadores ver: a. Todos los roles que han sido asignados a una identidad b. Qué grupos de acceso están asociados con el Rol c. A qué puertas tiene acceso una identidad | **Exigido** |  |
| 19. Roles: el PACS debe admitir una metodología de permiso basada en roles que se utilizará junto con las identidades. a. Los roles se asignarán a Identidades para determinar el acceso de la puerta y el acceso a la aplicación del sistema. b. Se podrán asignar varios roles a una identidad. i. Se puede definir una relación padre / hijo, por rol. ii. No se requerirá la duplicación de información de rol para múltiples roles. c. Cada rol tendrá una fecha de inicio y finalización definida. d. Permitir la asignación de roles de forma temporal. e. Los roles se pueden activar o desactivar manualmente mediante el uso de una casilla de verificación. f. Cada Rol constará de cualquier combinación de los siguientes componentes que determinarán qué Roles puede asignar un Operador a otras Identidades durante la inscripción: i. Grupos de acceso ii. Asignaciones de delegación iii. Asignaciones de roles | **Exigido** |  |
| 20. Dispositivo de captura de imágenes: el PACS admitirá cámaras basadas en IP para la captura de fotos y formatos TWAIN vía USB. a. El Operador podrá ver una imagen en vivo en la pantalla de la Identidad para moverla a una postura o posición adecuada antes de congelar la imagen. b. Si el Operador no está satisfecho con la imagen capturada, podrá volver a una vista en vivo y congelar una nueva imagen. c. Los ajustes de configuración para cámaras IP, así como la visualización de una imagen fija y en vivo de una persona, serán configurables por el usuario. | **Exigido** |  |
| 21. Captura de fotos: el PACS admitirá la captura de fotos mediante el uso de una cámara basada en IP o una cámara USB. a. El Operador podrá ver una imagen en vivo en la pantalla de la Identidad para moverla a una postura o posición adecuada y luego podrá congelar la imagen. b. Si el Operador no está satisfecho con la imagen capturada, podrá volver a una vista en vivo y congelar una nueva imagen. | **Exigido** |  |
| 22. Además, y opcionalmente, el PACS admite la capacidad de importar fotos JPEG estándar de la industria desde cámaras digitales u otras fuentes de captura de imágenes. | **Exigido** |  |
| 23. El PACS permitirá que la foto capturada se recorte mediante el uso del mouse para definir la ventana de recorte. Solo la información dentro de la ventana de recorte se guardará y almacenará en la estructura del directorio. a. Las imágenes se asociarán con la Identidad y se almacenarán en el directorio OpenLDAP. | **Exigido** |  |
| 24. Fechas de activación y desactivación de la Credencial: el PACS debe admitir las fechas de activación y desactivación de todas las credenciales creadas. | **Exigido** |  |
| a. Una credencial tendrá la capacidad de configurarse para activarse en una fecha futura desde el momento de la creación. b. Cuando una credencial alcanza su fecha / hora de desactivación, el PACS desactivará automáticamente los derechos de acceso asociados con esa credencial. c. Todos los derechos de acceso de una credencial se eliminarán después de la fecha de desactivación. d. En caso de que la Identidad se autorice nuevamente para el acceso, los nuevos derechos de acceso serán aplicables a la misma credencial, y no se requerirá la reemisión. | **Exigido** |  |
| 25. Rastro de auditoría de Credenciales: el PACS debe mantener un registro en línea de todas las credenciales emitidas a una identidad. a. Para cada registro, los detalles se registrarán, incluidas las fechas de activación y desactivación, el estado de la credencial y la identificación de la credencial. | **Exigido** |  |
| 26. Códigos de emisión de Credenciales: el PACS debe admitir un código de emisión de 2 dígitos como mínimo. | **Exigido** |  |
| 27. Códigos PIN: el PACS admitirá códigos PIN de hasta 8 dígitos. a. Cada titular de credenciales en el PACS tendrá la capacidad de elegir un PIN para asociarse a su registro. | **Exigido** |  |
| b. El PIN del titular de la credencial podrá modificarse si se compromete el código PIN original. c. Una identidad debe poder estar exenta de los requisitos de PIN dentro del sistema. | **Exigido** |  |
| 28. Opciones de credenciales: el PACS debe admitir las opciones de credenciales físicas precodificadas según el estándar de la industria, que incluyen: a. Credenciales compuestas tales como tarjetas de PVC b. Credenciales de proximidad que incluyen tecnología dual de PVC que incluye tecnología de banda magnética y de proximidad c. Credenciales Inteligentes de contacto. d. Credenciales MiFare e. Credenciales DESFIRE f. Credenciales HID iClass | **Exigido** |  |
| 29. Información del último acceso: último punto de entrada del titular de la credencial. a. Se mostrará en el formulario de identidad principal. b. Junto con un sello de fecha / hora para cuando ocurrió la entrada. c. Si el titular tiene varias credenciales, el formulario de credenciales también mostrará el último punto de entrada con el sello de fecha / hora para cada credencial en posesión del titular. | **Exigido** |  |
| 30. Última modificación del registro de identidad: el PACS mostrará la fecha y la hora de la última modificación a ese registro de identidad del formulario de identidad principal. | **Exigido** |  |
| 31. Múltiples credenciales activas: el PACS permitirá que las identidades tengan múltiples credenciales activas asociados con su registro. a. Se puede asignar un mínimo de 25 credenciales activos a una Identidad. | **Exigido** |  |
| 32. Impresión de credenciales a doble cara: el PACS permitirá la impresión en ambas caras de una credencial. | **Exigido** |  |
| 33. Revocar acceso a credenciales: el PACS permitirá a los operadores revocar los privilegios de acceso de un titular de credenciales actualizando el estado de la credencial. | **Exigido** |  |
| a. Una credencial con acceso revocado dejará de funcionar inmediatamente en todos los lectores de tarjetas. | **Exigido** |  |
| 34. Capacidades de búsqueda: el PACS tendrá la capacidad de buscar identidades por a. Nombre de pila, b. Apellido c. Identidad d. Campo de credencial en el sistema. | **Exigido** |  |
| 35. El PACS permitirá múltiples búsquedas de Identidad / credencial basadas en campos usando con lógica AND / OR. Los filtros incluirán, pero no se limitarán a: a. Es igual a b. Comienza con c. Termina con d. Contiene | **Exigido** |  |
| 36. Generador de lista de selección: el PACS incluirá un generador de lista de selección que permite a los administradores definir las opciones de selección del operador que aparecen en las listas de selección del formulario de identidad. Cada lista de selección tendrá un número ilimitado de selecciones predefinidas. | **Exigido** |  |
| 37. El PACS admitirá los campos estándar de Identidad y Credencial: a. Apellido b. Nombre de pila c. Segundo nombre d. ID del sistema externo e. Dirección f. Ciudad g. Estado | **Exigido** |  |
| h. Número de código postal i. Teléfono j. Teléfono del trabajo k. Dirección de correo electrónico l. Título m. Departamento | **Exigido** |  |
| n. División o. Locación p. Edificio q. Modificación del último registro r. Estado s. Tipo t. Fecha de emisión u. Iniciar sesión v. contraseña | **Exigido** |  |
| w. Confirmación de contraseña x. Temporizador de inactividad y. Última puerta de acceso z. Fecha en que accedió a la última puerta i. Foto ii. Número en relieve iii. Número interno iv. PIN v. Estado de la Credencial vi. Nivel de emisión vii. Fecha de activación viii. Fecha de Desactivación. | **Exigido** |  |
| 38. Actividad de transacción: el PACS debe proporcionar un formulario que enumere la actividad de la transacción más reciente asociada con una identidad, sin tener que ejecutar un informe. La información provista deberá incluir: a. Actividad de transacción b. Hora y Fecha c. Credencial utilizada. | **Exigido** |  |
| Campos definidos por el usuario: el PACS admitirá la capacidad de agregar ampos adicionales al formulario de registro de una identidad. a. Se podrán agregar hasta 10 formularios definidos por el usuario. b. Cada campo definido por el usuario recibirá un nombre / etiqueta de campo y se definirá como uno de los siguientes tipos de campo: i. Cadena de Caracteres ii. Valor entero iii. Valor booleano iv. Valor tipo fecha c. Hasta 300 campos definidos por el usuario estarán disponibles. d. Los campos definidos por el usuario se pueden usar con todas las búsquedas de Identidad en todo el PACS. | **Exigido** |  |
| 40. Herramienta de diseño de Credenciales: el PACS debe admitir una herramienta que permita la creación personalizada de diseños de distintivos. | **Exigido** |  |
| a. El PACS debe admitir cualquier tamaño de credencial, siempre que la impresora utilizada para la creación del distintivo admita el tamaño deseado. | **Exigido** |  |
| b. El PACS permitirá que se configuren múltiples objetos para un diseño de credencial, incluyendo i. Campos de texto alfanuméricos ii. Campos de la base de datos iii. Fotos iv. Fotos de identidad v. Gráficos / Logotipos | **Exigido** |  |
| c. Cada campo de texto y base de datos agregado al diseño deberá tener la capacidad de emplear las siguientes propiedades: i. Ubicación del objeto ii. Alto y ancho iii. Color de fondo iv. Rotación v. Tipografía de texto vi. Tamaño del texto vii. Color del texto viii. Alineación horizontal y vertical del texto. | **Exigido** |  |
| 41. Cada foto y campo gráfico agregado al diseño tendrá la capacidad de emplear las siguientes propiedades: i. Ubicación del objeto ii. Alto y ancho iii. Mantener la relación de aspecto iv. La herramienta PACS Badge Layout debe ser compatible con una paleta de colores que admita un mínimo de 16,7 millones de colores que se puedan aplicar a los objetos aplicables. | **Exigido** |  |
| **Funcionalidad para Monitoreo de Alarmas y Eventos** | **Exigido** |  |
| 1. Interfaz de usuario con pestañas (TABs): el PACS debe admitir una vista con pestañas para la interfaz de usuario de monitoreo. Las siguientes pestañas serán compatibles: | **Exigido** |  |
| a. El Monitor de eventos se utilizará para monitorear eventos a nivel del sistema, como la actividad del Operador y eventos a nivel de campo. b. El Monitor de alarmas se utilizará para monitorear eventos a nivel de campo, como la actividad de acceso a Identidad, alarmas de entrada y alarmas de puerta, así como eventos a nivel del sistema configurados como alarmas. | **Exigido** |  |
| c. Swipe and Show Verification se utilizará para ver la información de identidad en tiempo real a medida que los titulares de credenciales acceden a puertas específicas. d. La búsqueda se utilizará para encontrar transacciones de alarmas y eventos actualmente almacenados en el PACS. e. El estado del hardware se utilizará para ver en tiempo real los dispositivos de hardware de campo configurados en el sistema, así como para manipular / anular esos dispositivos. | **Exigido** |  |
| 2. Anunciación de alarma: el PACS permitirá a los administradores configurar la forma en que las alarmas y los eventos se anuncian en el Monitor de alarma. | **Exigido** |  |
| a. Admite notificaciones audibles en la estación de trabajo cuando las alarmas llegan al sistema. i. Los usuarios tendrán la capacidad de ajustar la configuración y los parámetros. ii. Los administradores podrán elegir un sonido específico para emparejar con cada tipo de alarma. | **Exigido** |  |
| 3. Cada alarma y evento tendrá las siguientes opciones de configuración: | **Exigido** |  |
| a. Visualización en el Monitor de Alarma. b. Permita que las alarmas más altas en prioridad se muestren en la parte superior del Monitor de Alarma cuando un Operador clasifica según la prioridad de la alarma. c. Mostrar instrucciones de texto que guiarán al Operador en la respuesta de alarma. | **Exigido** |  |
| d. Enviar automáticamente un mensaje de correo electrónico a uno o más destinatarios. e. Para las alarmas y eventos relacionados con el video, inicie automáticamente el reproductor de video para mostrar una transmisión de video en vivo desde la cámara que está asociada con la alarma o el evento que genera. | **Exigido** |  |
| 4. Administración y manejo de alarmas: el monitor de alarmas PACS proporcionará un conteo en tiempo real de todas las alarmas y eventos en el monitor de alarmas en espera de la acción del operador. | **Exigido** |  |
| 5. El PACS deberá admitir las siguientes opciones para manejar / responder a las alarmas y eventos luego de la selección: | **Exigido** |  |
| a. Reconocer la alarma. b. Revisar las instrucciones de texto sobre la respuesta de alarma predefinida. c. Introduzca notas ilimitadas sobre el motivo de la alarma y / o la acción tomada en respuesta a la alarma. | **Exigido** |  |
| d. Revisar la historia de la alarma. e. Para las alarmas y los eventos que incluyen un titular de credenciales, acceder al Registro de identidad de ese titular de credenciales. | **Exigido** |  |
| f. Borrar la alarma. i. Operador único habilitado. ii. El control de dos personas para borrar las alarmas debe hacer cumplir una política de que el borrado y la (s) alarma (s) del operador del monitor de alarma no pueden ser el mismo operador que reconoció previamente la alarma. iii. Eliminación de alarmas basada en roles que permitirá a los administradores del sistema asignar un rol o roles a la alarma. iv. Al Operador que se le permita borrar la alarma se le debe asignar uno de los Roles asignados a la alarma para que él / ella borre la alarma del Monitor de Alarma. | **Exigido** |  |
| 6. Administración y manejo de alarmas por bloques: el PACS debe ser compatible con la capacidad de administrar y manejar múltiples alarmas. a. Los operadores tendrán la capacidad de borrar o reconocer todas las alarmas seleccionadas en una sola acción. | **Exigido** |  |
| 7. Enrutamiento de alarmas: el PACS permitirá el enrutamiento de alarmas a identidades específicas que monitorean la aplicación en función de a. Agendas b. Tipo de evento c. Dispositivo | **Exigido** |  |
| 8. Enmascaramiento de alarmas: el PACS permitirá el enmascaramiento de alarmas específicas o tipos de alarmas basadas en agendas predefinidas o mediante anulaciones manuales. a. Las alarmas enmascaradas no se reportarán en los monitores de alarma. b. El registro de la base de datos de transacciones para los informes y el seguimiento de auditoría no se verá afectado por el estado Enmascarado. c. Un operador tendrá la capacidad de enmascarar o desenmascarar cualquier punto de alarma en el sistema según los permisos. | **Exigido** |  |
| 9. Clasificación de alarmas: el PACS permitirá que las alarmas y los eventos se clasifiquen en el Monitor de alarmas por cualquiera de las columnas visibles actualmente configuradas. | **Exigido** |  |
| 10. Barras de colores de priorización de alarmas: el PACS debe proporcionar la capacidad de enfatizar la prioridad de las alarmas mediante el uso de barras de colores dentro de la pantalla del monitor de alarmas. a. Cada prioridad de alarma tendrá asignado su propio color único definido por el usuario. b. Las barras de colores también tendrán la capacidad de asignarse a prioridades de alarma individuales o a un rango de prioridades de alarma. | **Exigido** |  |
| 11. Configuración de columnas: el PACS permitirá a los administradores definir qué columnas se muestran en el Monitor de alarma. a. Los administradores también podrán establecer el orden de las columnas del Monitor de alarma. Las columnas disponibles para la configuración incluirán: | **Exigido** |  |
| i. Hora ii. Último acceso iii. Fecha de expiración de la credencial iv. Fecha de emisión de la credencial v. Fecha del panel vi. Prioridad vii. Operador viii. Nombre de la identidad ix. Apellido de la identidad x. Número de tarjeta | **Exigido** |  |
| xi. Número en relieve xii. Mensaje xiii. Nombre / Descripción del evento xiv. Tipo de evento xv. Panel xvi. Fuente xvii. Ubicación xviii. Fuente alternativa xix. Dirección de entrada xx. Dirección del evento | **Exigido** |  |
| xxi. Tipo de fuente xxii. Banderas xxiii. Estado xxiv. Nivel de emisión xxv. Rol | **Exigido** |  |
| 12. Capacidades de correo electrónico: el PACS admitirá capacidades de correo electrónico integradas. a. El PACS podrá generar un mensaje de correo electrónico para enviar a uno o más destinatarios luego de una alarma o evento generado. b. La función de correo electrónico se interconectará con cualquier servidor de correo electrónico que utilice SMTP como su protocolo. | **Exigido** |  |
| 13. Monitoreo de eventos: el PACS admitirá una pestaña de Monitoreo de eventos que se utilizará para monitorear eventos a nivel del sistema, como la actividad del operador. a. Un Operador podrá elegir qué columnas de campo mostrar y podrá colocar esas columnas en su orden de preferencia. b. El Operador también podrá ordenar los eventos por cualquier columna actualmente mostrada en el Monitor de Eventos. c. Los administradores tendrán la capacidad de configurar el número de eventos recientes para mostrar en el Monitor de eventos al acceder a la pestaña Eventos. | **Exigido** |  |
| 14. Contador de resumen de estado de dispositivo de hardware de campo: el PACS debe admitir un contador de estado de dispositivo de hardware de campo en tiempo real que muestre un resumen del número total de puertas, puntos de entrada, controladores empresariales inteligentes y subpaneles activos, enmascarados y apagados. | **Exigido** |  |
| 15. Ficha Estado del dispositivo de hardware de campo: el PACS debe admitir el estado del sistema en tiempo real que describe todos los dispositivos de hardware de campo configurados. a. La pestaña de estado del sistema en tiempo real incluirá: i. Controladores de empresariales inteligentes ii. Módulos de control de entrada iii. Entradas de alarma iv. Salidas de relé v. lectores de tarjetas vi. El estado del hardware mostrará el estado en tiempo real de todos estos dispositivos (en línea vs. fuera de línea, alarmas activadas, estado de enmascaramiento, etc.). | **Exigido** |  |
| 16. El estado del sistema incluirá tres contadores: a. Contador activo: un contador del número de puntos activos. b. Contador sin conexión: un contador del número de dispositivos sin conexión. c. Contador enmascarado: un contador del número de puntos enmascarados. | **Exigido** |  |
| 17. La pestaña Estado de hardware mostrará todos los dispositivos de hardware por separado en su propia fila. Lo siguiente deberá existir en la pestaña: a. Nombre del dispositivo b. Controlador empresarial inteligente / Módulo de control de entrada / Nombre del módulo de control de salida c. Estado actual del dispositivo | **Exigido** |  |
| 18. El PACS también permitirá a los operadores afectar el modo de acceso de los lectores de tarjetas, puertas abiertas, enmascarar / desenmascarar las entradas de alarma y activar / desactivar / pulsar una salida de la pestaña. El PACS también permitirá que los operadores afecten el modo de acceso de múltiples dispositivos con una sola acción seleccionando múltiples dispositivos y luego ejecutando el comando. | **Exigido** |  |
| 19. El PACS admitirá la integración con el módulo de red N1 de Life Safety Power. Cuando esté configurado, el enlace de la fuente de alimentación LSP aparecerá en la pestaña Estado del dispositivo de hardware de campo y cuando se haga clic en el enlace, aparecerá la ventana de configuración y diagnóstico N1. | **Exigido** |  |
