

**PLIEGO DE BASES Y CONDICIONES**

---

Convocante:

**Servicio Nacional de Promoción Profesional (SNPP) / Ministerio de  
Trabajo, Empleo y Seguridad Social  
Servicio Nacional de Promoción Profesional**

Nombre de la Licitación:

**ADQUISICION E INSTALACIÓN DE SISTEMA DE CCTV  
PARA EL SNPP**  
(versión 10)

ID de Licitación:

**392088**



Modalidad:

**Licitación Pública Nacional**

Publicado el:

**24/03/2022**

*"Pliego para la Adquisición de Bienes - SBE"*  
*Versión 1*

## RESUMEN DEL LLAMADO

### Datos de la Convocatoria

ID de Licitación:	392088	Nombre de la Licitación:	ADQUISICION E INSTALACIÓN DE SISTEMA DE CCTV PARA EL SNPP
Convocante:	Servicio Nacional de Promocion Profesional (SNPP) / Ministerio de Trabajo, Empleo y Seguridad Social	Categoría:	24 - Equipos, accesorios y programas computacionales, de oficina, educativos, de imprenta, de comunicación y señalamiento
Unidad de Contratación:	Servicio Nacional de Promocion Profesional	Tipo de Procedimiento:	LPN - Licitación Pública Nacional

### Etapas y Plazos

Lugar para Realizar Consultas:	Consultas Virtuales a traves del portal	Fecha Límite de Consultas:	28/03/2022 07:30
Lugar de Entrega de Ofertas:	MOLAS LOPEZ N° 480 EDIFICIO DEL SNPP BLOQUE 1 PRIMER PISO OFICINA DE LA UOC	Fecha de Entrega de Ofertas:	08/04/2022 10:00
Lugar de Apertura de Ofertas:	MOLAS LOPEZ N° 480 EDIFICIO DEL SNPP BLOQUE 1 PRIMER PISO OFICINA DE LA UOC	Fecha de Apertura de Ofertas:	08/04/2022 10:15

### Adjudicación y Contrato

Sistema de Adjudicación:	Por Total	Anticipo:	No se otorgará anticipo
Vigencia del Contrato:	Hasta Cumplimiento Total de Obligaciones		

### Datos del Contacto

Nombre:	JOSÉ FERNANDO RUOTTI LENGUAZA	Cargo:	DIRECTOR
Teléfono:	603 062	Correo Electrónico:	uocsnpp@gmail.com

# ADENDA

## Adenda

Las modificaciones al presente procedimiento de contratación son los indicados a continuación:

REPÚBLICA DEL PARAGUAY

*SERVICIO NACIONAL DE PROMOCIÓN PROFESIONAL SNPP*

*LICITACIÓN PUBLICA NACIONAL POR SBE N° 04/2021 ADQUISICIÓN E INSTALACIÓN DE SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN CCTV PARA EL SNPP ID N° 392.088*

ADQUISICIÓN DE BIENES Y/O SERVICIOS

ADENDA 9

**Debe Decir:**

Visita al sitio de ejecución del contrato

La convocante dispone la realización de una visita al sitio con las siguientes indicaciones: Se podrá presentar Declaración Jurada en su remplazo

**Departamento de Informática**

Nombre del funcionario responsable de guiar la visita:

**Participación Obligatoria: NO**

Se podrá presentar Declaración Jurada en su remplazo

Fecha: 29 de octubre de 2021

Lugar: *Molas Lopez N° 480 e/ Tte. Cirilo Gill Edificio del SNPP*

hora: 09:00 hs Sede Central SNPP y a las 13:00 hs. CCP - PJ -San Lorenzo

procedimiento: *En el sitio Molas Lopez N° 480 e/ Tte. Cirilo Gill Sede Central del SNPP Dpto. Informática; con funcionarios del*

Al culminar la o las visitas, se labrará acta en la cual conste, la fecha, lugar y hora de realización, en la cual se identifique el nombre de las personas que asistieron en calidad de potenciales oferentes, así como del funcionario encargado de dicho acto.

Los gastos relacionados con dicha visita correrán por cuenta del oferente.

Cuando la convocante haya establecido que no será requisito de participación, el oferente podrá declarar bajo fe de juramento conocer el sitio y que cuenta con la información suficiente para preparar la oferta y ejecutar el contrato.

**LAS ESPECIFICACIONES TECNICAS QUEDAN REDACTADAS DE LA SIGUIENTE MANERA:**

**SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS**

ITEM	CODIGO DE CATALOGO	DESCRIPCIÓN	DESCRIPCIÓN ESPECIFICACIONES TECNICAS MINIMAS REQUERIDAS	CANTIDAD	UNIDAD DE MEDIDA	PRESENTACIÓN
1	46171619-9999	Sistema de circuito cerrado de video vigilancia	Según especificaciones tecnicas	1	unidad	unidad
Sub Items						
1.1	camara tipo 1: procesador de captura y procesamiento de imagen preparada para integración, inteligencia artificial e Depp Learning en el borde	según especificaciones tecnicas		2	unidad	unidad
1.2	camara tipo 2: domo 5 mpx	según especificaciones tecnicas		28	unidad	unidad
1.3	camara tipo 3: bullet 5 mpx	según especificaciones tecnicas		28	unidad	unidad

1.4	camara tipo 4: speed dome 5 mpx	según especificaciones tecnicas	1	unidad	unidad
1.5	tipo 1: servidor de gestión	según especificaciones tecnicas	1	unidad	kit
1.6	tipo 2 : servidor para sitio centralizado	según especificaciones tecnicas	1	unidad	kit
1.7	tipo 3: servidor de video wall	según especificaciones tecnicas	1	unidad	kit
1.8	tipo 4: servidor de video remoto	según especificaciones tecnicas	1	unidad	kit
1.9	tipo 5: servidor de aplicaciones y virtualización	según especificaciones tecnicas	1	unidad	kit
1,10	licencias tipo 1: servidor remoto	según especificaciones tecnicas	33	unidad	unidad
1.11	licencias tipo 4: servidor centralizado	según especificaciones tecnicas	70	unidad	unidad
1.12	biometria facial, registro de licencia perpetua, pago unico ilimitadas camaras de analitica facial	según especificaciones tecnicas	1000	unidad	unidad
1.13	licencias de integración y automatización de flujos modalidad instalación	según especificaciones tecnicas	1	unidad	unidad
1.14	sistema de control de acceso	según especificaciones tecnicas	1	unidad	unidad
1.15	molinete tipo 1 por pasaje flujo libre	según especificaciones tecnicas	1	unidad	kit
1.16	molinete tipo 2	según especificaciones tecnicas	1	unidad	kit
1.17	barreras de acceso alto flujo	según especificaciones tecnicas	1	unidad	kit
1.18	control de acceso IP multi tecnologia	según especificaciones tecnicas	3	unidad	kit
1.19	sensor de presencia IOT	según especificaciones tecnicas	2	unidad	kit

1,20	sensor de presencia IOT	según especificaciones técnicas	2	unidad	kit
1.21	Plataforma de gestión de alarmas integrada al VMS y conectividad IOT hasta 20 dispositivos por 24 meses	según especificaciones técnicas	1	unidad	unidad
1.22	servicio de integración de sistema de control inteligente	según especificaciones técnicas	1	unidad	global

Las características técnicas se describen en el numeral 3 de la presente Especificación Técnica y según cantidades indicadas en la Lista Equipos requeridos a ser suministrados.

Los equipos correspondientes detallados en alcance del suministro, deberá incluir la provisión, montaje y puesta en servicio de todos los componentes sea hardware y software con sus accesorios necesarios para optimizar su uso, los cuales se detallan en cada ítem respectivo.

### 3. Características Técnicas

3.1 Los equipos y sus respectivos componentes con sus características básicas específicas y licencias legales se detallarán a continuación

<b>ITEM 1</b>	<b>Cámara Tipo 1: Procesador de captura y procesamiento de imagen preparada para integración, Inteligencia Artificial y Deep Learning en el borde</b>
Características Generales	<p>Es un equipo de captura y procesamiento de imagen que por medio de reconocimiento óptico de caracteres (OCR), realiza la (LPR). El equipo actúa como una plataforma abierta que permite introducir aplicaciones de terceros para reducir las necesidades de equipamientos adicionales, con acelerador de Red Neural (NPU) compatible con soluciones de visión computacional</p> <p>Conformidad con las normas FCC, CE Compliance y homologación Anatel o normas similares y equivalentes</p> <p>Deberá disponer capacidad superior de procesamiento de analíticos, brinda el poder de las características deep learning, que sumada a la conectividad móvil, arroja una cámara inteligente.</p> <p>Resolución (Tamaño en píxeles del Sensor): 1636 x 1220 px. Tamaño Físico del Sensor: 1/1.8" o similar</p> <p>Sistema de Captura de Imagen: Global Shutter. Lente: CS Mount 13-55 mm o similar</p> <p>Shutter Mínimo   Máximo: 1/12500 (80 us) a 1/15.6 (64 ms) o similar</p>

Características  
Especificas

Tipo de Sensor de Imagen: CCD Tasa de Frames (Interna) :15 cps.o similar

Tasa de Cuadros (Transmisión): hasta 15 cps. o similar

Tensión de Alimentación: 9 ~ 32 VDC.

Tipo de Conectores: 2 LAN| USB A 2.0| Microfit 16 vías| Slot para SIM Card, |Slot para Micro SD| conector AUTO ÍRIS  
|Conectores SMA con sus respectivas antenas GPS, Wi-Fi, 4G/3G. o equivalentes

Potencia Mínima | Máxima: 8.5 ~ 12 W o equivalente.

Peso sin lente: aproximado 875 g

Dimensiones aproximadas: (A) x (L) x (C) - (mm) 75x74x189. Grado de protección IP: mínimo IP40.

Temperatura de operación: '-10 a 65 °C con humedad relativa del aire de 5% a 95% y sin condensación,  
cumpliendo en conformidad con la IEC 60068-2-2 o similar.

Entradas y Salidas (I/O): 4 puertas digitales bidireccionales individualmente programable con entradas con  
salidas opto-aisladas para conexión de señal de disparo o/u integración a otros dispositivos del sistema de  
integrado.

Interfaz de Red: 2 interfaces 10/100/1000 Mbps (Gigabit). Formato de Imagen: JPEG.

Formato de Vídeos H.264, H.265 e MJPEG. Protocolos de Comunicación 'RTSP y FTP. O equivalente

APIs (Application Programming Interface): REST O equivalente para integración con el sistema.

Capacidad de Almacenamiento Externo: Tarjeta de memoria microSD hasta 128GB o equivalente

Memoria RAM: 2GB LPDDR4 (2100 Mbps e 1050 MHz).

LPR incorporado.

Perfiles de Configuración de la Cámara: mínimo 4.

Múltiples exposiciones de 2 a 8 imágenes por disparo con distintas opciones de configuración de parámetros.

Función HDR (alto rango dinámico).

GPS para evidencia de imagen: Gen8C Lite Multi-constellation Glonass| BeiDou/Compass| Galileo e QZSS|  
Antena Externa 2 dBic típico o similar.

Wifi: IEEE 802.11 bandas b/g/n 2.4 GHz| Antena Externa 2.8 dBi típico,

4G: LTE-FDD/LTE-TDD/WCDMA/GSM |Antena Externa (1.42 dBi, 1.91 dBi| 2.51 dBi|

3.23 dBi|2.89 dBi) o similar.

Módulo eSIM para comunicación celular o similar.

CPU mínimo: Quad-core 1.2 GHz, con soporte a tecnología ARM y NEON o compatible

Software libre incorporado (ej: Linux) opción de cargar software analítico en la propia cámara a través de  
contenedores Docker. Utilizando a API REST, para las funciones de captura de imágenes y acceso a los analíticos  
| SDK y ejemplos de aplicaciones deberán estar disponibles O equivalente , software libre.

Características  
constructivas

Aluminio anodizado y panel frontal en policarbonato O equivalente en proteccion

**ITEM 2****Cámara Tipo 2: domo 5 mpx.****Características  
Generales o  
equivalentes**

Deberá ser una cámara IP que proporciona resolución de mínimo 5 MP en tiempo real a 24 cps. con una lente vari-focal de enfoque automático teniendo como referencia la distancia focal de 2.7~13.5mm con lente motorizado simultáneo y tecnología de color en la oscuridad para video de calidad en cualquier condición de iluminación, debe cumplir con los requisitos ONVIF-S (Opcional) facilitando su integración exitosa con cualquier solución de plataforma abierta en el mercado.

**IMAGEN**

Sensor de imagen CMOS de mínimo 5 MP de 1/2.8" cantidad total de píxeles 2592

(H) x 1944 (V), relación de aspecto 4:3.

**LENTE**

Distancia focal de 2.7 13.5 mm, F1.4, tipo P-iris vari-focal con enfoque automático y zoom motorizado, campo de visión (FoV, Campo de visión) 85° ~ 31°, distancia Infra roja con un rango de alcance de 30.48 m, zoom óptico digital siendo x 5 E/S.

**OPERACIONALES**

Modo del obturador: automático, manual, anti parpadeo, obturador lento

velocidad del obturador: 1/15 ~ 1/32000, obturador lento: 1/2, 1/3, 1/5, 1/6, 1/7.5, 1/10

Día (Color), Noche (Blanco y negro), reducción de ruido digital con función 3D, reducción de ruido digital 3D, rango dinámico amplio (WDR, Rango dinámico amplio) WDR real (WDR) dB120 dB.

**Zona de Privacidad**

Mínimo 16 máscaras de privacidad programables, compensación de luz de fondo (BLC), capacidad de voltear de forma horizontal y vertical, notificaciones de alarma, correo electrónico, FTP, salida de alarma y grabación de tarjeta SD.

**RED**

Puerto LAN 10/100Base-T, tipo de compresión de video

**Características  
específicas o  
equivalente**

H.265, H.264, MJPEG, resolución H.265: 2592x1944, 2304x1296, 2.1 MP/1080p, 720p, VGA, D1, CIF H.264: 2592x1944, 2304x1296, 2.1 MP/1080p, 720p, VGA, D1, CIF MJPEG: 2.1 MP/1080p, 720p, 800x600, VGA, 768x432, D1, CIF, velocidad de

fotogramas, hasta 24 cps en todas las resoluciones, velocidad de bits de video H.264/H.265: 32 Kbps ~ 14 Mbps MJPEG: 1 Mbps ~ 40 Mbps, doble control de uso de bits, H.265 o H.265/H.264/MJPEG simultáneo, capacidad de flujo de transmisión doble a diferentes velocidades y resoluciones.

**Norma IP .**

IPv4, IPv6

**Protocolo**

TCP/IP, UDP, AutoIP, RTP(UDP/TCP), RTSP, NTP, HTTP, HTTPS, SSL, DNS, DDNS, DHCP, FTP, SMTP, ICMP, SNMPv1/v2/v3 (MIB-2), ONVIF-S.

**Seguridad**



HTTPS(SSL), filtro IP, 802.1x, Autenticación implícita (ID/PW), que cumple con las normas del ONVIF, visualizador web en los SO: Sistema operativo Windows®, Mac®, Linux®, Navegador: Internet Explorer®, Google Chrome®, Mozilla Firefox®, Safari® y Software de gestión de video.

#### AMBIENTALES Y ELECTRICAS

Temperatura operativa -20 °C ~ 50 °C, humedad durante la operación relativa 10- 90 % (sin condensación), grado de protección IP Certificación IP66 Otras certificaciones o similares CE, FCC, RoHS

CC de 12 V, PoE (IEEE802.3af, clase 3), 12 V CC: máx. 7.4 W-PoE: máx. 8.7 W.

Características constructivas o equivalentes Deberá ser una carcasa tipo mini-dome (DOMO) de policarbonato clasificación IP66 antivandálica y IK-10 resistente a impactos mínimamente una ranura para tarjeta de memoria compatible con los estándares Micro SD/SDHC/SDXC Clase 10. Garantía de fábrica mínima 5 años.