| Llamada de registro de historial: el PACS debe ser compatible con la capacidad de activar el historial de una alarma. La ventana de llamada del historial mostrará la información de alarma asociada, incluida la marca de fecha y hora, las acciones de confirmación por parte de los operadores y las notas ingresadas. No se requerirá que el Operador salga del Monitor de Alarma para acceder a esta información y esta funcionalidad no evitará que la actividad de alarma adicionales aparezca en el Monitor de Alarma. | **Exigido** |  |
| 21. Llamada de registro de identidad: el PACS debe ser compatible con la capacidad de activar el formulario de identidad para mostrar el registro de identidad asociado con una alarma. a. La ventana de llamada de Identidad mostrará la información y la foto de la Identidad. No se requerirá que el Operador salga del Monitor de Alarma para acceder a esta información y esta funcionalidad no evitará que la actividad de alarma adicional informe al Monitor de Alarma. | **Exigido** |  |
| 22. Control del operador de los dispositivos de hardware de campo: el PACS permitirá a los operadores controlar manualmente el estado de los dispositivos de hardware de campo y sus puntos de entrada / salida desde el monitor de alarma. | **Exigido** |  |
| a. A nivel de Lectores de tarjetas controlar manualmente el estado del lector o según la agenda actual. i. Desbloqueado ii. Bloqueado iii. Código de facilidad iv. Sólo tarjeta v. solo PIN vi. Tarjeta y PIN vii. Tarjeta o PIN | **Exigido** |  |
| viii. Pulso para abrir la puerta. ix. Máscara / Desenmascarar x. Puerta forzada abierta / Puerta abierta xi. Deshabilitar la puerta xii. Restaurar la puerta a su estado correcto xiii. Enmascarar y desenmascarar entrada | **Exigido** |  |
| b. Salidas i. Encender ii. Apagar iii. Salidas tipo pulso | **Exigido** |  |
| 23. Los dispositivos de hardware de campo deben estar disponibles para control del operador desde la pestaña Estado del hardware. | **Exigido** |  |
| 24. El PACS utilizará un último comando activo. Por ejemplo, si una salida se desactiva debido a una programación y un Operador la enciende manualmente, la salida permanecerá encendida hasta que se apague manualmente o hasta que ocurra el siguiente intervalo programado. | **Exigido** |  |
| 25. Todos los controles manuales se registrarán en el registro de Auditoría del Operador con la hora del cambio, la función realizada por el operador y la descripción de la actividad realizada. | **Exigido** |  |
| 26. Mapas: el PACS admitirá mapas gráficos a través de la importación de fondos de mapas en los formatos que se enumeran a continuación: a. Mapa de bits (.bmp, .dib) b. JPEG (.jpg) c. Gráficos de red portátiles (.png) d. TIFF (.tif) e. Metarchivo de Windows (.wmf, .emf) f. Encapsulado Post Script (.eps) | **Exigido** |  |
| 27. El Administrador de PACS tendrá la capacidad de colocar iconos del sistema, incluidos lectores de tarjetas, puntos de entrada y salida, cámaras de video y otro hardware de campo de control de acceso para indicar su ubicación en la instalación. Si el administrador requiere que se actualice el mapa, cualquier ícono que se haya colocado en el mapa conservará la posición original. | **Exigido** |  |
| 28. Las capacidades de zoom estarán disponibles para proporcionar vistas más cercanas o más lejanas del área. Desde el Mapa, los operadores podrán: a. Reconocer una alarma b. Cambiar el modo de acceso de los lectores c. Enmascarar / Desenmascarar entradas d. Generar un Pulso, ajuste ON / OFF de una salida de relevo e. Lanzar una ventana de video | **Exigido** |  |
| 29. Indicadores de estado del sistema: El Monitor de alarma proporcionará indicadores de estado para mostrar el estado actual de varios elementos del PACS, incluidos: a. Número total de alarmas y eventos no reconocidos pendientes b. Estado de todos los dispositivos de hardware de campo (Controladores inteligentes de sistema, subpaneles, lectores de tarjetas, entradas y salidas), incluso fuera de línea, activo y enmascarado. c. La pestaña de estado del hardware mostrará todos los dispositivos que están en alarma, así como el estado en línea / fuera de línea para todos los dispositivos de hardware de campo. | **Exigido** |  |
| 30. Deslizar y mostrar (Verificación): el PACS debe admitir la funcionalidad de deslizar y mostrar que permite mostrar la foto del titular de la credencial a medida que pasa su credencial a través de un lector de tarjetas específico. a. Se deben poder activar hasta cuatro lectores de tarjetas para deslizar y mostrar en cada ventana del navegador. b. Deslizar y mostrar permite a los operadores verificar el titular de la credencial comparado con su foto cuando ingresan a un portal. | **Exigido** |  |
| **Funcionalidad de Configuración y Administración** | **Exigido** |  |
| 1. Registro de alarmas y eventos: el PACS debe rastrear y mantener un registro completo de todas las actividades de alarma y eventos. Todas las alarmas y eventos que ocurran se registrarán con la siguiente información: a. Nombre de la alarma b. Fecha y hora c. Donde ocurrió la alarma d. Información de Reconocimiento e. Todas las acciones del Operador asociadas a la alarma o evento. | **Exigido** |  |
| 2. La información de alarmas y eventos se puede ver a través del motor de informes de PACS, que debe incluir el número total de alarmas y eventos que se registran en el dispositivo tipo appliance del PACS. a. El número de alarmas y eventos almacenados estará limitado solo por la cantidad de espacio en disco disponible en el dispositivo PACS. | **Exigido** |  |
| 3. Tiempo de espera / cierre de sesión del operador: el PACS debe admitir una función de cierre de sesión automático que permita al sistema cerrar automáticamente la sesión del sistema después de un período de inactividad. Las opciones de tiempo de espera de cierre de sesión automático incluirán a. 10 minutos b. 15 minutos c. 30 minutos d. 1 hora e. Indefinido: no cerrar la sesión de un operador, independientemente de la duración de la inactividad. | **Exigido** |  |
| 4. Delegaciones: todas las características y funciones principales de PACS estarán protegidas por permisos mediante el uso de delegaciones. a. A cada cuenta de operador se le asignará un rol, que incluirá una lista de delegaciones asignadas a ese rol. b. El acceso del operador a las pantallas de PACS, así como su capacidad para ver, agregar, editar o eliminar objetos de PACS se controlarán a través de las delegaciones. | **Exigido** |  |
| 5. Licencias basadas en software: el PACS admitirá un modelo de aplicación de licencias basado en software. a. Una llave de hardware o dongle no será aceptable para controlar la asignación de licencias y sus funciones. | **Exigido** |  |
| 6. Información de diagnóstico del dispositivo Tipo Appliance: el PACS admitirá la capacidad de analizar información de diagnóstico en tiempo real para cada dispositivo tipo appliance del PACS al ver la página “Acerca de” del dispositivo. Los datos de diagnóstico incluirán a. Número de días en línea b. Carga actual c. Memoria d. Uso del espacio en disco e. Datos de comunicaciones de red | **Exigido** |  |
| 7. Ayuda en línea sensible al contexto: el PACS debe admitir ayuda en línea, sensible al contexto para asistir a los usuarios del sistema en la operación de este. | **Exigido** |  |
| a. Una vez dentro del programa de ayuda, los usuarios podrán navegar por los archivos de ayuda, moviéndose a otras áreas de la documentación sin tener que volver al software de la aplicación. b. Los archivos de Ayuda tendrán una tabla de contenido, índice y capacidad de búsqueda vinculados. | **Exigido** |  |
| c. Los archivos de Ayuda estarán disponibles en todos los idiomas compatibles con el PACS. i. Inglés ii. Español | **Exigido** |  |
| 8. Cuentas del operador: el PACS debe ser compatible con cuentas de operador. a. Cada cuenta de operador requerirá una contraseña de nombre de usuario única para acceder al sistema. b. A cada cuenta de operador también se le asignará un rol, que determinará el nivel de permiso para esa cuenta, controlando así las funciones que el operador puede desempeñar en el sistema. c. Todas las modificaciones a una cuenta de operador se informarán al supervisor de eventos y se registrarán en la estructura de directorios de LDAP para los procesos de auditoría e informes. d. El PACS admitirá tantas cuentas de operador como identidades configuradas. | **Exigido** |  |
| 9. Protección de contraseña: cada cuenta de operador requerirá un nombre de usuario y contraseña únicos que vincularían esa identidad a los derechos de delegación para acceder al PACS. a. Esto permitirá el acceso del operador a: i. Pantallas a las que puede acceder el Operador ii. Tareas que el Operador puede realizar b. Un Operador podrá cambiar su contraseña de PACS en cualquier momento. c. Se admitirán parámetros de contraseña segura. i. Exigir a los usuarios del sistema que ingresen al menos 8 caracteres. ii. Incluya al menos una letra mayúscula, una letra minúscula y un número. | **Exigido** |  |
| 10. Políticas: el PACS admitirá políticas que actuarán como plantillas que se aplicarán a los dispositivos de hardware de campo en el sistema para facilitar la configuración de dispositivos similares. a. Cada Política consistirá en una plantilla para lectores de tarjetas, entradas o salidas. b. El PACS deberá soportar un número ilimitado de políticas. | **Exigido** |  |
| 11. Grupos: el PACS debe admitir la agrupación de parámetros para facilitar la configuración. Los conceptos de agrupación deben incluir, pero no limitarse a: a. Roles b. Dispositivos de hardware de campo c. Políticas | **Exigido** |  |
| 12. Partición del sistema: el PACS proporcionará la capacidad de partición avanzada del sistema. a. A cada partición se le permitirá su propio grupo de identidades, hardware de campo y parámetros tales como horarios y grupos de acceso. b. Se permitirá que las identidades pertenezcan a una o múltiples particiones. c. La partición debe proporcionar una arquitectura flexible de "arrendatario / arrendador" en la que los usuarios de la partición solo puedan ver, agregar, modificar y eliminar identidades, parámetros del sistema y hardware de campo que pertenezcan a sus respectivas particiones. d. Los operadores PACS pueden asignarse a más de una partición. Una partición puede ser asignada a más de un operador. | **Exigido** |  |
| Registro de actividad del operador: el PACS debe rastrear y mantener un registro completo de toda la actividad de la cuenta del operador. Todos los cambios que se produzcan en la estructura del directorio se registrarán, dentro de los más importantes deberán estar: | **Exigido** |  |
| a. Actividad de inicio / cierre de sesión de la cuenta del operador b. Agregar, eliminar o cambiar registros de identidad c. Cambio a las configuraciones del sistema para incluir, entre otros, hardware de campo, grupos de acceso o programaciones d. La actividad realizada dentro del Monitor de Alarmas y Eventos incluye, pero no se limita a reconocer alarmas, abrir puertas o borrar eventos. | **Exigido** |  |
| e. Las actividades registradas incluirán como mínimo la siguiente información, pero no se limitarán a: i. Cuenta de operador ii. Fecha y hora de la actividad. iii. Actividad que se realizó. iv. Datos originales antes del cambio, si corresponde. v. Nuevos datos que fueron actualizados. | **Exigido** |  |
| f. La información de la actividad de la cuenta del operador se puede ver a través del motor de informes del PACS, que debe indicar el número total de eventos del operador que se registran en el dispositivo tipo appliance del PACS. g. El número de eventos almacenados en la cuenta del operador solo estará limitado por la cantidad de espacio en disco disponible en el dispositivo PACS. | **Exigido** |  |
| 14. Utilidad del programador del sistema: la utilidad de programación del sistema permitirá a los administradores del sistema programar acciones | **Exigido** |  |
| a. Bajo demanda o de un solo uso b. Con base recurrente c. Los tipos de acciones incluyen, pero no se limitan a ejecutar informes, actualizar perfiles de identidad, aplicar modos de puerta y ejecutar acciones globales. | **Exigido** |  |
| d. La Utilidad de Programación deberá satisfacer una amplia gama de necesidades de programación, que incluyen, entre otras: i. Cada hora, es decir, "Todos los días a la hora" ii. Día específico, hora específica, es decir, "todos los lunes a las 8:00 am" iii. Mensualmente, es decir, “el primer domingo de cada mes” iv. Fecha específica de recurrencia, es decir, “Cada 29 de febrero a las 12 del mediodía” v. Fecha específica en el futuro, es decir, “7 de diciembre de 2017 a las 5pm” vi. Las actividades recurrentes se pueden configurar para: 1. Una fecha de inicio y finalización maestra 2. Ejecutar indefinidamente vii. La utilidad de programación debe proporcionar un monitor de trabajo que permita al administrador del sistema: 1. Ver el estado de las tareas actualmente en ejecución. 2. Ver una lista cronológica de futuras tareas programadas 3. Ver un registro histórico de tareas completadas | **Exigido** |  |
| 15. Informes: el PACS debe admitir un mínimo de 19 informes estándar. | **Exigido** |  |
| a. Los informes tendrán la capacidad de crearse ya sea como: i. documento PDF ii. documento de hoja de cálculo b. Una vez generado, el informe puede ser: i. Guardado en un archivo ii. Impreso en una impresora local o en red iii. Cada informe tendrá la capacidad de personalizarse / filtrarse en datos relevantes para ese informe en particular. | **Exigido** |  |
| c. Los informes estándar de PACS incluirán: i. Informe de auditoría de concesión de acceso: el Informe de auditoría de concesión de acceso presentará información sobre toda la actividad de concesión de acceso que fue generada manualmente por un Operador e incluirá la puerta que se abrió, el tiempo y el Operador que ejecuta la concesión de la puerta. ii. Informe del grupo de acceso: el informe del grupo de acceso presentará información sobre todos los grupos de acceso del PACS incluidos, entre otros, los siguientes: 1. Los roles que se asignan al grupo. 2. El Horario asignado al grupo. 3. El número de puertas asignadas al grupo. 4. Lista de las puertas asignadas al grupo. 5. Informe de alarma: el Informe de alarma presentará información sobre todas las alarmas que se produjeron en el sistema, incluido el nombre del panel, las medidas tomadas por el operador, el operador que responde a la alarma y cualquier nota del operador relacionada con la alarma. | **Exigido** |  |
| iii. Informe de dispositivo: el informe de puerta de enlace debe presentar información sobre cada dispositivo PACS definido, que incluye: 1. El tipo de dispositivo PACS 2. El nombre y dominio DNS 3. La zona horaria local y la configuración del horario de verano 4. Se habilita una lista de fabricantes de hardware de campo. 5. Una lista de controladores empresariales inteligentes está configurada para informar al panel | **Exigido** |  |
| iv. Informe de área: el Informe de área debe presentar información sobre todas las áreas definidas. Cada entrada al área debe incluir el nombre del área, el dispositivo PACS donde existe el área y las puertas asignadas al área. | **Exigido** |  |
| v. Informe de registro de auditoría: el informe de registro de auditoría debe presentar información sobre cada cambio realizado en el PACS por un operador. Cada entrada del registro de auditoría incluirá: 1. Fecha / hora 2. Descripción 3. El Operador que realizó el cambio. 4. El tipo de cambio. 5. Los detalles del cambio. 6. La información original antes del cambio (si existe) | **Exigido** |  |
| vi. Informe de la cámara: el Informe de la cámara presentará información sobre cada cámara configurada en el sistema, incluido el Nombre de la cámara y sus atributos. | **Exigido** |  |
| vii. Informe de colaboración: el Informe de colaboración presentará información sobre todos los scripts de colaboración definidos en el PACS, incluido el tipo de colaboración y si la colaboración está activa. | **Exigido** |  |
| viii. Informe de la delegación: el Informe de la delegación presentará información sobre todos los grupos de delegación definidos en el PACS, incluida la identidad asignada a la delegación y el permiso configurado para esa delegación. | **Exigido** |  |
| ix. Informe de acceso a la puerta: el Informe de acceso a la puerta debe presentar información sobre el acceso del titular de la credencial a cada puerta en el PACS, incluido el cronograma al que el titular de la credencial puede acceder. | **Exigido** |  |
| x. Informe de configuración de la puerta: el Informe de configuración de la puerta debe presentar información sobre la configuración completa de cada puerta definida en el PACS. | **Exigido** |  |
| xi. Informe de eventos: el Informe de eventos presentará información sobre eventos definidos en el sistema junto con sus atributos, que incluyen: 1. Nombre del evento 2. Tipo de evento asignado 3. Prioridad 4. Horario de enmascaramiento 5. Si el evento está configurado para enmascararse y / o registrar el evento | **Exigido** |  |
| xii. Informe de tipo de evento: el informe de tipo de evento presentará información sobre cada tipo de evento definido en el PACS, este incluye: 1. Horario de supresión 2. Prioridad 3. Tiempo de retransmisión 4. Procedimiento de retransmisión 5. Procedimiento 6. Si el tipo de evento está configurado para enmascararse, registrar el evento y / o enviarse al monitor de alarma | **Exigido** |  |
| xiii. Informe del grupo: el informe del grupo debe presentar información sobre todos los grupos definidos, incluido el nombre del grupo, el tipo y la información de los miembros, como los lectores de tarjetas y los roles. | **Exigido** |  |
| xiv. Informe de días festivos: el Informe de días festivos debe presentar información sobre cada día feriado definido, incluida la fecha del día festivo, la cantidad de días en que el día festivo está vigente y el tipo (s) asignado al día festivo. | **Exigido** |  |
| xv. Informe de acceso por titular de una credencial (identidad): el informe de acceso de la identidad debe presentar información sobre cada identidad definida con respecto a qué puertas tienen acceso. El informe incluirá el cronograma en el que se ha otorgado acceso a cada lector, así como las asignaciones de grupo de acceso y rol que permiten el acceso a cada lector. | **Exigido** |  |
| xvi. Informe de resumen de Titulares de una credencial (identidad): el informe de resumen de identidad presentará información sobre cada identidad definida con respecto al estado y tipo de identidad, la emisión de credenciales y la fecha de caducidad, y qué roles y grupos de acceso se han asignado a la identidad. | **Exigido** |  |
| xvii. Informe del panel: el informe del panel debe presentar información sobre la configuración completa de cada controlador empresarial inteligente configurado en el PACS. | **Exigido** |  |
| xviii. Informe de políticas: el Informe de políticas debe presentar información sobre todas las políticas definidas en el PACS, incluyendo: 1. Nombre de la política 2. Estado activo 3. Qué componentes de hardware abarca la política | **Exigido** |  |
| xix. Informe de rol: el informe de rol debe presentar información sobre cada rol definido, que incluye: 1. Información del rol padre 2. Fechas de activación / desactivación. 3. Roles hijo 4. Identidades asignadas a ese rol 5. Grupos de acceso asignados a ese rol 6. Puertas asignadas a ese rol. | **Exigido** |  |
| xx. Informe de programación: el informe de programación presentará información sobre cada programación definida, incluido su modo y cada intervalo configurado 1. Días de la semana, 2. tipos de festivos 3. tiempos de inicio y finalización del intervalo | **Exigido** |  |
| xxi. Informe de Credenciales: el Reporte de Credenciales presentará información sobre todas las credenciales del sistema, incluido el número de la credencial, la identidad a la que está asignada y el estado activo / desactivado. | **Exigido** |  |
| xxii. Informe de transacciones: el Informe de transacciones debe presentar información sobre cada transacción generada en el nivel de hardware de campo. Cada evento de registro de transacciones debe incluir: 1. Fecha / hora 2. Origen del evento 3. Nombre y tipo de evento 4. Información de identidad y su credencial. | **Exigido** |  |
| xxiii. Informes rápidos: el PACS debe admitir informes rápidos. 1. Cada uno de los informes estándar definidos en la sección Informes tendrá la capacidad de aplicarles filtros de datos relevantes, antes de ejecutarlos, para proporcionar un informe con información más específica que el informe genérico. La configuración del Informe rápido se diseñará para ejecutarse una vez y no se guardará. 2. Los informes rápidos tendrán la capacidad de enviar sus resultados a un formato de archivo PDF o un formato de archivo de hoja de cálculo. | **Exigido** |  |
| xxiv. Informes personalizados: el PACS admitirá informes personalizados. 1. Cada uno de los informes estándar definidos en la sección Informes tendrá la capacidad de aplicarles filtros de datos relevantes, antes de ejecutarlos, para proporcionar un informe con datos más específicos que el informe genérico. 2. Los informes personalizados se diseñarán para ejecutarse varias veces y se guardarán en el formulario de informes personalizados para una ejecución rápida en el futuro. 3. Los informes personalizados deben tener la capacidad de enviar sus resultados a un formato de archivo PDF o un formato de archivo de hoja de cálculo. 4. A cada Informe personalizado se le dará un nombre único para identificarlo en la lista de Informes personalizados. | **Exigido** |  |
| 16. Soporte remoto: el PACS tendrá capacidad de soporte remoto para permitir que el integrador de sistemas o fabricante de valor agregado y acceda al dispositivo del cliente para: a. Solución de problemas b. Diagnósticos c. Carga del Sistema d. Asistencia con la configuración. | **Exigido** |  |
| 17. El PACS ofrecerá la capacidad de obtener datos de registro del log de eventos del software para obtener un mejor soporte de la aplicación. | **Exigido** |  |
| 18. Replicación basada en cuadrícula: el PACS admitirá la arquitectura de replicación basada en cuadrícula automatizada de la estructura de directorios del dispositivo para los clientes que implementan múltiples dispositivos tipo appliance. a. La arquitectura de replicación debe ser de igual a igual y no requiere un servidor de base de datos dedicado para permitir la replicación de identidades y datos de configuración en todos los dispositivos. b. El PACS admitirá comunicaciones cifradas entre dispositivos utilizando cifrado SSL. c. La replicación permitirá que los datos LDAP de todos los dispositivos se sincronicen con cada uno de los otros en el sistema, permitiendo que el dispositivo PACS se reconstruya a partir de los datos replicados encontrados en otro dispositivo del sistema. | **Exigido** |  |
| 19. Funcionalidad Hot Standby: el PACS debe ser compatible con una arquitectura de Hot standby y conmutación por error. a. Para cada dispositivo, un dispositivo Hot Standby se configurará para monitorear el estado de su dispositivo asociado principal. b. En caso de que un dispositivo no funcione, el dispositivo de espera activa debe ser capaz de detectar automáticamente un problema y asumir el control del sistema. | **Exigido** |  |
| 20. Actualizaciones de software: el PACS admitirá actualizaciones mediante la descarga desde el sitio web del fabricante o la recepción por correo electrónico de los archivos de actualización. a. No se requerirá interacción física con el dispositivo PACS para realizar una actualización exitosa del software del sistema. | **Exigido** |  |
| 21. Respaldos del sistema: el PACS tendrá la capacidad de respaldar y restaurar la estructura de directorios de LDAP. a. Las copias de seguridad se ejecutarán simultáneamente con el resto del sistema y no requerirán que todos los operadores se desconecten del PACS. b. Las copias de seguridad deben incluir datos de transacción y datos de configuración del sistema. c. Las copias de seguridad del dispositivo se pueden cifrar mediante el cifrado AES. d. Copias de seguridad del dispositivo para: i. Dispositivo de almacenamiento USB ii. Directorio compartido de Windows o carpeta compartida de red iii. Servidores SCP e. Las copias de seguridad se realizarán: i. Automáticamente en un horario diario predefinido ii. Manualmente a través de la interfaz de usuario. | **Exigido** |  |
| 22. Reinicio y apagado del dispositivo tipo appliance: el PACS debe admitir las capacidades de reinicio y apagado del dispositivo. a. La interfaz de usuario de PACS admitirá tanto el reinicio como el apagado del dispositivo. b. Los derechos y el acceso para reiniciar y apagar el dispositivo se denotarán mediante inicio de sesión. | **Exigido** |  |
| 23. Visualización de hora global: el PACS debe admitir la visualización de fecha y hora localizada. | **Exigido** |  |
| 24. Registros de datos del sistema: el PACS debe admitir registros de datos del sistema para ayudar con los diagnósticos y la solución de problemas. a. Los registros estándar deben incluir registros del servidor web, registros de comunicación de hardware de campo, registros del software del sistema y registros de transacciones del sistema. b. Todos los registros serán visibles en un formato de texto plano. | **Exigido** |  |
| **Funcionalidad para Integración con Sistemas de Gestión de Video (VMS)** | **Exigido** |  |
| 1. Integración con servidores de video digital: el PACS debe admitir la integración de video digital con servidores de video digital | **Exigido** |  |
| 2. Los servidores de video digital se integrarán con los monitores de alarma de modo que, como mínimo: a. Las alarmas generadas por el sistema se vincularán a video en vivo y grabado del sistema de administración de video (VMS). b. Cualquier alarma / evento en el PACS tendrá la capacidad de asociarse con un videoclip digital en tiempo real. c. Cada alarma / evento en el PACS activará el VMS para almacenar: i. Un número predefinido de segundos de video antes de que ocurriera el evento ii. Un número predefinido de segundos de video después del evento | **Exigido** |  |
| 3. Conectividad LAN / WAN: el PACS debe ser compatible con la conectividad para transmitir el video en vivo de una cámara o para revisar el video grabado almacenado de la actividad de eventos o alarmas en el Monitor de Alarma a través de redes de comunicación de datos que incluyen, entre otros: a. LAN / VLAN / WLAN (red de área local / LAN virtual / LAN inalámbrica) b. WAN (red de área amplia) c. MAN (Red de área gestionada) d. VPN (red privada virtual) | **Exigido** |  |
| 4. Asociación de dispositivos: cada dispositivo de hardware de campo de control de acceso que esté configurado en el PACS tendrá la capacidad de asociarse con una cámara desde el VMS. a. Un número ilimitado de asociaciones de dispositivos será posible. b. Una cámara debe tener la capacidad de estar asociada con múltiples dispositivos de hardware de control de acceso. c. Un dispositivo de hardware de control de acceso tendrá la capacidad de estar asociado con varias cámaras. d. Cuando se asocian varias cámaras a un solo evento de hardware de control de acceso o alarma, todas las cámaras asociadas aparecerán en el reproductor de video en la vista de matriz apropiada. | **Exigido** |  |
| 5. Marcado previo y posterior del video basado en eventos: cuando se activa una alarma, el PACS notificará al VMS para que marque el tiempo de pre y post grabación para el videoclip asociado. a. Pre-Roll será la cantidad de segundos de video que el VMS almacenará antes de la hora del evento. b. Post-Roll será la cantidad de segundos de video que el VMS almacenará después de que se genere un evento asociado. c. Los tiempos de pre y post roll serán configurables hasta 10 y 100 segundos respectivamente. | **Exigido** |  |
| 6. Eventos de video almacenados: cada condición de alarma / evento tendrá la capacidad de marcar el inicio de un evento de video o el final de un evento de video en tiempo real. Por ejemplo, cuando se activa una puerta abierta, el VMS marcará el inicio del evento de video. Cuando la alarma se restaura, el VMS puede marcar el final del evento de video. | **Exigido** |  |
| 7. Informe de eventos del VMS: el PACS admitirá los siguientes eventos VMS entrantes. a. Panel Desconectado / Panel NORMAL Desconectado. Este evento informará las pérdidas de conexión y las restauraciones de los servidores de video digital. b. Detección de movimiento / No más movimiento detectado. Este evento informará los eventos de movimiento de las cámaras en el VMS. c. Pérdida de video / Video restaurado. Este evento informará las pérdidas de conexión y las restauraciones de las cámaras analógicas conectadas al VMS. d. Pérdida de conexión / conexión restaurada. El evento informará las pérdidas de conexión y las restauraciones de las cámaras IP conectadas al servidor VMS. | **Exigido** |  |
| 8. Recuperación de video: al generar una alarma que tiene un video asociado, el Operador podrá recuperar el segmento de video asociado con la alarma. a. Una vez iniciado, el Operador tendrá la capacidad de ajustar la hora de inicio y finalización del segmento de video. | **Exigido** |  |
| 9. Reproductor de video: el reproductor de video debe admitir una vista de matriz para la visualización de cámaras en línea. a. El número de ventanas de video en la matriz dependerá de la velocidad de fotogramas y la resolución de las cámaras y número de videos que se estén viendo. | **Exigido** |  |
| b. La vista de matriz permitirá dimensionar las ventanas de esta. c. El PACS proporcionará la capacidad de lanzar más de una cámara con una alarma generada. i. Cuando se genera una alarma con múltiples cámaras, se abrirá una ventana de matriz mostrando todas las cámaras asociadas. ii. El operador también tendrá la capacidad de cambiar entre otras cámaras si el dispositivo que generó el evento tiene más de una cámara asociada. iii. Los operadores podrán reproducir simultáneamente el video grabado de cualquier clip, incluso mientras se graba ese clip de video. iv. El operador tendrá la opción de cambiar al modo en vivo desde una cámara en cualquier momento durante la operación. | **Exigido** |  |
| d. El reproductor de video digital deberá mostrar la fecha y la hora del cuadro del video clip, así como el modo actual del reproductor (reproducir o en vivo). | **Exigido** |  |
| Control de reproducción: el PACS debe proporcionar los siguientes controles de reproducción para ver el video grabado: a. Iniciar y detener la reproducción: el operador podrá iniciar y detener la reproducción. b. Pausa y reanudación: el operador podrá pausar y reanudar la reproducción actual. c. Reproducción en reversa: el operador podrá invertir video en velocidad normal. d. Saltar hacia atrás: el operador podrá usar el botón Saltar hacia atrás para rebobinar la reproducción. e. Avance de fotogramas: el operador debe poder usar el botón de avance de fotogramas para avanzar el video clip fotograma a fotograma. f. Inicio automático del reproductor de video: cualquier alarma / evento generado debe ser configurable para iniciar automáticamente el reproductor de video en el monitor de alarma PACS. | **Exigido** |  |
| 11. Comandos de PAN / TILT / ZOOM: el PACS debe admitir los controles de PTZ del monitor de alarma. Las configuraciones de comando soportadas estarán disponibles para: a. Paneo a la Izquierda b. Paneo a la derecha c. Tilt hacia arriba d. Tilt hacia abajo e. Acercarse f. Alejarse g. Enfoque cercano h. Enfoque lejano i. Apertura de Iris j. Cierre del Iris k. Ir a preajuste (preset) l. Detener el movimiento de PTZ | **Exigido** |  |
| 12. Preajustes de PTZ en alarma: el PACS debe admitir los preajustes de PTZ predefinidos que se ejecutan en función de la generación de alarma. a. Cada evento / alarma en el PACS podrá asignarse a un preajuste PTZ en la cámara asociada. b. Tras la generación de la alarma, la cámara asociada realizará un movimiento PTZ automáticamente a su ubicación preconfigurada. | **Exigido** |  |
| 13. Alarmas de detección de movimiento de video: el PACS informará las alarmas de detección de movimiento de video de tal manera que a. Cuando una cámara monitoreada detecta movimiento en su rango de sitio, informará una alarma de "Detección de movimiento" al monitor de alarma PACS. b. Cuando la cámara ya no detecta movimiento, informará una alarma de "Restauración de detección de movimiento" al Monitor de alarma PACS. | **Exigido** |  |
| 14. Suavizado del evento de detección de movimiento de video: el PACS permitirá el suavizado del evento de detección de movimiento de video que ayudará a eliminar la generación de múltiples alarmas de detección de movimiento debido a que un objeto ingresa y sale del campo de visión de la cámara de forma repetida y rápida. | **Exigido** |  |
| a. Los administradores deben poder establecer un período de tiempo desde que se restaura un evento de movimiento inicial, que no se detecta ningún otro movimiento de video antes de informar la alarma. b. Si se detecta movimiento durante el tiempo de suavizado, el PACS esperará a que cese el movimiento, y luego nuevamente esperará a que el tiempo de suavizado configurado expire sin nuevo movimiento antes de informar la alarma. | **Exigido** |  |
| 15. Enmascaramiento de eventos de detección de movimiento de video: el PACS tendrá la capacidad de enmascarar eventos de detección de movimiento de video por cámara. a. Cada cámara tendrá la capacidad de asignarse un horario; durante el cual se enmascararán los eventos de detección de movimiento de video generados por esa cámara. | **Exigido** |  |
| 16. Alarmas fuera de línea: si un servidor VMS o alguna de las cámaras asociadas se desconectan, se enviará una alarma específica al monitor de alarma PACS. | **Exigido** |  |
| 17. Vista de imagen fija: durante la reproducción de un video grabado, el operador podrá crear una imagen fija. Esta operación no afectará a ninguna otra operación y no alterará el video grabado. | **Exigido** |  |
| 18. Iconos de video: el PACS debe soportar iconos de video. Las alarmas que ingresan al Monitor de alarmas generado por un dispositivo que tiene una cámara asociada mostrarán un icono junto a la alarma para alertar al Operador de que el video está asociado con la alarma. | **Exigido** |  |
| 19. Lista de estado del servidor de video / cámara de video: el PACS debe admitir una página de lista de estado que debe mostrar el estado de conexión de todos los servidores de video y cámaras configurados. | **Exigido** |  |
| 20. Delegaciones de video: las delegaciones definidas por el usuario restringirán el acceso de seguridad de cada Operador a operaciones específicas del sistema, como el monitoreo de video y la asociación de cámaras a dispositivos. | **Exigido** |  |
| 21. Verificación de Credenciales: El sistema de VMS estará en la capacidad de poder invocar un panel de visualización de su interfaz gráfica exclusivo para supervisar los titulares de tarjeta que están presentando su credencial en una puerta determinada y ver información básica contenida en el PACS como su foto, los datos del titular de la tarjeta y si está o no autorizado a ingresar por esa puerta. | **Exigido** |  |
| 22. Tareas Automatizadas y Alarmas: El sistema de VMS estará en capacidad de reconocer eventos relacionados con las puertas o entradas del PACS que sirvan como disparadores dentro del sistema de VMS para activar tareas automáticas o alarmas de este. | **Exigido** |  |
| **Funcionalidad para Integración con Sistemas de Terceros** |  |  |
| 1. El PACS admitirá una utilidad de colaboración que permitirá la transferencia de información en tiempo real o programada, incluidas imágenes y eventos, entre el PACS y los sistemas de TI, seguridad y otros sistemas de terceros. | **Exigido** |  |
| 2. Una interfaz de usuario permitirá la generación de colaboraciones de importación y exportación. Se aplicará una fecha de inicio y finalización para ejecutar la colaboración durante los intervalos programados solo entre ciertas fechas. | **Exigido** |  |
| 3. El PACS admitirá la sincronización de identidades entre múltiples instalaciones dispares del PACS a través de las importaciones de identidad recurrentes y las exportaciones de identidad configuradas entre los sistemas. | **Exigido** |  |
| 4. El PACS debe admitir un mínimo de 32 Colaboraciones por dispositivo tipo appliance del PACS. | **Exigido** |  |
| 5. El PACS deberá soportar los siguientes tipos de colaboración: a. LDAP Pull (aplicable a identidades) b. Oracle RDBMS Pull (aplicable a identidades) c. LDAP SQL Server Pull (aplicable a identidades) d. Importación de identidad desde un archivo CSV e. Exportación de identidad a un archivo CSV f. Eventos push usando formato XML | **Exigido** |  |
| 6. Identity Pulls: permitirá que los datos relacionados con Identidades como son credenciales, roles, particiones y fotos se importen a la estructura de directorios del sistema. La importación de información se realizará en la siguiente forma. | **Exigido** |  |
| a. Agregar / Modificar: si existe un registro en el archivo en la estructura del directorio, se reemplazará de acuerdo con la configuración de diseño especificada. b. Los registros que no existen ya se agregarán a la estructura del directorio. c. Admitirá imágenes que se importarán a la estructura de directorios de OpenLDAP. | **Exigido** |  |
| 7. Cada colaboración utilizará un registro de errores que informará todos los errores que ocurran durante la importación de un archivo. Todos los errores se pueden ver desde este registro y, una vez corregidos, la importación se puede ejecutar una segunda vez para descargar los registros corregidos. | **Exigido** |  |
| 8. Una vez que se complete la importación de información de una colaboración, los cambios se descargarán automáticamente a los controladores empresariales inteligentes en tiempo real a medida que la información se esté importando a la estructura del directorio. | **Exigido** |  |
| 9. Inserción de eventos: permitirá que las alarmas y eventos se exporten desde el PACS a otros motores de informes de terceros. | **Exigido** |  |
| 10. Los eventos deberán tener la opción de ser exportados con información detallada de respuesta de alarma, incluidos reconocimientos, Borrados y Notas del operador. | **Exigido** |  |
| 11. Filtros de datos: las colaboraciones permitirán a los administradores seleccionar un subconjunto de datos para las operaciones de exportación o importación. |  |  |
| a. Los filtros se utilizarán para definir qué registros se seleccionarán para la importación o exportación. |  |  |
| **Garantías** | **Exigido** |  |
| El oferente deberá presentar junto con su oferta carta de autorización firmada por un representante del fabricante con potestades sobre nuestra región, por la cual se autorice al oferente a proveer los equipos ofertados. | **Exigido** |  |
| Los técnicos de la empresa oferente deberán estar certificados por el fabricante. Los profesionales deberán residir en Paraguay, así como ser personal estable y formar parte de la nómina de la empresa oferente. | **Exigido** |  |
| Garantía escrita del fabricante de al menos 3(tres) años | **Exigido** |  |