#### ITEM 3 Cámara Tipo 3: Bullet 5 mpx

Características Generales o equivalentes Deberá ser una cámara IP que proporciona resolución de mínimo 5 MP en tiempo real a 24 cps, con una lente vari-focal de enfoque automático teniendo como referencia la distancia focal de 2.7~13.5 mm con zoom motorizado, que soporte códec H.265/H.264/MJPEG simultáneo y tecnología de color en la oscuridad para video de calidad en cualquier condición de iluminación, que cumplen los requisitos ONVIF-S facilitando su integración exitosa con cualquier solución de plataforma abierta en el mercado, entrada de sensor de alarma, salida de relé, servidor Web integrado, capacidad de arranque en frío a -40°C.

#### IMAGEN

Sensor de imagen CMOS de mínimo 5 MP de 1/2.8", cantidad total de píxeles 2592

(H) x 1944 (V), iluminación de escena relación de aspecto 4:3.

#### LENTE

Distancia focal de 2.7~13.5 mm, F1.4, tipo de lente P-iris vari-focal con enfoque automático y zoom motorizado, campo de visión (FoV, Campo de visión) 85° ~ 31°, distancia infra roja con un rango de alcance de 42.67 m,

zoom óptico siendo x 5, E/S, entrada/salida de audio 1/1, compresión de audio: G.711, entrada/salida de alarma: 1/1.

#### OPERACIONALES

Modo del obturador en automático o manual, anti parpadeo, obturador lento.

Velocidad del obturador de 1/15 ~ 1/32000, obturador lento de 1/2, 1/3, 1/5, 1/6, 1/7.5, 1/10, control automático de mejoras (AGC) en automático día y noche, automático día (Color), noche (Blanco y negro), reducción de ruido digital con función 3D, rango dinámico amplio (WDR, Rango Dinámico Amplio) siendo WDR real (WDR) dB120 dB.

#### Zona de Privacidad

Mínimo 16 máscaras de privacidad programables, compensación de luz de fondo (BLC), capacidad de voltear de forma horizontal y vertical, función de notificaciones de alarma, correo electrónico, FTP, salida de alarma y grabación de tarjeta SD.

#### RED

Características específicas o equivalente Puerto LAN 10/100 Base-T, tipo de compresión de video H.265, H.264, MJPEG, resolución H.265: 2592x1944, 2304x1296, 2.1 MP/1080p, 720p, VGA, D1, CIF H.264: 2592x1944, 2304x1296, 2.1 MP/1080p, 720p, VGA, D1, CIF MJPEG: 2.1 MP/1080p,

720p, 800x600, VGA, 768x432, D1, CIF ,velocidad de fotogramas, hasta 24 cps en todas las resoluciones, velocidad de bits de video H.264/H.265: 32 Kbps ~ 14 Mbps MJPEG: 1 Mbps ~ 40 Mbps, doble control de uso de bits, H.265 o H.265/H.264/MJPEG simultáneo, capacidad de flujo de transmisión doble a diferentes velocidades y resoluciones.

#### Normas IP

IPv4, IPv6.

#### Protocolo

TCP/IP, UDP, Auto IP, RTP(UDP/TCP), RTSP, NTP, HTTP, HTTPS, SSL, DNS, DDNS, DHCP, FTP, SMTP, ICMP, SNMPv1/v2/v3 (MIB-2), ONVIF.

#### Seguridad

HTTPS (SSL), filtro IP, 802.1x, Autenticación implícita (ID/PW).

Visualizador web en las plataformas: sistema operativo Windows®, Mac®, Linux® con los navegadores: Internet Explorer®, Google Chrome®, Mozilla Firefox®, Safari® y Software de gestión de video.

#### AMBIENTALES Y ELECTRICAS

Temperatura operativa -40 °C ~ 50 °C, humedad durante la operación relativa 10- 90 % (sin condensación), grado de protección IP con Certificación IP66, otras certificaciones CE, FCC, RoHS o similares

CC de 12 V, PoE (IEEE802.3af, clase 3), 12 V CC: máx. 9 W, PoE: máx. 10.5 W.

Características constructivas o equivalentes

Deberá ser una carcasa tipo bala (Bullet) clasificación IP66 y resistente a la intemperie para cumplir con la Certificación IP66, mínimamente una ranura para tarjeta de memoria compatible con los estándares Micro SD/SDHC/SDXC. Garantía de fábrica mínima 5 años.

#### ITEM 4

#### Cámara Tipo 4: Sped Dome 5 mpx.

Características Generales o equivalentes

Deberá ser una cámara tipo PTZ con movimiento horizontal 0 a 360°, vertical -10 ~ 190° a una velocidad máxima de 380°/seg. y un zoom de 30x para proporcionar imágenes claras a una resolución de hasta 4 K en tiempo real de 24 cps, con tecnología todo color, para lograr un color sorprendente en la oscuridad, el zoom debe ser óptico de 30x e infra rojo de alta potencia con un alcance de hasta 350 m

#### IMAGEN

Deberá ser una cámara IP que proporciona resolución de mínimo de hasta 4 K, sensor de imagen CMOS de 1/1.7 de 4 K, cantidad total de píxeles 4168 x 3062, Píxeles activos 3840 x 2160, sistema de escaneo progresivo, iluminación de escena mínima 0.75 lux (color), 0 Lux (blanco y negro).

#### LENTE

Distancia focal 6 ~ 180 mm, lente tipo PTZ con zoom motorizado 30x, distancia del IR 350 m de alcance, ángulo de visión de 55.4 ~ 2.7°, zoom digital/óptico de 30x E/S, entrada/salida de audio 1/1 Compresión de audio G.711, alerta audible de mínimo 3 archivos de audio definidos por el usuario entrada/salida de alarma 4/1, activación manual 4 activaciones programables

#### OPERACIONALES

El modo del obturador debe ser automático, anti parpadeo, velocidad del obturador de 1/10,000 ~ 1 seg., contraluz, anti neblina, rango dinámico amplio (WDR) real de 120 dB, reducción de ruido digital, balance de blancos automático o manual, día y noche, Día (Color), Noche (Blanco y negro), con funciones de espejo y volcado, zonas de privacidad mínimo 16 máscaras programables, detección de movimiento 16 zonas programables siendo 8 áreas incluidas y 8 áreas excluidas, modo de grabación en tarjeta SD (grabación de evento y continua), almacenamiento de eventos en memoria intermedia FTP Anterior: 30 seg., Posterior: 30 seg., tarjeta SD Anterior: 10 seg., Posterior: 60 seg., notificaciones de alarma por correo electrónico, servidor FTP, activación de salida de alarma, activación de salida de audio, activación preprogramada, servidor de notificaciones, notificaciones XML o grabación en tarjeta SD.

#### **FUNCIÓN PTZ**

Características  
específicas o  
equivalente

Alcance de movimiento horizontal 360° sin fin, velocidad de movimiento horizontal Máx. 380°/seg. (preprogramado), alcance de movimiento vertical -10 ~ 190°, velocidad de movimiento vertical Máx. 380°/seg. (preprogramado), preprogramado 256 recorrido 8 Patrón 8, con funciona inicial.

#### **RED**

LAN RJ-45 (10/100 Base-T), tipo de compresión de video H.265 (perfil principal),

H.264 (perfil de línea base, perfil principal, perfil alto), MJPEG, resolución 3840x2160, 3072x2048, 2592x1944/1520, 2560x1440, 1920x1080, 1440x1080, 1280x1024/720, 1024x768, 800x600/480, D1, 640x480, 400x240, CIF, velocidad de bits de video flujo Cuádruple (H.265x3/H.264, MJPEGx1), códec inteligente de alta transmisión, control de uso de bits, transmisión múltiple CVBR/VBR a H.265,

H.264 (velocidad de fotogramas y ancho de banda controlables), velocidad de fotogramas Hasta 24 fps en todas las resoluciones, capacidad de flujo de transmisión, transmisión doble a diferentes velocidades y resoluciones

#### **Normas IP:**

IPv4, IPv6

#### **Protocolo**

TCP/IP, UDP, HTTP, HTTPS, QoS, FTP, UPnP, RTP, RTSP, RTCP,

DHCP, ARP, Zeroconf, Bonjour. Seguridad y autenticación de contraseña, autoridad multiusuario, filtrado IP, HTTPS (SSL), acceso máximo de usuarios :10 usuarios en vivo, 3 en reproducción, cumple con las normas ONVIF.