**Ítem 7: Pantalla para NOC**

|  |  |  |  |
| --- | --- | --- | --- |
| **ESPECIFICACIONES TÉCNICAS MÍNIMAS** | | | |
| **Nombre del Bien o Servicio Conexo** | **Descripción Técnica** | **Mínimo Exigido** | **El bien ofertado cumple con las especificaciones requeridas (SI/NO)** |
| **Marca:** | **Especificar** | |  |
| **Modelo:** | **Especificar** | |  |
| **Procedencia:** | **Especificar** | |  |
| **Cantidad:** | **01 (uno)** | **Exigido** |  |
| **Descripción** | **Video Wall 2x2** | **Exigido** |  |
| **Tamaño del panel:** | ≥ 55" o superior | **Exigido** |  |
| **Resolución** | Full HD (1920x1080) | **Exigido** |  |
| **Brillo** | 500 nit o superior | **Exigido** |  |
| **Operación** | Diseñado para operación 24/7 | **Exigido** |  |
| **Tipo:** | Panel con marco ultradelgado para video Wall | **Exigido** |  |
| **Marcos:** | Distancia marca a marco: ≤ 2 mm | **Exigido** |  |
| **Angulo de visión horizontal/vertical:** | ≥ 178°/178° | **Exigido** |  |
| **Contraste:** | ≥ 4.000:1 o superior | **Exigido** |  |
| **Alimentación** | Frecuencia de operación: 50/60 Hz | **Exigido** |  |
| Fuente de alimentación interna 100 - 240 Vac | **Exigido** |  |
| **Ambiental** | Temperatura de operación: 0° a 40°C como mínimo | **Exigido** |  |
| **Conectividad** | 1xUSB 2.0 | **Exigido** |  |
| DisplayPort | **Exigido** |  |
| 2xHDMI 2.0 (HDCP 2.2) | **Exigido** |  |
| RJ-45 | **Exigido** |  |
| RS-232C | **Exigido** |  |
| **Certificaciones:** | FCC Part 15, IEC 60950-1, EN60950-1, cUL60950-1, CE, EN55022, EN55024 | **Exigido** |  |
| **Accesorios:** | Se deben incluir todos los accesorios para montar los equipos en la pared (VESA compatible) y los necesarios para conectarlos a las estaciones de monitoreo (cable HDMI, cables de interconexión, control remoto, baterías, cable de alimentación, etc.) | **Exigido** |  |
| **Autorización del fabricante:** | Carta de autorización del fabricante o distribuidor autorizado para nuestro país para presentar oferta de sus equipos para esta licitación | **Exigido** |  |
| **Garantía del fabricante:** | Carta de garantía del fabricante de al menos 2 años | **Exigido** |  |

**Ítem 8: Sistema de detección y extinción de incendios automática Sala de Equipos**

|  |  |  |  |
| --- | --- | --- | --- |
| **ESPECIFICACIONES TÉCNICAS MÍNIMAS - Sistema de detección y extinción automática** | | | |
| **Nombre del Bien o Servicio Conexo** | **Descripción Técnica** | **Mínimo Exigido** | **El bien ofertado cumple con las especificaciones requeridas (SI/NO)** |
| **Marca:** | **Especificar** | |  |
| **Modelo:** | **Especificar** | |  |
| **Procedencia:** | **Especificar** | |  |
| **Cantidad:** | **01 (uno)** | **Exigido** |  |
| **Descripción:** | **Sistema de detección y extinción de incendios automática para Sala Equipos del DC** | **Exigido** |  |
| **Cañerías** | Deben estar construidas de acero. El espesor de todos los ductos deberá ser el necesario para aguantar la presión del gas en toda su trayectoria y deberá ser mencionado por cada oferente. | Exigido |  |
| Todos los ductos y accesorios deben estar galvanizados o tendrán otras protecciones especiales contra la corrosión atmosférica. | Exigido |  |
| El diámetro de los mismos deberá ser determinado por el cálculo hecho por un software específico para este tipo de aplicaciones que sea certificado UL. | Exigido |  |
| Si la oferta implica la instalación de varios contenedores, los mismos deberán tener el mismo tamaño y tener la misma carga, en caso de realizar arreglos múltiples. Otra opción para el tendido del sistema de cañerías es realizar ductos individuales desde los contenedores hasta los difusores. | Exigido |  |
| Durante la instalación todos los materiales deberán estar almacenados en un ambiente seco y después de realizado el proceso de corte y enroscado, deberán removerse de los caños y accesorios, todo rastro de aceite, grasas y otros residuos utilizando soluciones desgrasantes. | Exigido |  |
| Todo el sistema de cañerías ya sea vertical u horizontal deberá estar convenientemente sujetada a la estructura de Hormigón Armado, paredes o techos. | Exigido |  |
| Se utilizarán abrazaderas metálicas que deberán soportar los ductos bajo todas condiciones de operación y servicio. Ellas deben permitir la expansión y contracción de la cañería y prevenir tensiones excesivas. Las abrazaderas deben estar ancladas a la estructura del edificio y evitar así el movimiento longitudinal o lateral del sistema de cañerías, así como el balanceo de las mismas. | Exigido |  |
| Se deben tener en cuenta las fuerzas ejercidas en los contenedores y el sistema de cañerías durante la descarga. Cada sección de los ductos debe estar asegurada previniendo el movimiento vertical o lateral. Un soporte adicional deberá colocarse en las cercanías de cada difusor (nozzle) para soportar la fuerza generada durante la descarga del sistema. Ninguna sección o segmento de cañerías deberá colocarse sin abrazadera o soporte. | Exigido |  |
| No se aceptarán conexiones enroscadas simplemente acopladas sino en toda la longitud de la unión o accesorio. Cada conexión debe estar convenientemente limpiada y removida de todo residuo. | Exigido |  |
| Durante el ensamblaje de las cañerías deberá utilizarse cinta Teflón. Las uniones deberán estar sujetadas para soportar las presiones alcanzadas. | Exigido |  |
| **Sistema de Extinción** | El sistema de extinción de incendios utilizando gas extintor del tipo ecológico, deberá estar conectado al sistema de detección electrónica de incendios, a ser proveído conforme a las características citadas más arriba. | Exigido |  |
| El panel de extinción deberá ser un equipo fabricado específicamente para uso como sistema de extinción automática, y deberá estar listado UL, y FM. | Exigido |  |
| El mismo deberá contar con: | Exigido |  |
| Dos circuitos de detección. | Exigido |  |
| Dos circuitos de salidas NACs o de señalización | Exigido |  |
| Dos circuitos de Salidas de descarga o conexión a electroválvula. | Exigido |  |
| Tres salidas de rele tipo C programables. | Exigido |  |
| Una salida de alimentación auxiliar permanente. | Exigido |  |
| El sistema contra incendios deberá operar de la siguiente manera: | Exigido |  |
| • Nivel Uno: | Exigido |  |
| El Data Center estará convenientemente protegido mediante detectores de humo y calor, ubicados estratégicamente. Cuando uno de los detectores o una zona del equipo de detección es activado por la presencia de humo en las instalaciones, las señales son enviadas al Panel Central, el cual debe realizar una serie de acciones: cortar el sistema de ventilación, hacer sonar alarmas y como medida de precaución, el sistema espera por una segunda alarma. | Exigido |  |
| • Nivel Dos: | Exigido |  |
| Cuando el segundo detector de humo o la segunda zona de detectores se activa, suena una alarma adicional y comienza una cuenta regresiva de 30 segundos (este tiempo es programable hasta 180 segundos) para liberar el gas. Durante los 30 segundos, la inminente descarga se puede cancelar. Al finalizar la cuenta, el gas es liberado para detener la reacción química del fuego. El gas almacenado es introducido al área a través del sistema de cañerías y los difusores (nozzles). El mismo debe alcanzar una concentración del 7 % en un máximo de diez segundos y debe suprimir rápidamente el fuego. | Exigido |  |
| El sistema debe contar con la posibilidad de que el agente extintor sea liberado en forma automática en la forma indicada más arriba, o en forma manual. | Exigido |  |
| Una unidad de descarga eléctrica accionada manualmente debe ser proveída e instalada en el acceso al Datacenter. Esta unidad debe estar claramente señalizada. A través de la misma, se puede colocar al sistema en forma manual o en forma automática | Exigido |  |
| **Accesorios del sistema** | Mangueras de descarga: |  |  |
| Para conectar la válvula a la cañería vertical u horizontal se usarán mangueras de descarga flexibles. Si la oferta incluye un sistema de múltiples contenedores, se deberán instalar válvulas de chequeo dentro de los ductos para prevenir la descarga del agente extintor a través de las mangueras que deban ser desconectadas del sistema de cañerías para revisiones de los contenedores o por algún otro motivo. | Exigido |  |
| Contacto operado a presión: |  |  |
| Un contacto operado a presión debe estar conectado a la válvula del contenedor o al arreglo múltiple con el objeto de señalar la descarga del sistema, operar alarmas, causar el apagado del sistema, etc. cuando el sistema se active. | Exigido |  |
| Solenoide eléctrico: | Exigido |  |
| Utilizado para accionar el mecanismo de descarga. Este solenoide debe estar conectado eléctricamente al Panel Central de Detección de incendios. | Exigido |  |
| Difusores: | Exigido |  |
| El área para proteger deberá contar con dos difusores conectados al o a los contenedores del gas. Material de construcción debe ser aluminio. Los difusores deben estar ubicados en el techo del local y en el piso falso y deben dispersar el agente extintor en 360° grados. Deben estar diseñados para completar la descarga en 10 segundos o menos. | Exigido |  |
| **Agente extintor** | Características: | Exigido |  |
| Tipo: FM200, ≥ 150 Kg. | Exigido |  |
| Ecológicamente limpio y eficaz. | Exigido |  |
| Poder destructor de la capa de ozono: cero. | Exigido |  |
| Seguro para áreas ocupadas. Respirable. | Exigido |  |
| No tóxico para las personas. | Exigido |  |
| Gas limpio. No deja residuos para su limpieza posterior. | Exigido |  |
| Tiempo de descarga de 10 segundos o menos. | Exigido |  |
| No conductor de la electricidad | Exigido |  |
| No debe provocar choque térmico. | Exigido |  |
| No debe degradar el patrimonio custodiado. | Exigido |  |
| No debe producir daños a instrumentos y equipamientos sensibles. | Exigido |  |
| Apto para fuegos de clase A (materiales sólidos). | Exigido |  |
| Debe estar presurizado con Nitrógeno a la presión de 24 bar. a 20° C. | Exigido |  |
| Debe estar almacenado en un número reducido de cilindros de acero. | Exigido |  |
| Debe estar almacenado a presión en fase líquida (gas licuado). Se descarga a través de la red de tuberías hasta los difusores situados en el riesgo expandiéndose y convirtiéndose en gas. | Exigido |  |
| El área protegida debe ser inundada por el gas con una concentración del 7 %. | Exigido |  |
| Normas: ISO – UL y NFPA 2001 | Exigido |  |
| Pruebas. | Exigido |  |
| Una vez completado el sistema de cañerías y antes de la conexión de los contenedores, difusores, etc. se realizarán pruebas para verificar la existencia o no, de pérdidas en las cañerías. | Exigido |  |
| Se deberá aplicar una presión de 7 bar con nitrógeno o aire por espacio de 10 minutos, una vez que estén cerradas todas las salidas del sistema de cañerías. | Exigido |  |
| La caída de presión no deberá ser mayor de 0,5 bar después de 10 minutos. | Exigido |  |
| Bajo ninguna condición agua deberá ser usada en las pruebas. | Exigido |  |
| También, se verificarán todas las uniones y los soportes en toda la trayectoria de las cañerías. | Exigido |  |
| Todas las pruebas de los circuitos eléctricos del sistema de extinción deben ser realizadas de conformidad con manual del panel central de control del sistema de detección, con el fin de comprobar la activación del solenoide. Todas estas pruebas realizadas en el sistema eléctrico deben ser hechas con el solenoide desconectado de la válvula. | Exigido |  |
| Instalación | Debe estar incluida la instalación de todo el sistema en sistema llave en mano. Todas las adecuaciones civiles requeridas deberán estar incluidas en la oferta. | Exigido |  |
| Mantenimiento Preventivo | Se debe incluir en la oferta un mantenimiento preventivo mensual de todo el sistema por un periodo de 12 meses una vez concluida la instalación. | Exigido |  |

**Ítem 9: Sistema de detección y extinción de incendios automática Sala de Energía**

|  |  |  |  |
| --- | --- | --- | --- |
| **ESPECIFICACIONES TÉCNICAS MÍNIMAS - Sistema de detección y extinción automática** | | | |
| **Nombre del Bien o Servicio Conexo** | **Descripción Técnica** | **Mínimo Exigido** | **El bien ofertado cumple con las especificaciones requeridas (SI/NO)** |
| **Marca:** | **Especificar** | |  |
| **Modelo:** | **Especificar** | |  |
| **Procedencia:** | **Especificar** | |  |
| **Cantidad:** | **01 (uno)** | **Exigido** |  |
| **Descripción:** | **Sistema de detección y extinción de incendios automática para Sala Energía.** | **Exigido** |  |
| **Cañerías** | Deben estar construidas de acero. El espesor de todos los ductos deberá ser el necesario para aguantar la presión del gas en toda su trayectoria y deberá ser mencionado por cada oferente. | Exigido |  |
| Todos los ductos y accesorios deben estar galvanizados o tendrán otras protecciones especiales contra la corrosión atmosférica. | Exigido |  |
| El diámetro de los mismos deberá ser determinado por el cálculo hecho por un software específico para este tipo de aplicaciones que sea certificado UL. | Exigido |  |
| Si la oferta implica la instalación de varios contenedores, los mismos deberán tener el mismo tamaño y tener la misma carga, en caso de realizar arreglos múltiples. Otra opción para el tendido del sistema de cañerías es realizar ductos individuales desde los contenedores hasta los difusores. | Exigido |  |
| Durante la instalación todos los materiales deberán estar almacenados en un ambiente seco y después de realizado el proceso de corte y enroscado, deberán removerse de los caños y accesorios, todo rastro de aceite, grasas y otros residuos utilizando soluciones desgrasantes. | Exigido |  |
| Todo el sistema de cañerías ya sea vertical u horizontal deberá estar convenientemente sujetada a la estructura de Hormigón Armado, paredes o techos. | Exigido |  |
| Se utilizarán abrazaderas metálicas que deberán soportar los ductos bajo todas condiciones de operación y servicio. Ellas deben permitir la expansión y contracción de la cañería y prevenir tensiones excesivas. Las abrazaderas deben estar ancladas a la estructura del edificio y evitar así el movimiento longitudinal o lateral del sistema de cañerías, así como el balanceo de las mismas. | Exigido |  |
| Se deben tener en cuenta las fuerzas ejercidas en los contenedores y el sistema de cañerías durante la descarga. Cada sección de los ductos debe estar asegurada previniendo el movimiento vertical o lateral. Un soporte adicional deberá colocarse en las cercanías de cada difusor (nozzle) para soportar la fuerza generada durante la descarga del sistema. Ninguna sección o segmento de cañerías deberá colocarse sin abrazadera o soporte. | Exigido |  |
| No se aceptarán conexiones enroscadas simplemente acopladas sino en toda la longitud de la unión o accesorio. Cada conexión debe estar convenientemente limpiada y removida de todo residuo. | Exigido |  |
| Durante el ensamblaje de las cañerías deberá utilizarse cinta Teflón. Las uniones deberán estar sujetadas para soportar las presiones alcanzadas. | Exigido |  |
| **Sistema de Extinción** | El sistema de extinción de incendios utilizando gas extintor del tipo ecológico, deberá estar conectado al sistema de detección electrónica de incendios, a ser proveído conforme a las características citadas más arriba. | Exigido |  |
| El panel de extinción deberá ser un equipo fabricado específicamente para uso como sistema de extinción automática, y deberá estar listado UL, y FM. | Exigido |  |
| El mismo deberá contar con: | Exigido |  |
| Dos circuitos de detección. | Exigido |  |
| Dos circuitos de salidas NACs o de señalización | Exigido |  |
| Dos circuitos de Salidas de descarga o conexión a electroválvula. | Exigido |  |
| Tres salidas de rele tipo C programables. | Exigido |  |
| Una salida de alimentación auxiliar permanente. | Exigido |  |
| El sistema contra incendios deberá operar de la siguiente manera: | Exigido |  |
| • Nivel Uno: | Exigido |  |
| El Data Center estará convenientemente protegido mediante detectores de humo y calor, ubicados estratégicamente. Cuando uno de los detectores o una zona del equipo de detección es activado por la presencia de humo en las instalaciones, las señales son enviadas al Panel Central, el cual debe realizar una serie de acciones: cortar el sistema de ventilación, hacer sonar alarmas y como medida de precaución, el sistema espera por una segunda alarma. | Exigido |  |
| • Nivel Dos: | Exigido |  |
| Cuando el segundo detector de humo o la segunda zona de detectores se activa, suena una alarma adicional y comienza una cuenta regresiva de 30 segundos (este tiempo es programable hasta 180 segundos) para liberar el gas. Durante los 30 segundos, la inminente descarga se puede cancelar. Al finalizar la cuenta, el gas es liberado para detener la reacción química del fuego. El gas almacenado es introducido al área a través del sistema de cañerías y los difusores (nozzles). El mismo debe alcanzar una concentración del 7 % en un máximo de diez segundos y debe suprimir rápidamente el fuego. | Exigido |  |
| El sistema debe contar con la posibilidad de que el agente extintor sea liberado en forma automática en la forma indicada más arriba, o en forma manual. | Exigido |  |
| Una unidad de descarga eléctrica accionada manualmente debe ser proveída e instalada en el acceso al Datacenter. Esta unidad debe estar claramente señalizada. A través de la misma, se puede colocar al sistema en forma manual o en forma automática | Exigido |  |
| **Accesorios del sistema** | Mangueras de descarga: |  |  |
| Para conectar la válvula a la cañería vertical u horizontal se usarán mangueras de descarga flexibles. Si la oferta incluye un sistema de múltiples contenedores, se deberán instalar válvulas de chequeo dentro de los ductos para prevenir la descarga del agente extintor a través de las mangueras que deban ser desconectadas del sistema de cañerías para revisiones de los contenedores o por algún otro motivo. | Exigido |  |
| Contacto operado a presión: |  |  |
| Un contacto operado a presión debe estar conectado a la válvula del contenedor o al arreglo múltiple con el objeto de señalar la descarga del sistema, operar alarmas, causar el apagado del sistema, etc. cuando el sistema se active. | Exigido |  |
| Solenoide eléctrico: | Exigido |  |
| Utilizado para accionar el mecanismo de descarga. Este solenoide debe estar conectado eléctricamente al Panel Central de Detección de Incendios. | Exigido |  |
| Difusores: | Exigido |  |
| El área para proteger deberá contar con dos difusores conectados al o a los contenedores del gas. Material de construcción debe ser aluminio. Los difusores deben estar ubicados en el techo del local y en el piso falso y deben dispersar el agente extintor en 360° grados. Deben estar diseñados para completar la descarga en 10 segundos o menos. | Exigido |  |
| **Agente extintor** | Características: | Exigido |  |
| Tipo: FM200, ≥ 35 Kg. | Exigido |  |
| Ecológicamente limpio y eficaz. | Exigido |  |
| Poder destructor de la capa de ozono: cero. | Exigido |  |
| Seguro para áreas ocupadas. Respirable. | Exigido |  |
| No tóxico para las personas. | Exigido |  |
| Gas limpio. No deja residuos para su limpieza posterior. | Exigido |  |
| Tiempo de descarga de 10 segundos o menos. | Exigido |  |
| No conductor de la electricidad | Exigido |  |
| No debe provocar choque térmico. | Exigido |  |
| No debe degradar el patrimonio custodiado. | Exigido |  |
| No debe producir daños a instrumentos y equipamientos sensibles. | Exigido |  |
| Apto para fuegos de clase A (materiales sólidos). | Exigido |  |
| Debe estar presurizado con Nitrógeno a la presión de 24 bar a 20° C. | Exigido |  |
| Debe estar almacenado en un número reducido de cilindros de acero. | Exigido |  |
| Debe estar almacenado a presión en fase líquida (gas licuado). Se descarga a través de la red de tuberías hasta los difusores situados en el riesgo expandiéndose y convirtiéndose en gas. | Exigido |  |
| El área protegida debe ser inundada por el gas con una concentración del 7 %. | Exigido |  |
| Normas: ISO – UL y NFPA 2001 | Exigido |  |
| Pruebas. | Exigido |  |
| Una vez completado el sistema de cañerías y antes de la conexión de los contenedores, difusores, etc. se realizarán pruebas para verificar la existencia o no, de pérdidas en las cañerías. | Exigido |  |
| Se deberá aplicar una presión de 7 bar con nitrógeno o aire por espacio de 10 minutos, una vez que estén cerradas todas las salidas del sistema de cañerías. | Exigido |  |
| La caída de presión no deberá ser mayor de 0,5 bar después de 10 minutos. | Exigido |  |
| Bajo ninguna condición agua deberá ser usada en las pruebas. | Exigido |  |
| También, se verificarán todas las uniones y los soportes en toda la trayectoria de las cañerías. | Exigido |  |
| Todas las pruebas de los circuitos eléctricos del sistema de extinción deben ser realizadas de conformidad con manual del panel central de control del sistema de detección, con el fin de comprobar la activación del solenoide. Todas estas pruebas realizadas en el sistema eléctrico deben ser hechas con el solenoide desconectado de la válvula. | Exigido |  |
| Instalación | Debe estar incluida la instalación de todo el sistema en sistema llave en mano. Todas las adecuaciones civiles requeridas deberán estar incluidas en la oferta. | Exigido |  |
| Mantenimiento Preventivo | Se debe incluir en la oferta un mantenimiento preventivo mensual de todo el sistema por un periodo de 12 meses una vez concluida la instalación. | Exigido |  |