Visualizador web SO: Sistema operativo Windows®, Mac®, Linux®

Navegador: Internet Explorer®, Sincronización con el tiempo de red Servidor NTP, aceptar actualización remota respaldo y restablecimiento

Operación y eléctrica:

Temperatura operativa -30 °C ~ 55 °C, humedad durante la operación Humedad relativa 0 ~ 90 % (sin condensación) otras certificaciones CE, FCC, RoHS, PoE (UPoE, Clase 4), 12 V CC. Consumo de energía PoE: 28 W, 500 mA, 12 V CC: 28 W, 2.3 A

Características  
constructivas o  
equivalentes

Dentro de una carcasa de aluminio para el conjunto PTZ, domo de policarbonato con clasificación IK-10 resistente a impactos. Grado de protección IP: Clasificación IP66.

#### **ITEM 5**

#### **Tipo 1: Servidor de Gestión**

Construido con propósito de gestión con SQL STD. Solución escalable, desarrollado e ideal para análisis. Aceleración de GPU.

Características  
Generales

Arquitectura flexible.

VMS optimizado y certificado. Probado en laboratorio.

Garantía 5 años de fábrica.

Procesador: Familia de procesadores específicos para servidores hasta 8 núcleos, frecuencia básica de 1.8 Ghz hasta 3.2, cache de 11mb hasta 16.5mb compatible con la carga de trabajo del sistema ofertado. Sistema operativo: IOT integrado (OEM) precargados con su Hardware, Núcleo híbrido (Kernel), con soporte al menos hasta 2027

Características Especificas o Equivalente	Memoria	Opción predeterminada de 32 GB Almacenamiento máximo de datos	Hasta 128 Salidas de video VGA
	GPU: placa grafica	Redes 1 x 1GbE	
	USB	Delantero: 2 x USB 2.0	
		Trasero: 2 x USB 3.0	

Sistema operativo RAID: 2 SSD de hasta 240 GB (RAID 1) Monitoreo de hardware preinstalado.

Caracteristicas constructivas o equivalentes	Formato 2 U
	Dimensiones del producto (métrico) (H x B x T)44,55 x 73,03 x 8,74 cm

**ITEM 6                      Tipo 2: Servidor para sitio centralizado**

Dispositivo de almacenamiento de video comercial empresarial . El servidor deberá estar especialmente diseñado para instalaciones de video vigilancia de nivel empresarial. Desde el transporte hasta las instalaciones gubernamentales y cualquier lugar intermedio.

El servidor debe ser un equipo de ingeniería avanzada que pueda transformar un práctico servidor, en una máquina de rendimiento mejorado/optimo.

Deberá estar preparado para una gran cantidad de cámaras, soportar como mínimo 200 camaras 5MP y las aplicaciones de gran retención, proporcionando un rendimiento de velocidad de grabación de 400-600 Mbps y potencialmente superior en la aplicación VMS.

Caracteristicas Generales o equivalentes	Deberá estar preparado para instalaciones de nivel empresarial, entorno de misión crítica y soporte técnico. Estar optimizado, certificado y garantizado, con la marca del VMS ofertado en el ítem 11 (Licencias Tipo 4: Servidor Centralizado). Preinstalado de fábrica una herramienta de monitoreo de hardware diseñada para monitorear, informar y administrar el entorno y el rendimiento del hardware de los servidores lo que garantiza el máximo tiempo de actividad, para el control total del hardware de seguridad con un panel de control fácil de usar que le permita evaluar, administrar y hacer cambios de forma remota. Las alertas instantáneas reportan problemas antes que los operadores lo hagan, haciendo que el TI sea más proactivo.
	Preinstalado un sistema de optimización de transferencia de datos de alto rendimeinto desde discos duros externos. Garantía 5 años de fábrica

Preinstalado un sistema de optimización de transferencia de datos de alto rendimeinto desde discos duros externos. Garantía 5 años de fábrica

Procesador: Familia de procesadores específicos para servidores hasta 8 núcleos, frecuencia básica de 1.8 Ghz hasta 3.2, cache de 11mb hasta 16.5mb compatible con la carga de trabajo del sistema ofertado  
Sistema operativo: Para servidor mínimamente 2019, específico para servidores, soporte hasta 2024, núcleo híbrido, arquitectura x86-64, Infraestructura Hiper-Convergente, Acceso al dispositivo de alojamiento para contenedores, incluye protección contra amenazas avanzadas, que permita ejecutar. Deberá contar con una interface para administración unificada, donde desde una única consola se pueda administrar sistemas externos y servidores remotos, sino también otras herramientas de línea de comando como PowerShell

	Memoria	Opción predeterminada de 32 GB hasta 64 GB Almacenamiento máximo de datos Hasta 384TB RAW
Características específicas o equivalente	Salidas de video VGA en GPU	
	Redes 4 x 1GbE (opcional + 2x 10GbE SFP + Configuración) USB	Delantero: 2 x USB 2.0
	Trasero: 2 x USB 3.0	
	Sistema operativo RAID: 2 SSD de 240 GB (RAID 1) Nivel de RAID de datos: PERC H740P JBOD, 0, 1, 5, 6, 10 Monitoreo de hardware NVR	Preinstalado
Características constructivas o equivalentes	Factor de Forma 2 U	
	Bahías de Unidades del sistema Operativo 2 x M.2 BOSS PCIe Card Bahías de Unidades de los Datos Up to 18 x 3.5 Data Drives (14 Hot	
	Swappable, 4 Fixed). Fuente de Alimentación 1+1 750W cambio en caliente	
	Humedad de Funcionamiento 5% ~ 90% non-condensing Dimensiones 17.08 x 3.4 x 28.16 in / 434 x 86 x 715 mm	
<b>ITEM 7 Tipo 3: Servidor de Video Wall</b>		
Características Generales	Sistema de Video Wall (muralla de video)	
	Todos los monitores existentes deben ser compatibles con los equipos y servidores de la central de monitoreo.	
	Se debe prever un hardware de video Wall con configuración minina en matrix 2x4, compatible con los servidores de video y debe estar con la solución embarcada y totalmente compatible con solución de video vigilancia propuesta.	
	Deberá ser de la misma marca/proveedor,	
	Los equipos tienen que tener un servidor nativo y un software nativo para la instalación y puesta en funcionamiento de lo que es el SO y el VMS dentro del propio equipo y finalmente debe tener una herramienta tal que permita tener la imagen completa de un equipo a la hora de una falla, para poder restaurarlo de manera intuitiva. Estos equipos deben estar en red.	
	Plataforma de gestión de video:	
	Software preinstalado de fábrica para el monitoreo del hardware:	
	Monitoreo intuitivo del sistema: monitorear la información del sistema o la señal de estado de los elementos clave de los dispositivos desde un solo panel.	
	Gestión sencilla del ecosistema: desde un único menú desplegable, puede navegar para gestionar clientes, usuarios, puertas de enlace y dispositivos.	
	El sistema deberá detectar problemas de índole técnico que permita al TI reportar dichos eventos a través de un informe directamente a la fábrica.	