**Ítem 10: Readecuación del Data Center**

|  |  |  |  |
| --- | --- | --- | --- |
| **ESPECIFICACIONES TÉCNICAS MÍNIMAS** | | | |
| **Nombre del Bien o Servicio Conexo** | **Descripción Técnica** | **Mínimo Exigido** | **El bien ofertado cumple con las especificaciones requeridas (SI/NO)** |
| **Marca:** | **Especificar** | |  |
| **Modelo:** | **Especificar** | |  |
| **Procedencia:** | **Especificar** | |  |
| **Cantidad:** | **01 (uno)** | **Exigido** |  |
| **Descripción** | **Readecuaciones Data Center** | **Exigido** |  |
| **Piso Técnico** | En las áreas previstas para el Datacenter, el NOC, Sala de Energía y Sala de Archivos deberán reemplazarse los pisos elevados con terminación metálica y relleno sólido anti-llama, el área a cubrir es de 120 m2, esta dimensión es referencial, el oferente deberá verificar la misma en la visita técnica a realizarse en el local | **Exigido** |  |
| El ensamblado deberá ser perfecto, con posibilidad de realizar cambios en la ubicación de las unidades, el sistema de piso elevado deberá prever refuerzos especiales en los sitios donde soportaran la carga de los servidores, la distribución de los mismos se realizará conforme a las necesidades y conforme las indicaciones de los técnicos de la Convocante | **Exigido** |  |
| Debe cumplir con el Estándar NFPA 75, TIA-942, EIA-TIA 609 | **Exigido** |  |
| Las dimensiones de las placas son de 600 x 600 mm con espesura de 30 o 32 mm | **Exigido** |  |
| Deben de estar hechos de una variedad de materiales que combinan propiedades de dureza, anti-llamas y propiedades antiestática | **Exigido** |  |
| Crucetas y bases: Sirven de acoplamiento esférico de encaje invertido para acomodación perfecta de las placas, garantiza un riguroso trabamiento y nivelación de los cantos. Su principal función es transferir y distribuir la carga recibida, garantizando la estabilidad y equilibrio del conjunto | **Exigido** |  |
| El material de las mismas debería ser no inflamable y especialmente tratado para retardo en caso de incendio | **Exigido** |  |
| Todo el piso debe ser eléctricamente continuo y debe estar completamente puesto a tierra | **Exigido** |  |
| El estándar TIA-942 recomienda soportar cargas distribuidas de piso de 250 lbf/ft2 (12kPA) (con una carga mínima permitida de 150 lbf/ft2 [7.2 kPA]) | **Exigido** |  |
| Bases: Su principal función es transferir y distribuir la carga recibida, garantizan la estabilidad y equilibrio del conjunto. Ella está compuesta de tubo de acero al carbono de una base determinada y altura variable | **Exigido** |  |
| Debe tener posibilidad de realizar cambios en la ubicación de las unidades, por medio de un mango con ventosas que deberá ser incluido en la oferta | **Exigido** |  |
| Por el piso falso deben circular los cables de comunicación entre todas las unidades, ubicarse las cajas de conexión y los cables de alimentación eléctrica | **Exigido** |  |
| Los materiales del Piso técnico deben ser: de acero relleno de concreto celular y revestimiento de laminado plástico o melamínico. Será de bases ajustables en acero galvanizado | **Exigido** |  |
| La convocante se reserva el derecho de solicitar una demostración de los bienes ofertados si fuese necesario | **Exigido** |  |
| **Obras civiles** | Revoque y pintura de paredes del Data Center y el NOC con pintura sintética anti-llamas | **Exigido** |  |
| Reemplazo de cielo raso en el Data Center | **Exigido** |  |
| Reemplazo de iluminación del Data Center por artefactos de tipo LED | **Exigido** |  |
| **Limpieza** | Limpieza Integral del Data Center | **Exigido** |  |
| **Recertificación de puntos de red** | Recertificación de 24 (veinticuatro) puntos de red dentro del Data Center y el NOC. (Ver Anexo I) | **Exigido** |  |
| **AA de precisión** | Mantenimiento Preventivo del equipo de AA de precisión de la marca Caross. 4 (cuatro) mantenimientos preventivos semestrales | **Exigido** |  |
| **AA de confort** | Mantenimiento Preventivo y Correctivo de los equipos de AA de confort. 12 (doce) mantenimientos preventivos semestrales que incluyan limpieza de la unidad evaporadora, condensadora, limpieza de filtros, verificación del nivel de gas refrigerante, verificación de capacitores, etc. | **Exigido** |  |

**Ítem 11: Licencias de Virtualización**

|  |  |  |  |
| --- | --- | --- | --- |
| **ESPECIFICACIONES TÉCNICAS MÍNIMAS** | | | |
| **Nombre del Bien o Servicio Conexo** | **Descripción Técnica** | **Mínimo Exigido** | **El bien ofertado cumple con las especificaciones requeridas (SI/NO)** |
| **Marca:** | **Especificar** | |  |
| **Modelo:** | **Especificar** | |  |
| **Procedencia:** | **Especificar** | |  |
| **Cantidad:** | **3 (Tres)** | **Exigido** |  |
| **Descripción** | **Licencias de virtualización** | **Exigido** |  |
| Licencia de VMware vSphere Essentials Plus Kit + Vmware vSPhere: instalación, configuración y administración V6. | **Exigido** |  |
| **Soporte** | Support/Subscription VMware vSphere Essentials Plus Kit + Vmware vSPhere for 1 year. | **Exigido** |  |

**Ítem 12: Mantenimiento del Datacenter**

**Ítem Contrato Abierto por cantidades mínimas y máximas**

|  |  |  |  |
| --- | --- | --- | --- |
| **ESPECIFICACIONES TÉCNICAS MÍNIMAS** | | | |
| **Nombre del Bien o Servicio Conexo** | **Descripción Técnica** | **Mínimo Exigido** | **El bien ofertado cumple con las especificaciones requeridas (SI/NO)** |
| **Cantidad Mínima** | **200 (doscientas) horas** | **Exigido** |  |
| **Cantidad Máxima** | **400 (cuatrocientas) horas.** | **Exigido** |  |
| **Descripción** | **Soporte técnico preventivo y correctivo** | **Exigido** |  |
| **Cantidad:** | Soporte técnico preventivo y correctivo bajo demanda, para garantizar el correcto funcionamiento de toda la infraestructura del Datacenter. | **Exigido** |  |

**Plan de Entrega y realización de los servicios**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ITEM** | **DESCRIPCION** | **UNIDAD DE MEDIDA** | **CANTIDAD** | **PLAZO Y LUGAR DE ENTREGA** | | |
| **PLAZO** | LUGAR |
| 1 | Router de borde | Unidad | 2 | 60 (sesenta) Días calendarios, a partir de la recepción orden de compra | Dirección General de Firma Digital y Comercio Electrónico. Ministerio de Industria y Comercio (MIC). Cap. Pedro Villamayor esq. Cap. Nicolas Blinoff. Asunción – Paraguay. |
| 2 | Servidor | Unidad | 3 | 60 (sesenta) Días calendarios, a partir de la recepción de la orden de compra |
| 3 | Storage | Unidad | 1 | 60 (sesenta) Días calendarios, a partir de la recepción de la orden de compra |
| 4 | UPS 40 KVA | Unidad | 1 | 60 (sesenta) Días calendarios, a partir de la recepción de la orden de compra |
| 5 | Sistema de CCTV | Unidad | 1 | 60 (sesenta) Días calendarios, a partir de la recepción de la orden de compra |
| 6 | Sistema de Control de Acceso | Unidad | 1 | 60 (sesenta) Días calendarios, a partir de la recepción de la orden de compra |
| 7 | Pantalla NOC (2x2) | Unidad | 1 | 60 (sesenta) Días calendarios, a partir de la recepción de la orden de compra |
| 8 | Sistema de detección y extinción de incendios automática (Sala de Equipos) | Unidad | 1 | 60 (sesenta) Días calendarios, a partir de la recepción de la orden de compra |
| 9 | Sistema de detección y extinción de incendios automática (Sala de Energía) | Unidad | 1 | 60 (sesenta) Días calendarios, a partir de la recepción de la orden de compra |
| 10 | Readecuación del Data Center | Unidad | 1 | 90 (noventa) Días calendarios, a partir de la recepción de la orden de compra |
| 11 | Licencia de virtualización | Unidad | 3 | 30 (treinta) Días calendarios, a partir de la recepción de la orden de compra |
| 12 | Mantenimiento del Data Center | Horas | Conforme a la necesidad | 2 (horas) contados a partir de recepción de la solicitud de realización del mantenimiento. |

1. Planos o Diseños:

El plano se encuentra se encuentra adjunto al presente documento.

1. Indicadores de Cumplimiento de Contrato

Los documentos requeridos para acreditar el cumplimiento contractual serán:

1. Nota de Remisión de los bienes emitido por el proveedor.
2. Acta de Recepción Definitiva emitida por el MIC.

Serán presentados 1 nota de remisión y 1 Acta de Recepción Definitiva por cada entrega realizada.

**Frecuencia:** Única

**Planificación de indicadores de cumplimiento:**

|  |  |  |
| --- | --- | --- |
| **INDICADOR** | **TIPO** | **FECHA DE PRESENTACIÓN PREVISTA** |
| Nota de Remisión (Solo a efectos de certificar la entrega de los Bienes) o Nota de realización de los servicios en caso de servicios (solo a efectos de certificar la realización de los servicios) | Nota de Remisión | Dentro del plazo de entrega y realización de los servicios previsto. |
| Acta de Recepción Definitiva (Verificado el cumplimiento de las especificaciones técnicas). | Acta de recepción Definitiva | Dentro de los 15 días hábiles de la recepción de los bienes o realización de los servicios. |

SECCIÓN IV.

CONDICIONES ESPECIALES DEL CONTRATO (CEC)

Las siguientes Condiciones Especiales del Contrato (CEC) complementarán y/o enmendarán las Condiciones Generales del Contrato (CGC) que se encuentran publicadas en el Portal de Contrataciones Públicas y forman parte de los documentos de la Subasta. En caso de haber conflicto, las provisiones aquí dispuestas prevalecerán sobre las de las CGC.

|  |  |
| --- | --- |
| **CGC 4.2 (b)** | La versión de la edición de los Incoterms será*:* **NO APLICA** |
| **CGC 7** | Para notificaciones, la dirección del Contratante será:  Atención: Dirección de Contrataciones del Ministerio de Industria y Comercio.  Dirección: Avda. Mcal. López Nº 3.333 e/ Salaskin y Dr. Weiss  Piso/Oficina: Planta Baja  Ciudad: Asunción, Paraguay  Teléfono: 021 - 616 3184/6  Fax: 021 - 616 3184/6  Dirección electrónica: nelson.galvan@mic.gov.py |
| **CGC 9.6** | El mecanismo formal de resolución de conflictos será: conforme a lo establecido en la Ley 2051/03 de Contrataciones Públicas. No se utilizará el arbitraje. |
| **CGC 11** | Detalle de los documentos de Embarque y otros documentos que deben ser proporcionados por el Proveedor son: **NO APLICA.**  La Contratante deberá recibir los documentos arriba mencionados antes de la llegada de los Bienes; si no recibe dichos documentos, todos los gastos consecuentes correrán por cuenta del Proveedor. |
| **CGC 14** | **El precio del contrato estará sujeto a reajustes.**  La fórmula y el procedimiento para el reajuste será el siguiente: Los precios ofertados estarán sujetos a reajustes siempre y cuando se haya reflejado una variación del Dólar Americano igual o superior a 500 puntos referente a la fecha de apertura física de las ofertas, conforme a la siguiente fórmula:  **P= PoxC**  **Co**  **Donde:**  P=Precio reajustado de la Oferta  Po= Precio original de la oferta  C=Tipo de cambio del Mercado Libre Fluctuante (venta) del dólar emitido por el Banco Central del Paraguay correspondiente al día anterior de la emisión de la factura.  Los reajustes deberán ser solicitados por escrito al MIC, por el Proveedor. La solicitud debe realizarse indefectiblemente dentro del mes siguiente al cual se produjeron las variaciones, bajo pena de no poder solicitarlo posteriormente. No se reconocerán reajustes de precios si el suministro se encuentra atrasado respecto al plazo de entrega establecido. El reajuste tendrá aplicación sobre los bienes entregados posteriores al mes en el cual se produjeron las variaciones, previa resolución de la máxima autoridad de la Institución. |
| **CGC 15.1; 15.2 y 15.3** | Las formas y condiciones de pago al Proveedor en virtud del Contrato serán las siguientes: Los pagos serán en guaraníes, conforme al plan de caja efectivamente transferidos por el Ministerio de Hacienda para el Ministerio de Industria y Comercio.  Las facturas serán recepcionadas en la Dirección General de Administración y Finanzas del Ministerio de Industria y Comercio.  Los pagos serán dentro de los 60 días de recibidas la factura y remisión correspondientes.  El oferente deberá dar cumplimiento al Art. 41 de la Ley N° 3439/07 “De Contrataciones Públicas” que establece una contribución sobre contratos suscriptos equivalente al cero punto cuatro por ciento (0.4%) sobre el importe de cada factura o certificado de obra.  Para solicitar el pago, el proveedor adjudicado deberá presentar:  Una nota de solicitud pago dirigido a la Dirección General de Administración y Finanzas del MIC acompañado de la factura correspondiente debidamente completada, el Acta de Recepción Definitiva, el Certificado de Cumplimiento Tributario al día, el Certificado de Cumplimiento con el Seguro Social (IPS) al día, y el Formulario FIS – FIP autenticado.  El proveedor deberá emitir y remitir a la Institución, el recibo de cancelación por la transferencia recibida en su cuenta corriente, dentro de los 15 (quince) días hábiles, posterior a la fecha de acreditación. |
| **CGC 15.5** | Todos los pagos se efectuarán en Guaraníes. |
| **CGC 15.6** | En caso de mora de los pagos previstos en la CEC 15.6 por parte de la Convocante, la tasa de interés que se aplicará es del (0,5) % (Cero coma cinco por ciento) por cada día de atraso hasta que haya efectuado el pago completo. La mora será computada a partir del día siguiente del vencimiento del pago. |
| **CGC 16.1** | No se otorgará Anticipo Financiero. |
| **CGC 17.1** | El Proveedor será responsable del pago de todos los impuestos y otros tributos o gravámenes. |
| **CGC 18.1 y 18.2** | El valor de la Garantía de Fiel cumplimiento de contrato, es del 10 % (diez por ciento) del valor total del contrato. La Garantía de cumplimiento de Contrato deberá ser presentada por el Contratista dentro de los 10 días siguientes a partir de la fecha de suscripción del Contrato, de conformidad a lo dispuesto en el Art. 39 de la Ley 2051/03. La Garantía de fiel cumplimiento de contrato deberá tener un plazo mínimo de 120 días contados a partir de la fecha de suscripción del contrato. Si en dicho plazo no se ha realizado el cumplimiento total de las obligaciones el proveedor deberá prorrogar la garantía de fiel cumplimiento conforme al plazo indicado por el Ministerio de Industria y Comercio hasta el cumplimiento total de las obligaciones. |
| **CGC 18.5** | La liberación de la Garantía de Cumplimiento tendrá lugar: La Garantía de Cumplimento será liberada por la Contratante y devuelta al Proveedor, a requerimiento de parte, a más tardar treinta (30) días contados a partir de la fecha de Cumplimiento de las obligaciones del Proveedor en virtud del Contrato, incluyendo cualquier obligación relativa a la garantía de los bienes. |
| **CGC 22.3** | Se admitirá la subcontratación para la ejecución del ítem 10 – Readecuación del Data Center siempre y cuando el porcentaje no exceda el 60% del monto total del contrato.  El proveedor sólo podrá concertar con un tercero la ejecución parcial del contrato cuando éste tengan capacidad para contratar y no esté comprendido en alguna de las causales de prohibición señaladas en el Artículo 40.  El subcontratista sólo ostentará derechos frente al proveedor por razón de la subcontratación y en ningún caso frente al contratante.  Frente a la Contratante responderá siempre el proveedor de todas las obligaciones que le correspondan por razón del contrato.  En cualquier caso de subcontratación, cesión de hecho o de derecho o delegación, serán siempre solidarias las obligaciones subcontratadas, cedidas o delegadas.  El Contratista seguirá siendo totalmente responsable de los actos, deficiencias y negligencias de todo subcontratista, sus representantes, empleados o trabajadores, en la misma medida que si se tratara de sus propios actos, deficiencias o negligencias o de las de sus propios representantes, empleados o trabajadores.  En el caso de que el proveedor cuente con un subcontratista para la ejecución del ítem 10 – Readecuación del Data Center deberá presentar dentro de los 10 (diez) dias de la firma del Contrato los siguientes documentos:  1 – Contrato de subcontratación entre el proveedor y el subcontratista para la Ejecución del Ítem 10 – Readecuación del Data Center.  2 – Listado de Personales asignados para la realización del Servicio.  3 – Listado de materiales con sus correspondientes marcas y procedencias que serán utilizados para la realización de los servicios, los cuales serán aprobados por el Fiscal designado por la institución.  4 – Listado de maquinarias, equipos y herramientas que utilizará para la realización de los servicios.  La Administración del Contrato realizará el analisis del cumplimiento de las documentaciones presentadas y será la encargada de la aprobación del Subcontratista que será informado al proveedor adjudicado.  El retraso de la presentación de las documentaciones generará multas establecidas en la CGC 28. Pudiendo ser causal de recisión del contrato imputable al proveedor. |
| **CGC 24.2** | El embalaje, la identificación y la documentación dentro y fuera de los paquetes serán como se indica a continuación: NO APLICA. |
| **CGC 25** | La cobertura de seguro será según se establece en los Incoterms. NO APLICA. |
| **CGC 26** | El Proveedor está obligado bajo los términos del Contrato a transportar los Bienes al lugar en entrega, incluyendo seguro y almacenamiento, y tal como se estipulará en el Contrato, será contratado por el Proveedor, y todos los gastos relacionados estarán incluidos en el Precio del Contrato. |
| **CGC 27.1** | Las inspecciones y pruebas serán como se indica a continuación:  **Inspecciones de los Bienes y Servicios:**  Al momento de la recepción de los bienes o realización de los servicios la Dirección General de Firma Digital y Comercio Electrónico firmará en el caso de bienes la Nota de Remisión del Proveedor y en el caso de servicios la Nota comunicando la realización de los servicios por parte del proveedor al único efecto de certificar la entrega o realización del servicio.  Una vez que se realicen los controles pertinentes y certifique adecuadamente que el suministro o los servicios se ajusta a las Especificaciones Técnicas y demás documentos del Contrato, se emitirá el Acta de Recepción Definitiva o de realización de los servicios, que habilitará al proveedor a solicitar el pago.  **Inspección del ítem 10 – Readecuación del Data Center.**  Para la ejecución del ítem 10 – Readecuación del Data Center el Ministerio de Industria y Comercio designará a un fiscal quien será el encargado de verificar el cumplimiento de los servicios con la presentación de los informes que serán definidos en la etapa contractual.  Una vez que se realicen los controles pertinentes y certifique adecuadamente que el servicio se ajusta a las Especificaciones Técnicas y demás documentos del Contrato, se emitirá la Certificación de la readecuación realizada firmada por el fiscal y el administrador del contrato, que habilitará al proveedor a solicitar el pago. |
| **CGC 27.2** | Las inspecciones y pruebas se realizarán en la oficina de la Dirección General de Firma Digital y Comercio Electrónico. Dirección: Capital Pedro Villamayor esquina Capitan Nicolas Blinoff. |
| **CGC 28** | El valor de las multas será del 1 % (uno por ciento) del monto total del item por cada día de atraso en la entrega de los bienes o prestación de los servicios contratados.  Asimismo, se aplicará el porcentaje de 0,1 % (cero coma uno por ciento) del monto total del contrato por cada día de atraso del plazo establecido por en el Pliego de Bases y condiciones o por el Administrador del contrato para la entrega de documentaciones o informaciones requeridas por la Convocante al proveedor. |
| **CGC 29.3** | El período de validez de la Garantía será conforme al plazo establecido en las Especificaciones Técnicas. Para fines de la Garantía, el lugar de destino será la Sede Central del Ministerio de Industria y Comercio. Avda. Mcal Lopez Nº 3333 casi Dr. Weiss. |
| **CGC 29.5** | El plazo para reparar o reemplazar los bienes o servicios será de 10 (diez) días calendario contados a partir de la recepción de la Notificación de Incumplimiento realizada por el Ministerio de Industria y Comercio. Dicho plazo no será contemplado como una prorroga en la entrega por lo que se aplicará las multas establecidas en la CGC 28. |
| **CGC 35.1 (a) (vi)** | La Contratante podrá terminar el Contrato en lo casos establecidos en la CGC 35.1 y los Art. 57, 58, 59 y 60 de la Ley 2051/03 y en los casos establecidos en las Condiciones Especiales del Contrato. |

SECCIÓN V

**Modelo de Contrato N° \_\_\_\_\_\_\_**

Entre el MINISTERIO DE INDUSTRIA Y COMERCIO, domiciliada en la Avda. Mcal. López Nº 3.333 e/ Salaskin y Dr. Weiss, ciudad de Asunción de la República del Paraguay, representada para este acto por\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, con Cédula de Identidad N° \_\_\_\_\_\_\_\_, denominada en adelante la CONTRATANTE, por una parte, y, por la otra, la firma \_\_\_\_\_\_\_\_\_\_\_\_, domiciliada en \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, República del Paraguay, representada para este acto por \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, con Cédula de Identidad N° \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, denominada en adelante el PROVEEDOR, denominadas en conjunto "LAS PARTES" e, individualmente, "PARTE", acuerdan celebrar el presente "ADECUACION DEL DATA CENTER DE LA DIRECCION GENERAL DE FIRMA DIGITAL Y COMERCIO ELECTRONICO", el cual estará sujeto a las siguientes cláusulas y condiciones:

**1. OBJETO**.

El presente contrato se refiere a la “ADECUACION DE DATA CENTER DE LA DIRECCION GENERAL DE FIRMA DIGITAL Y COMERCIO ELECTRONICO”, que serán suministrados por el proveedor y cumplirá con las Especificaciones Técnicas detalladas en el programa de Suministros del Pliego de Bases y Condiciones, en las Especificaciones Técnicas y en la Planilla de Precios.

**2. DOCUMENTOS INTEGRANTES DEL CONTRATO.**

Los documentos contractuales firmados por las partes y que forman parte integral del Contrato son los siguientes:

(a) Contrato;

(b) El Pliego de Bases y Condiciones y sus Adendas o modificaciones;

(c) Las Instrucciones al Oferente (IAO) y las Condiciones Generales del Contrato (CGC) publicadas en el portal de Contrataciones Públicas;

(d) Los datos cargados en el SICP;

(e) La oferta del Proveedor;

(f) La resolución de adjudicación del Contrato emitida por la Contratante y su respectiva notificación;

(g) Garantía de Fiel Cumplimiento del Contrato.

Los documentos que forman parte del Contrato deberán considerarse mutuamente explicativos; en caso de contradicción o discrepancia entre los mismos, la prioridad se dará en el orden enunciado anteriormente, siempre que no contradigan las disposiciones del Pliego de Bases y Condiciones, en cuyo caso prevalecerá lo dispuesto en este”.

**3. IDENTIFICACIÓN DEL CRÉDITO PRESUPUESTARIO PARA CUBRIR EL COMPROMISO DERIVADO DEL CONTRATO**.

El crédito presupuestario para cubrir el compromiso derivado del presente Contrato está previsto conforme al Certificado de Disponibilidad Presupuestaria vinculado al Programa Anual de Contrataciones (PAC) con el ID Nº XXX.XXX

**4. PROCEDIMIENTO DE CONTRATACIÓN**

El presente Contrato es el resultado del procedimiento de Licitación Pública Nacional Nº 03/2019 por el Procedimiento de Subasta a la Baja Electrónica “Adecuación del Data Center de la Dirección General de Firma Digital y Comercio Electrónico” convocado por el Ministerio de Industria y Comercio. La adjudicación fue realizada según acto administrativo N°\_\_\_\_\_\_\_

**5. PRECIO UNITARIO Y EL IMPORTE TOTAL A PAGAR POR LOS BIENES y/o SERVICIOS.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Nro. De Orden | Nro. De Ítem/Lote | Descripción | Marca | Procedencia | Unidad de Medida | Cantidad | Precio Unitario | Monto Total |
|  |  |  |  |  |  |  |  |  |

Total: *[sumatoria]*

El monto total del presente contrato asciende a la suma de: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

El Proveedor se compromete a proveer los Bienes a la Contratante y a subsanar los defectos de éstos de conformidad a las disposiciones del Contrato.

La Contratante se compromete a pagar al Proveedor como contrapartida del suministro de los bienes y servicios y la subsanación de sus defectos, el Precio del Contrato o las sumas que resulten pagaderas de conformidad con lo dispuesto en las Condiciones Especiales del Contrato (CEC).

Para el ítem

**6. VIGENCIA DEL CONTRATO**

 El contrato entrará en vigor desde la fecha de suscripción hasta el cumplimiento total de las obligaciones.

**7. ESPECIFICACIONES TECNICAS PLAZO, LUGAR Y CONDICIONES DE LA PROVISIÓN DE BIENES.**

**A) Especificaciones técnicas.**

*(Conforme a los ítems adjudicados)*

**b) Plazo de Entrega de los Bienes y realización de los servicios.**

*(Conforme a los ítems adjudicados)*

**8. ADMINISTRACIÓN DEL CONTRATO.**

La administración del contrato estará a cargo de la Dirección General de Firma Digital y Comercio Electrónico.

**9. FORMA Y TÉRMINOS PARA GARANTIZA EL CUMPLIMIENTO DEL CONTRATO.**

La garantía para el fiel cumplimiento del contrato se regirá por lo establecido en las Condiciones Generales y Especiales del Contrato, la cual se presentará a más tardar dentro de los 10 (días) calendarios siguientes a la firma del contrato. La garantía de fiel cumplimiento debe ser equivalente al 10 % del monto total del contrato.-

**10. MULTAS.**

Las multas y otras penalidades que rigen en el presente contrato serán aplicadas conforme con las Condiciones Especiales y Generales del Contrato. Superado el monto equivalente a la Garantía de Fiel Cumplimiento de Contrato, la Contratante podrá aplicar el procedimiento de rescisión de contratos de conformidad al Artículo 59 inc. c) de la Ley N° 2.051/03 “De Contrataciones Públicas”, caso contrario deberá seguir aplicando el monto de las multas que correspondan.