	<p>Procesador: Familia de procesadores específicos para servidores hasta 8 núcleos, frecuencia básica de 1.8 Ghz hasta 3.2, cache de 11mb hasta 16.5mb compatible con la carga de trabajo del sistema ofertado</p> <p>Sistema operativo: IOT integrado (OEM) precargados con su Hardware, Núcleo híbrido (Kernel), con soporte al menos hasta 2027</p>
Características específicas o equivalente	<p>Hasta 64 GB DDR4 2666MHz Almacenamiento hasta 2 SSD de 256 GB (RAID 1)</p> <p>Gráficos: hasta 2 x (Memoria de GPU 4 GB GDDR5 - Interfaz de Memoria 128-bit - Ancho de Banda de Memoria Hasta 80 GB/s) - Unidad óptica CD / DVD / RW óptico de línea delgada</p> <p>Conectividad 2 x 1 GbE</p> <p>Puertos de E / S traseros 6 puertos USB 3.1</p> <p>Gabinete: Torre</p>
Características constructivas aproximadas	<p>Fuente de alimentación: 950W 80PLUS Gold Certified Power Supply Disco interno Drives 2 TB Data Drive</p> <p>Front I/O Ports 2 x USB 3.1 Type-A 2 x USB 3.1 Type-C</p>

#### ITEM 8 Tipo 4: Servidor de Video Remoto

	<p>Compatibilidad con cámaras ampliadas acepta más de 10.000 dispositivos a su VMS.</p>
Características Generales o equivalentes	<p>Un único punto de contacto para la asistencia del VMS y de los dispositivos, posibilidad de realizar intervenciones de asistencia sobre el terreno para sustituciones y reparaciones de hardware.</p> <p>Deberá ser un sistema servidor de video de bastidor pequeño, pero también flexible para crecer dentro de la infraestructura de TI existente.</p> <p>Tamaño: Montaje en bastidor 1U , CPU: de 4 nucleos, 4 subprocesos, de 3.2 a 4.2 Ghz, cache 6mb, velocidad de bus 8Gt/s compatible con 64-bit</p> <p>GPU: Placa grafica ultra HD , frecuencia base 350 Mhz, secuencia de gráficos hasta 1.2Ghz, memoria de gráficos gata 64Gb, que soporte hasta 4k @ 60Hz, resolución máxima, 4096x2304 @ 24Hz o compatible</p> <p>RAM:mínimo 16 GB DDR4</p> <p>RAM:16 GB DDR4</p> <p>Sistema operativo: IOT integrado (OEM) precargados con su Hardware, Núcleo híbrido (Kernel), con soporte al menos hasta 2027. Almacenamiento VMS/OS:1 x 256 GB (M.2 PCIe NVMe)</p> <p>Número de discos duros: 2 x 3.5 (accesibles desde el exterior)</p> <p>Almacenamiento en bruto: de 4/8/16/24 hasta 32 TB (unidades tipo empresarial 24/7) Controlador y compatibilidad RAID, controlador Intel® Rapid Storage o similar, RAID 0,1 (Software RAID) o similar Puertos de visualización 2 x USB 3.1 tipo C/puerto de visualización iGFX, adaptador de USB-C a video VGA incluido Interfaz de red 1x 1 GbE (RJ45).</p>
Características específicas o equivalente	<p>1x 1/2.5/5/10 GbE (RJ45).</p> <p>Ranuras PCIe disponibles: Una ranura PCI Express® x16 Gen 3 de anchura doble y altura completa.</p> <p>Una ranura PCI Express x4 Gen 3 de altura completa Archivado a NAS externo, a través de puerto LAN Credencial y cifrado de clave</p> <p>Módulo de plataforma segura (TPM 2.0) Información de hardware:</p> <p>Garantía de hardware: 5 años de garantía de fabrica para todo el sistema. Alimentación:100~240 V, 50/60 Hz</p>

	Consumo máximo:550 W con hasta un 94 % de eficiencia Protección
	OVP (exceso de tensión), OCP (exceso de corriente), OTP (exceso de temperatura), SCP (cortocircuito).
	Estándares sobre emisiones y seguridad, CE (clase A), UKCA, FCC, RCM, UL, México (NOM), VCCI, conformidad con disposiciones comerciales, conforme a NDAA o normas similares.
Características constructivas o equivalentes	Humedad 10-85 % de humedad relativa (sin condensación)
<b>ITEM 9</b>	<b>Tipo 5: Servidor de Aplicaciones y Virtualización</b>
Características generales o equivalentes	Servidor para aplicaciones y analítica con un procesador de hasta 16 GB de memoria de rango dual, controlador de almacenamiento con 2 MB de caché y batería de almacenamiento inteligente, 2 bahías de unidades de factor formato reducido, un adaptador Ethernet de 1 Gb y 1 puertos, un kit de rieles SFF fáciles de instalar, un kit de brazo para gestionar cables, una fuente de 500 W. Garantía de fábrica de 3 años.
	Procesador: Familia de procesadores específicos para servidores hasta 8 núcleos, frecuencia básica de 1.8 Ghz hasta 3.2, cache de 11mb hasta 16.5mb compatible con la carga de trabajo del sistema ofertado. Memoria: hasta 32GB (2 x 16GB) PC4-2666V-R DDR4 RDIMM
Características específicas o equivalente	2 x Hot Plug 3.5in Large Form Factor Smart Carrier Smart Array E208i-a SR
	Fuente 500W Ethernet 1Gb
	Garantía de fábrica de 3 años.
Características constructivas	Formato 2 U
<b>ITEM 10</b>	<b>Licencias Tipo 1: Servidor Remoto</b>
	Deberá posibilitar la integración con otros sistemas y aplicaciones, periodo de retención ilimitado, para tener acceso a las grabaciones de vídeo siempre que las necesite. Deberá ser practico y fácil de actualizar.
	<b>Herramientas de búsqueda</b>
Características generales	Cifrado basado en certificados para proteger el tráfico de datos (vídeo, audio, metadatos), originado en el servidor de grabación y recuperado por los componentes conectados.
	Protección mediante contraseña, aceleración por hardware, almacenamiento Edge y servidores failover, mapas con múltiples capas, autenticación doble, gestor de alarmas, metadatos, mapas y alarmas.
	Licencias perpetuas, hasta 48 cámaras por servidor de grabación. 1 servidor de grabación por sistema para esta licencia.
	Motor de reglas flexible. Rendimiento y escalabilidad. Gestión centralizada.
	Microsoft Active Directory. Buffering pregrabación en RAM.
	Descodificación acelerada por hardware (Quick Sync) Quality Recording
	<b>Integración</b>
Características específicas o equivalente	Integración de aplicaciones de terceros, screen recorder, metadatos, Add-on
	<b>Ciberseguridad y derechos de usuario</b> Autenticación Kerberos
	Cifrado de comunicación (grabación, gestión y servidor móvil) Acceso restringido de usuario por tipo de cliente

**Doble autorización** Monitorización e investigación Función de mapa

Búsqueda centralizada Máscara de privacidad Notificación push Gestor de alarmas Panel de usuario

Failover y redundancia Servidor de eventos failover Servidor failover de gestión

#### ITEM 11 Licencias Tipo 4: Servidor Centralizado

Características mínimas del sistema de gestión de video vigilancia confiable.

El SNPP necesita una vigilancia constante y fiable durante las 24 horas y los 7 días de la semana y 365 días del año.

La plataforma debe ser altamente personalizable, ofreciendo múltiples funciones de acuerdo a las necesidades de la Institución.

Considerando que no existe una solución única para todos los escenarios de video vigilancia y que cada operación es diferente, este concepto de plataforma debe ser abierta a las necesidades de la Institución, permitiendo la compatibilidad con varias marcas, modelos de cámaras y dispositivos.

Además, la plataforma de poseer la capacidad de incrementar equipos a gran escala. Deberá admitir un número ilimitado de servidores de grabación para que pueda ampliar el sistema sin problemas. Deberá conectar varios sitios con una arquitectura de infraestructura abierta y flexible, que permite conectar los sistemas individuales multimarca en una jerarquía padre/hijo de sitios federados, Gestionando de manera centralizada la video vigilancia distribuida en varias instalaciones.

Características  
Generales o  
equivalentes

El sistema integral de vigilancia, debe ser abierta y con capacidad de aprovechar la innovación de toda una industria, siendo compatible el 100% con otras marcas y dispositivos, que permita la posibilidad de agregar nuevas tecnologías a medida que se desarrollan, lo que facilite actualizar y mejorar continuamente el sistema de seguridad.

Interfaz gráfica fácil de utilizar, amigable.

El diseño deberá combinar simplicidad, sofisticación y ofrecer a los operadores la posibilidad de tener el control absoluto de cualquier situación al instante. Esto deberá garantizar un aprendizaje sencillo y una gran facilidad de uso, sin renunciar a prestaciones avanzadas.

Interfaces fáciles de utilizar que se deben ajustar a usuarios individuales en función de los niveles de seguridad y las áreas de responsabilidad.

Mapas interactivos que le ofrecen una completa panorámica general de la instalación local y remotas completas.

Búsqueda centralizada para que pueda buscar secuencias de vídeo, alarmas, eventos, marcadores y movimiento en un mismo sitio.

Sin brechas de seguridad,

Toda la plataforma deberá estar en un entorno estructurado: seguridad en el diseño, seguridad por defecto y seguridad en la implementación, diferentes mecanismos de seguridad que mantienen su sistema y sus datos protegidos contra amenazas internas y externas y en cumplimiento a la ley de datos.

Sistema

Tipo de implementación Gestionado centralmente, multiservidor. Licencias perpetuas.

Número de cámaras por servidor de grabación ilimitada. Número de servidores de grabación por sistema ilimitado. Motor de reglas flexible.

Rendimiento y escalabilidad Gestión centralizada.



Características  
específicas o  
equivalente

Microsoft Active Directory. Buffering pregrabación en RAM.

Decodificación acelerada por hardware (Quick Sync). Almacenamiento Edge.

Scalable Video. Quality Recording.

Decodificación de vídeo acelerada por hardware (GPU). Monitor del sistema.

Integración.

Integración de aplicaciones de terceros Screen Recorder.

Metadatos. Add-on .

Video Wall. Interoperabilidad

Interconnect ubicación central/remota. Federated Architecture ubicación central/remota. Ciberseguridad y derechos de usuario Autenticación Kerberos.

Cifrado de comunicación (grabación, gestión y servidor móvil). Acceso restringido de usuario por tipo de cliente.

Doble autorización.

Cifrado base de datos de medios y firma digital. Derechos de gestión por niveles.

Verificación en dos pasos. Monitorización e investigación Función de mapa.

Búsqueda centralizada. Máscara de privacidad. Notificación push.

Gestor de alarmas. Panel de usuario. Marcador manual.

Marcadores basados en reglas. Plano inteligente.

Bloqueo de evidencias. Failover y redundancia Servidor de eventos failover. Servidor failover de gestión.

Servidor de grabación failover (activo/pasivo).

ITEM 12

**Biometría Facial, registro de Licencia Perpetua, único pago, ilimitadas cámaras de analítica facial**

Características  
Generales o  
equivalentes

Deberá ser un motor de reconocimiento facial puro que permite el procesamiento eficiente y preciso de rostros en imágenes y transmisión de video en vivo y puede ejecutarse en una amplia gama de dispositivos.

La identificación sin contacto para fines de seguridad y control de acceso que agrega las funciones de extracción y coincidencia del descriptor facial.

Un descriptor de rostro es un conjunto de características que describen el rostro, invariante para la transformación del rostro, el tamaño u otros parámetros. La coincidencia de descriptores faciales permite juzgar con cierta probabilidad si dos imágenes faciales recibidas pertenecen a la misma persona.

Contar con la opción de uso típicos para 68 puntos de referencia para la segmentación y la estimación de la postura de la cabeza.

Deberá contar con una precisión de la estimación de género del 99,8%.

Interpretación amplia de la manifestación de ciertas emociones: Enfado, asco, temor, felicidad, sorpresa, tristeza y neutral.

Deberá ser una exclusiva arquitectura modular unificada que permitan el alojamiento y la gestión simultánea de casos de reconocimiento e identificación de rostros de uso múltiple en prácticamente cualquier Framework.

Capacidad para la recopilación de datos sobre el tráfico de clientes, ingreso, edad, sexo e incluso el estado emocional permiten detectar y segmentar la tendencia del publico visitante.

El algoritmo de analítica de reconocimiento facial también deberá ser instalado en el ítem 1 (Cámara Tipo 1: Procesador de captura y procesamiento de imagen preparada para integración, Inteligencia Artificial y Deep Learning) en un contenedor tipo Docker en el propio hardware para lograr el procesamiento en el borde.

El sistema de biometría facial, detección de rostro y reconocimiento deben estar integrados nativamente en la plataforma de gestión de video solicitada en los ítems 10 y 11(Licencias Tipo 1: Servidor Remoto, Licencias Tipo 4: Servidor Centralizado). deberá estar integrado por API con el sistema de KYC de lectura de cédulas de identidad y/o documento equivalente, también deberá estar integrado por API con el sistema de gestión de control de acceso de los molinetes de flujo rápido, para que de esta manera, una vez registrado en el sistema, las autenticaciones serán por el hardware de procesamiento de imagen ítem 1 (Cámara Tipo 1: Procesador de captura y procesamiento de imagen preparada para integración, Inteligencia Artificial y Deep Learning) 1:N liberando o no el acceso o generando alarmas de acuerdo a los registros en la base de datos e inteligencia.

El procesamiento de la analítica Facial no debe usar GPU (no hacer uso o trabajar por el procesador GPU de la placa de video).

Para cámaras remotas no deberá usar más de 0.5 mb x cámara.

Deberán ser licencias de único pago, perpetua e ilimitada para la cantidad de cámaras instaladas y conectadas al sistema.

Sin limitación de cámara para el reconocimiento facial (la limitación esta únicamente por la capacidad del hardware). Integración nativa con el sistema de video y sistema de control de acceso.

La plataforma deberá asentar 1.000 registros de reconocimiento facial en la base de datos del servidor, valido para todas las camaras activas del sistema.

La tecnología de reconocimiento facial ofertada deberá contar con aprobación del NIST (National Institute of Standards and Technology) (FRVT), precisión superior al 99% o norma similar y equivalente o.

Características específicas o equivalente

El servidor de gestión de datos biométricos deberá estar disponible en todas las cámaras del alcance de este proyecto con las siguientes prestaciones:

Identificar grupos de visitantes. Identificar ruta de los visitantes. Identificar tiempo de espera.

Estimar la edad, género, emociones. Detección de rostro.

Extracción de descriptores faciales.

Almacenamiento de descriptores faciales y búsqueda rápida. Agrupación lógica del descriptor facial.

Descriptor facial 1: 1, 1: N y N: N coincidencia.

Estimación de atributos faciales (por ejemplo, género, edad y emociones).

Registro de eventos de coincidencia de rostros y generación de notificaciones.

Deberá contar con herramienta para la detección y el seguimiento de rostros en múltiples fuentes. Permite al usuario elegir las imágenes faciales más adecuadas para reconocimiento facial de una secuencia de fotogramas de vídeo.

Características constructivas o equivalentes

API tiene la capacidad de integrarse a cualquier software y hardware de Video Vigilancia modernizándolo con Algoritmos de Inteligencia Artificial.

ITEM 13

Licencias de Integración y Automatización de Flujos Modalidad instalación

Características  
Generales o  
equivalentes

La plataforma LOW-CODE de multi integración y automatización de flujo de trabajo deberá ser una herramienta basada en nodos, distribuida bajo el modelo de software libre y abierta (Commons Clause) de código justo.

La herramienta deberá dar opciones de mover y transformar datos entre diferentes aplicaciones y bases de datos de manera rápida, sencilla y sin quedar atrapado en documentos API y solucionar errores de C.O.R.S. (Cross-Origin Resource Sharing).

Descripción general del nodo

Los nodos son los componentes básicos de los flujos de trabajo de la herramienta. Son un punto de entrada para recuperar datos, una función para procesarlos o una salida para enviarlos. El proceso de datos incluye filtrar, recomponer y cambiarlos. Puede haber uno o varios nodos para cada API, servicio o aplicación. Puede conectar varios nodos, lo que permitirá crear con ellos, flujos de trabajo simples y complejos de forma intuitiva.

Características  
específicas o  
equivalente

Integraciones

Deberá estar disponible para más de 200 integraciones (nodos) diferentes que le permitirá conectar varios servicios existentes y crear nuestros flujos de trabajo de automatización entre aplicaciones o dentro de la misma aplicación, además deberá contar con ejemplos de flujos de trabajo automatizado.

Prestaciones de esta herramienta

Nuevas u todas las integraciones que no sean nativas entre sistemas, se deberán hacer a través de esta herramienta.

Deberá ser auto hospedado, fácilmente ampliable e incluso utilizable con herramientas internas.

La herramienta LOW-CODE de integración y automatización de flujo de trabajo deberá ser ejecutada en un servidor local.

El oferente deberá proveer toda la documentación para la creación de nuevas integraciones (nodos) personalizados.

Características  
constructivas o  
equivalentes

La plataforma deberá ser instalada, configurada y mantenida para su instancia de operación.

OAuth administrado para autenticación.

La herramienta contará con actualizaciones sencillas a las versiones más recientes sin costos adicionales. (Commons Clause) de código justo

La modalidad de entrega de esta herramienta será: licencia Commons Clause de código justo, la instalación, documentación y su respectivo entrenamiento.

ITEM 14

Sistema de Control de Acceso

Sistema de control de acceso y credenciales con gestión integrada en una única plataforma, con las siguientes prestaciones:

Multi-Idioma: en español como lengua principal. Capacidad de Gestionar de Acceso y Seguridad. Capacidad de Gestionar Porterías y Visitantes. Capacidad de Gestionar Tercerizados y Aliados.

Capacidad de Control de EPI para Colaboradores, Visitantes y Tercerizados. Capacidad de Gestionar el Control de la Flota de Vehículos.

Deberá estar integrado con la plataforma de gestión de videovigilancia ofertada en el ítem 10 y 11 (Licencias Tipo 1: Servidor Remoto, Licencias Tipo 4: Servidor Centralizado).

Con capacidad de controlar registros de tarjetas y biometría.

Características

Generales o equivalentes

Deberá estar integrado con la plataforma de gestión de biometría facial ofertada en el ítem 12 (Biometría Facial, registro de Licencia Perpetua, pago único, ilimitadas cámaras de analítica facial).

Capacidad de Monitoreo y prevención de salud por Reconocimiento Facial: Temperatura, el uso de Mascaras.

Deberá ser Arquitectura 100% Web.

Contar con transmisión segura de datos Http sobre SSL.O Transmisión de Datos y páginas encriptadas.

Rastreo y auditoría con logs protegidos. Gestión de Usuarios vía Active Directory.

Disponible para servidores dedicados con opción de Cloud. Uso de Token para ambientes críticos conformidad con las leyes vigentes que reguan el manejo de datos y LGPD

Capacidad de Integración con Sistema de Gestión Empresarial (ERP) del SNPP (Sistemas, aplicaciones y productos para el procesamiento de datos.) por API.

Sistema de control de acceso y credenciales con gestión integrada

La solución de seguridad integrada deberá cumplir los siguientes criterios:

El software debe ser compatible con varias tecnologías de seguridad, como ser: Subsistema de control de acceso, subsistema de supervisión por imágenes, subsistema de detección de incendios, gestión de la identificación, gestión de alarmas, gestión de las puertas de entrada, control de los activos, gestión de la frecuencia, gestión y supervisión de los vehículos, reconocimiento facial, lectura e identificación de las matrículas de los vehículos, automatización y gestión de los servicios públicos.

El sistema debe ser una solución de seguridad con recursos avanzados que garanticen la asistencia, el apoyo operativo y estadístico a todas y cada una de las situaciones, en áreas internas, externas o remotas (en cualquiera de las sedes del SNPP establecidas a nivel Nacional), supervisadas en tiempo real o no, localmente y a distancia. Otro aspecto importante que deben observar los oferentes es, que la solución tendrá que ser integrada con las tecnologías disponibles en nuestros subsistemas, es decir, que las soluciones establecidas como el Sistema de Monitoreo de Vídeo Vigilancia, entradas, alarmas, intrusión e incendio, tengan una estrecha interrelación y puedan intercambiar información entre sí de forma totalmente full dúplex,

permitiendo generar acciones y reacciones instantáneas y coordinadas, proporcionando información correcta y eficaz a los administradores de la solución y dentro del marco de la observancia y el cumplimiento de las normas y reglamentos técnicos necesarios para el correcto y fiel cumplimiento de este objetivo.

En particular, con respecto a las características del software destinadas al control de acceso, así como toda la línea de dispositivos de control debe ser ofertado para leer y escribir tarjetas inteligentes - Mifare®, sin contacto, ISO 14443A, que permite la inserción de datos biométricos (huella digital) para la validación positiva en los puntos de control considerados de alta seguridad, lo que permite una ganancia en la flexibilidad en la operación, sin degradar el rendimiento y el bajo costo de la gestión de la información.

Los dispositivos para la lectura de tarjetas deben funcionar sin necesidad de realizar consultas al servidor para validar la información leída, por lo que las tarjetas de identificación deben llevar toda la información necesaria para validar el acceso. La solución ofertada deberá ser potente, es decir, tanto el hardware como el software de control de accesos deben soportar tarjetas de las siguientes tecnologías:

\* tarjeta de código de barras, \* código de barras 2D, \* bandas magnéticas, \* Qrcode,

\* RFID 125 Khz abatrack y wiegand de proximidad, \* tarjetas inteligentes Mifare®,

\* tarjetas inteligentes de contacto, \* tarjetas inductivas,

\* también activaciones por contraseña numérica, y cada tecnología puede o no combinarse con validación biométrica en la forma 1:1 o 1: N.

La solución también debe soportar la lectura y escritura en tarjetas de tipo PKI las tarjetas con triple tecnología, es decir, tarjeta inteligente Mifare®, tarjeta inteligente con chip de contacto y RFID 125 Khz.

Para las tarjetas PKI, debería ser posible leer los datos biométricos en los dispositivos AFIS. (Sistema de Identificación Automática por Huellas Digitales -AFIS - Automated Fingerprint Identification Systems por sus siglas en inglés).

#### Funciones de los dispositivos de control de acceso a la plataforma

Para cumplir con el sistema propuesto el software, entre otras características específicas, debe disponer, ya en su versión nativa, cuanto sigue:

Debe presentarse en un menú con funciones y subfunciones por ítems cuya finalidad será incorporar datos para que el sistema pueda alimentarse de todo tipo de información posible y necesaria, y a partir de esta información, proveer el monitoreo y la gestión de acceso y seguridad;

La solución debe ser completamente jerárquica, permitiendo la creación de perfiles de acceso para cada tipo de usuario, es decir, operador de conserjería, administradores, operador de registro, operador de seguridad, operador de CCTV, etc.

El administrador principal de la solución podrá restringir los elementos accesibles en el menú de cada usuario, aunque pertenezcan a la misma clase, sin embargo, cualquier liberación o restricción debe ser almacenada en un registro de auditoría para ser recuperada a través de perfiles de filtro e informes.

Además de los registros relacionados con los cambios en los perfiles de acceso al sistema, el software debe contar con registros de auditoría de las acciones realizadas en el sistema por los usuarios registrados, y se puedan

emitir informes a través de filtros específicos.

Debe trabajar en diferentes frentes de seguridad, como el monitoreo de alarmas de incendio, la gestión de imágenes, la gestión de flotas, el control georreferenciado de personas, el control de accesos, la RFID, el monitoreo web móvil, la manipulación y la intrusión, así como la gestión de estas alarmas en modo manual y automático.

Permitir la visualización de imágenes en tiempo real de las zonas controladas. Obtener grabaciones de los momentos desencadenantes de los sucesos.

Ajustes de la cámara controlados según las necesidades de la imagen (zoom y dirección).

En este caso, al buscar un acceso concreto, el software debe traer el clip de vídeo asociado a él, lo que debe permitir ver la imagen de quién ha accedido a un punto de control determinado, ya sea una puerta, un molinete o una barrera vial.

El software debe disponer de recursos para controlar el tiempo de apertura de la puerta, generando alarmas cuando el tiempo de apertura es superior al establecido, intentos de robo e intentos de acceso indebidos.

El software debe permitir verificar la fecha/hora y el lugar del acceso realizado por el propietario de una tarjeta de identificación o registro biométrico - registro de auditoría (log Eventos).

También debe interactuar con el subsistema de CCTV ofertado en los ítems

10 y 11 (Licencias Tipo 1: Servidor Remoto, Licencias Tipo 4: Servidor Centralizado) para la recuperación de las imágenes correspondientes a cada evento de acceso generado, de las alarmas relacionadas con la detección de imágenes y también de las alarmas relacionadas con la intrusión de acceso.

Debe permitir el registro, en una base de datos para su auditoría, de "todos los eventos", a saber: eventos de control de apertura de puertas autorizados, no autorizados, y eventos administrativos (como la creación de un nuevo usuario, por ejemplo, operador, etc.);

Según el nivel de seguridad, debe ser posible, en determinados puntos de acceso restringido, operar con doble tecnología: - identificación y/o validación positiva (mediante la lectura de la tarjeta de identificación y la biometría de las huellas dactilares o facial).

La tecnología dual, no debería interferir en los tiempos de respuesta del sistema ya que los datos de validación biométrica formarán parte de los datos incorporados en las tarjetas de identificación "Smart Card".

Los datos biométricos estarán nativos o integrados a la base de datos del sistema de gestión de biometría facial ofertado en el ítem 12 (Biometría Facial, registro de Licencia perpetua, único pago, ilimitadas cámaras de analítica facial) recibiendo mínimamente estos datos:

Detección de rostro.

Extracción de descriptores faciales.

Almacenamiento de descriptores faciales y búsqueda rápida. Agrupación lógica del descriptor facial.

Descriptor facial 1: 1, 1: N y N: N coincidencia.

Estimación de atributos faciales (por ejemplo, género, edad y emociones).

Función de pánico o coacción

Los puntos de acceso bajo control de identificación biométrica deben prever la implementación de la función "biometría de pánico";

La Biometría del Pánico" se configura en la opción de utilizar una biometría alternativa a la normal para el acceso, pero en este caso generando un evento como alarma de pánico al centro de monitoreo, movilizándolo el protocolo de seguridad y consecuentemente el equipo de seguridad para

que acudan al lugar donde se encuentra el usuario bajo coacción, pero aun liberando el acceso a la puerta.

La ejecución de esta compleja función, el sistema de gestión de datos biométricos deberá contar con estimación de atributos faciales precisamente interpretaciones amplias de emociones, en la práctica es entrenar una expresión facial de la manifestación que corresponde a una emoción (el pánico) previamente entrenada y envía como evento al sistema de gestión de acceso.

Cada imagen debe ser registrada con fecha, hora y lugar de origen.

Las imágenes deben localizarse a través de una búsqueda con parámetros de fecha, hora o lugar y enviarse por correo electrónico a un destinatario registrado.

Debe permitir la importación y exportación de datos de sistemas heredados con procesos automáticos configurados en la aplicación a través de archivos con interfaces definidas.

Además de los datos personales, el SOFTWARE debe ser capaz de exportar datos para controlar los horarios de trabajo, las tolerancias de tiempo de acceso.

Debe utilizar la tecnología TCP-IP para controlar a las personas en las zonas supervisadas y restringidas al acceso común.

Para equipos integrados, en una sola terminal de control debe ser posible controlar hasta 24 sensores (de presencia, activos, pasivos, magnéticos y de vibración) y 1 Mb de memoria total.

Con los equipos integrados al sistema en caso de fallo de la comunicación (en la red de datos o en la red eléctrica), los terminales deben funcionar sin conexión y en este modo deben disponer de inteligencia distribuida que trabaje con listas de liberación o bloqueo, garantizando el acceso seguro de las personas autorizadas.

La seguridad interna del sistema (datos e información) debe mantenerse mediante perfiles de acceso y contraseñas y credenciales configurados durante la instalación del producto.

El software debe ser inmune al fraude, ya que la información debe estar encriptada en la base de datos, que se suministrará junto con el software de control.

El software debe tener una interfaz intuitiva y amigable, con excelente navegabilidad y presentación, y el monitoreo de eventos no autorizados con generación de alarmas en una pantalla gráfica, a través de mapas gráficos de las instalaciones de la SNPP, debe ser parte integral de la solución ofertada.

El software debe tener archivos de ayuda individuales dentro de cada aplicación que informen sobre el funcionamiento específico de cada pantalla. Estas ayudas deben ser accesibles en todo momento cuando surjan preguntas sobre el registro, en la barra de navegación principal del sistema. (deberán estar en idioma español).

Como elemento de seguridad de la solución, el SNPP solicita, como requisito indispensable, que el software esté protegido contra copias indebidas a través de un dispositivo físico, y que disponga de una herramienta web para el control de versiones, emisión de actualizaciones y cuestiones relacionadas.

Debe ser posible registrar varias clases de usuarios, nuevos empleados, aprendices, visitantes, terceros, visitantes especiales (con largos periodos de acceso frecuente y consecutivo), pudiendo registrarse unitariamente y/o en grupos, incluso mediante rutinas específicas de importación de datos vía XML, CSV, archivos txt y vía base de datos o de la API a la Plataforma LOW- CODE de multi integración y automatización de flujo de trabajo.

Emitir informes de acceso, utilizar planos de las áreas del SNPP (que se implementarán en el sistema) para monitorear los ambientes, etc.

El software debe tener un módulo de gestión para ser utilizado por el administrador del sistema, que podrá supervisar el acceso a las instalaciones del SNPP, así como extraer informes y configurar los equipos a través de su interfaz.

Debe tener el reconocimiento facial integrado con el sistema de control de acceso, lo que permite activar el dispositivo de control de la puerta a través de la biometría facial del usuario o recibir algún evento como el pánico biométrico u otros.

Como condición fundamental para las integraciones, las bases de datos de los dos sistemas (control de acceso y gestión de datos biométricos) deben permitir acceso total a la Plataforma LOW-CODE de multi integración y automatización de flujo de trabajo lo que dará total autonomía a la SNPP para crear nuevas integraciones y flujos de trabajo personalizables de acuerdo a las necesidades y las prestaciones de cada sistema u otros a futuro.

Debe conservar los historiales de toda la información de los empleados, manteniendo un registro desde la contratación hasta el despido de ese empleado.

Del mismo modo, debe mantener registros de todas las acciones realizadas en el sistema en las áreas de control que impactan en el proceso de configuración corporativa (reglas de negocio).

La seguridad interna del sistema (datos e información) debe mantenerse mediante perfiles de acceso y contraseñas (credenciales), configurados en la instalación del producto. Esta información debe ser encriptada antes de ser almacenada en la base de datos, para garantizar la seguridad de la información.

El sistema debe tener una interfaz intuitiva y amigable, con una navegabilidad y presentación óptimas.

El software debe ser una herramienta de trabajo que supervise los eventos en tiempo real.

El sistema debe utilizar tecnología y entorno 100% web, siendo necesario para su uso desde cualquier puesto de trabajo, únicamente un navegador.

Debe ser posible insertar planos de los lugares con los dispositivos de control colocados en ellos para una supervisión fácil e intuitiva, pudiendo interactuar con estos dispositivos.

Debe ser posible en la misma planta activar, desactivar, configurar, comprobar si está en línea o fuera de línea, insertar y quitar, etc. todos los dispositivos que son controlados por el software a través de las plantas.

El software debe tener una interfaz para el registro de usuarios, nuevos usuarios, visitantes y vehículos.

Características  
específicas o  
equivalente

Debe permitir la programación de visitas a través del sistema vía web, es decir, sin necesidad de utilizar un software cliente, con opciones de reprogramación, rescate de vistas anteriores y módulo de visualización y control de vistas programadas.

Debe tener un módulo compatible con tótem de autoservicio, para generar tarjetas de visita, emitir QRcode, asignar credencial al rostro, emitir tarjetas temporales para empleados, servidores, terceros o cualquier otro tipo de personas gestionadas por el sistema. También debe tener recursos para comprobar la foto de la persona y comprobar el QRcode recibido por correo electrónico por el