La rescisión del contrato o la aplicación de multas por encima del porcentaje de la Garantía de Cumplimiento del Contrato deberá comunicarse a la DNCP a los fines previstos en el artículo 72 de la Ley N° 2051/03 “De Contrataciones Públicas”.

**11. CAUSALES Y PROCEDIMIENTO PARA SUSPENDER TEMPORALMENTE, DAR POR TERMINADO ANTICIPADAMENTE O RESCINDIR EL CONTRATO.**

Las causales y el procedimiento para suspender temporalmente, dar por terminado en forma anticipada o rescindir el contrato, son las establecidas en la Ley N° 2.051/03, y en las Condiciones Generales y Especiales del Contrato (CGC y CEC).

**12. SOLUCIÓN DE CONTROVERSIAS.**

Cualquier diferencia que surja durante la ejecución de los Contratos se dirimirá conforme las reglas establecidas en la legislación aplicable y en las Condiciones Generales y Especiales del Contrato.

**13. ANULACIÓN DE LA ADJUDICACIÓN**

Si la Dirección Nacional de Contrataciones Públicas resolviera anular la adjudicación de la Contratación debido a la procedencia de una protesta o investigación instaurada en contra del procedimiento, y si dicha nulidad afectara al Contrato ya suscrito entre LAS PARTES, el Contrato o la parte del mismo que sea afectado por la nulidad quedará automáticamente sin efecto, de pleno derecho, a partir de la comunicación oficial realizada por la D.N.C.P., debiendo asumir LAS PARTES las responsabilidades y obligaciones derivadas de lo ejecutado del contrato.

EN TESTIMONIO de conformidad se suscriben 3 (tres) ejemplares de un mismo tenor y a un solo efecto en la Ciudad de \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ República del Paraguay al día\_\_\_\_\_\_\_\_\_\_\_ mes\_\_\_\_\_\_\_\_\_\_\_ y año\_\_\_\_\_\_\_\_\_\_\_\_\_.

Firmado por: *[indicar firma]* en nombre de la Contratante.

Firmado por: *[indicar la(s) firma(s)]* en nombre del Proveedor.

LA SECCION VI – FORMULARIO:

LA SECCION VI – SE ENCUENTRA ADJUNTO AL PRESENTE DOCUMENTO EN FORMATO MODIFICABLE A FIN DE QUE EL OFERENTE LO PUEDA UTILIZAR EN LA PREPARACION DE SU OFERTA

SECCIÓN VII – ANEXOS

**ANEXO Nº I**

**DOCUMENTOS QUE COMPONEN LA OFERTA**

|  |
| --- |
| * + - 1. **Documentos sustanciales para Personas Físicas y Jurídicas** |
| **Formulario de Oferta \***  *[El formulario de oferta y lista de precios, serán generados electrónicamente a través del SICP, y deberán ser completado y firmado por el Oferente]* |
| **Garantía de Mantenimiento de Oferta\***  *[La garantía de mantenimiento de oferta debe ser extendida conforme al modelo indicado en la Sección VI, bajo la forma de una garantía bancaria o póliza de seguro de caución. Debe cumplir con los requisitos indicados en las Instrucciones al Oferente]* |
|  |
| * + - 1. **Documentos legales** |
| Oferentes Individuales. **Personas Físicas.** |
| 1 - Fotocopia simple de la Cédula de Identidad del firmante de la oferta.\* |
| 2 - Constancia de inscripción en el Registro Único de Contribuyentes - RUC. |
| 3 - Fotocopia simple de la Patente Municipal vigente. |
| 4 - En el caso que suscriba la oferta otra persona en su representación, deberá acompañar una fotocopia simple de su cédula de identidad y una fotocopia simple del poder suficiente otorgado por Escritura Pública para presentar la oferta y representarlo en los actos de la licitación. No es necesario que el Poder esté inscripto en el Registro de Poderes.\* |
| 5 - Fotocopia simple del Certificado de Cumplimiento Tributario vigente. |
|  |
| * + - 1. **Documentos legales** |
| Oferentes Individuales. **Personas Jurídicas.** |
| 1 - Fotocopia simple de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos.\* |
| 2 - Constancia de inscripción en el Registro Único de Contribuyentes RUC |
| 3 - Documentos de Identidad de los representantes o apoderados de la Sociedad. |
| 4 - Fotocopia simple de la Patente Municipal vigente |
| 5 - Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al oferente. Estos documentos pueden consistir en: un poder suficiente otorgado por Escritura Pública (no es necesario que esté inscripto en el Registro de Poderes); ó los documentos societarios que justifiquen la representación del firmante, tales como las actas de asamblea y de directorio en el caso de las sociedades anónimas.\* |
| 6 - Fotocopia simple Certificado de Cumplimiento Tributario vigente. |
|  |
| * + - 1. **Oferentes en Consorcio.** |
| 1 - Cada integrante del Consorcio que sea una persona física domiciliada en la República del Paraguay deberá presentar los documentos requeridos para Oferentes individuales especificados en el apartado (C) precedente. Cada integrante del Consorcio que sea una persona jurídica domiciliada en el Paraguay deberá presentar los documentos requeridos para Oferentes individuales en el apartado (D) precedente. |
| 2 - Fotocopia simple del Consorcio constituido o del acuerdo de intención de constituir el Consorcio , en el que se indicarán con precisión los puntos establecidos en el artículo 48, incisos 2° y 3° del Decreto Reglamentario N° 5.174/05. El acuerdo de intención deberá hallarse instrumentado, como mínimo en un documento privado con certificación de firmas por Escribano Público. El Consorcio constituido deberá estar formalizado por Escritura Pública. |
| 3 - Fotocopia simple de los Documentos que acrediten las facultades de los firmantes del acuerdo de intención de consorciarse. Estos documentos pueden consistir en:  i) un poder suficiente otorgado por escritura pública por cada Miembro del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o  ii) los documentos societarios de cada Miembro del Consorcio, que justifiquen la representación del firmante, tales como actas de asamblea y de directorio en el caso de las sociedades anónimas. |
| 4 - Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al Consorcio, cuando se haya formalizado el Consorcio. Estos documentos pueden consistir en:  un poder suficiente otorgado por escritura pública por la Empresa Líder del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o  los documentos societarios de la Empresa Líder, que justifiquen la representación del firmante, tales como actas de asamblea y de directorio en el caso de las sociedades anónimas. |
| **F) Documentos adicionales a la oferta que demuestren que los Bienes o Servicios ofertados cumplen con las especificaciones de la Sección III, Suministros Requeridos.** |
| 1 –Catálogos técnicos emitidos por el fabricante que demuestre que los bienes ofertados cumplen con las especificaciones técnicas. |
| 2 - Autorización del Fabricante, Representante o Distribuidor de la marca ofertada de los bienes requeridos conforme a la Sección III – Requisito de los Bienes y/o Servicios Requeridos En caso de representantes o distribuidor deberá presentar las documentaciones que demuestren la cadena de autorizaciones hasta llegar al fabricante. |
| 3 - Planilla de Datos Garantizados conforme a lo establecido en la Sección III – Requisito de los Bienes y/o Servicios Requeridos. Cumple/no cumple. |
| 4- Declaración Jurada del oferente en el cual manifiesta los bienes cuentan con garantía por el plazo establecido en las especificaciones técnicas y que la garantía, así como la asistencia técnica especializada puede ser ejecutada en cualquiera de los CAS del país indicando cuáles son los CAS que existen en el país. |
| 5 – Fotocopia de la Certificación ISO 9001 o similar en los bienes requeridos conforme a la Sección III – Requisito de los Bienes y/o Servicios requeridos. |
| 6 – Fotocopia de Certificación ISO 9001 o similar del oferente a los efectos de garantizar la calidad de los servicios. |
| ***G)*****Documentos que demuestren que el Oferente está calificado para ejecutar el contrato en caso que su oferta sea aceptada, de conformidad con la cláusula 26 de las Instrucciones a los Oferentes.** |
| 1 - Balance General y Cuadro de Estado de Resultados de los años 2016, 2017 y 2018 para contribuyente de IRACIS |
| 2 - IVA General de los 3 últimos meses conforme al calendario perpetuo de vencimientos emitido por la SET para oferentes contribuyentes sólo del IVA General |
| 3 - Formulario 106 de los 3 años (216, 2017 y 2018) para oferentes contribuyentes del IRPC |
| 4 - Formulario 104 de los 3 años (2016, 2017 y 2018) para oferentes contribuyentes de Renta Personal. |
| 6- Fotocopia de contratos y/o facturaciones de venta de provisión de equipos informáticos emitidos dentro de los tres años (2016, 2017 y 2018). El promedio de la suma de los tres últimos años deberá ser de por lo menos el 50% del monto máximo ofertado. No se requiere al menos un contrato o facturación por cada año. |
| 7- El oferente o el subcontratista a ser contratado por el oferente para la realización de los servicios del ítem 10 – Readecuación del Data Center deberá presentar Fotocopia de contratos y/o Facturaciones que demuestre que cuenta con experiencia en Construcciones y/o readecuaciones y/o ampliaciones de Obras en General dentro de los últimos 2 (dos) años 2017 y 2018 cuya sumatoria de contratos sea al menos el 50 % del monto ofertado en el Ítem 10 – Readecuación del Data Center. |
| 8 - En el caso de que el oferente designe a un subcontratista para la realización de los servicios del ítem 10 – Readecuación del Data Center deberá presentar:   1. Declaración Jurada del oferente en el cual se compromete a contratar una persona física o jurídica para la Realización del Servicio establecido en el Ítem 10 – Readecuación del Data Center en el cual se detalle los datos del subcontratista: Nombre o Razón Social, RUC, Teléfono, Dirección, correo electrónico, nombre del/los represente/s legal/es del subcontratista. El monto a ser subcontratado no deberá ser superior al 60 % del monto total de la oferta. 2. Documento que demuestre que el/los represente/s legal/es del Subcontratista a ser contratado por el oferente cuenta con la capacidad de comprometer a la firma ya sea estos (Fotocopia simple de Estatuto Social, Constitución de la Sociedad, Poderes Generales o especiales ante Escribanía Pública, Actas de Directorio o Actas de Asamblea. En el caso de personas físicas la fotocopia de cedula de identidad del propietario de la firma subcontratista. En el caso de que el subcontratista designe a otra persona la representación legal, deberá presentar el Poder ante Escribanía Pública). 3. Declaración Jurada del Art. 40 firmada por el/los represente/s legal/les del Subcontratista a ser designado para el desarrollo de los servicios. 4. Declaración Jurada del subcontratista a ser designado por el oferente en el cual manifieste contar con todas las herramientas, equipos, insumos, materiales y personales capacitados para la realización del servicios y se compromete a firmar un contrato de subcontratación con el oferente en el caso de ser adjudicado. |
| 9- Fotocopia de como mínimo 2 (dos) contratos de provisiones de Sistema de Detección y Extinción de Incendios automática en Data Centers. |
| 10- Fotocopia de como mínimo 2 (dos) contratos de provisiones de UPS trifásicas de potencia igual o superior a las solicitadas en este llamado. |
| 11- Fotocopia de como mínimo 3 (tres) contratos de provisiones de storage SAN de la misma marca al ofertado en este llamado. |
| 12- Fotocopia de como mínimo 4 (cuatro) contratos de provisiones de Router de Borde de la misma marca al ofertado en este llamado |
| 13- Fotocopia de como mínimo 2 (dos) contratos de provisiones de Servidores de la misma marca y modelo al ofertado en este llamado. |
| 14- Fotocopia de como mínimo 2 (dos) contratos de provisiones de Monitores Profesionales de la misma marca a los ofertados en este llamado. |
| 15- Fotocopia de como mínimo 1 (un) contrato de provisión de UPS de la misma marca y potencia (igual o superior) al solicitado en este llamado. |
| 16- Fotocopia de como mínimo 2 (dos) contratos de provisión de sistemas de detección y extinción de incendios automática con gas FM200, ECARO o Novec. |
| 17- Fotocopia de como mínimo 1 (un) de contrato de provisión de mantenimiento del Data Center. |
| **H) Cualquier otro documento adicional requerido.** |
| 1 - Certificado de Origen Nacional del bien o servicio ofertado emitido por el Ministerio de Industria y Comercio. La no presentación del documento no implica la descalificación de la oferta sino la no aplicación del margen de preferencia. |

\***Documentos Sustanciales conforme a la cláusula 24.2 de las IAO SBE**

Los oferentes que presenten la Constancia del Sistema de Información de Proveedores del Estado (SIPE) emitida por el sistema, al momento de la presentación de las ofertas no necesitarán acompañar los documentos que consten en la misma, siempre que dichos documentos se hallen “ACTIVO e HISTORÍCO”.

Las personas físicas o jurídicas interesadas en participar en los procedimientos de contratación por la modalidad de Subasta a la Baja Electrónica, deberán estar inscriptas y habilitadas en el Sistema de Información de Proveedores del Estado (SIPE).

Las CONSORCIOS o COASEGUROS interesados en participar en los procedimientos de contratación por la modalidad de Subasta a la Baja Electrónica, deberán estar inscriptos y habilitados en el Sistema de Información de Proveedores del Estado (SIPE).

| **ANEXO N° II** |
| --- |

**DOCUMENTOS A PRESENTAR PARA LA FIRMA DEL CONTRATO**

Los siguientes documentos deberán ser para la firma del contrato cuando no hayan sido presentados junto con la oferta, y no consten como “activos” en el SIPE.

|  |
| --- |
| * + - 1. **Personas Físicas / Jurídicas** |
| 1. Certificado de no encontrarse en quiebra o en convocatoria de acreedores expedido por la Dirección General de Registros Públicos; |
| 1. Certificado de no hallarse en interdicción judicial expedido por la Dirección General de Registros Públicos; |
| 1. Constancia de no adeudar aporte obrero patronal expedida por el Instituto de Previsión Social. |
| 1. En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación. |

|  |
| --- |
| * + - 1. **Documentos. Consorcios** |
| 1. Cada integrante del Consorcio que sea una persona física o jurídica deberá presentar los documentos requeridos para oferentes individuales especificados en los incisos (a), (b), (c) y (d) del apartado 1. precedente. |
| 1. Consorcio constituido, en el que se establecerán con precisión los puntos establecidos en el artículo 48 inciso 4° del Decreto Reglamentario N° 5174/05. El Consorcio debe estar formalizado por Escritura Pública. |
| 1. Documentos que acrediten las facultades del firmante del contrato para comprometer solidariamente al Consorcio. |
| 1. En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación. |

|  |
| --- |
| * + - 1. **Documentos de Origen Extranjero. Personas Físicas / Jurídicas y/o Consorcios** |
| 1. Si la oferta adjudicada estuviera acompañada de documentos emitidos por autoridades extranjeras, el Oferente deberá acompañar los documentos debidamente apostillados para los países partes del “Convenio para la supresión de la exigencia de legalización de documentos públicos extranjeros o de la Haya del 5 de octubre de 1961”, caso contrario los documentos deberán estar legalizados por el Consulado Paraguayo del país de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay. 2. Los documentos de origen privado emitidos en el extranjero deberán estar legalizados por el Consulado Paraguayo del país de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay |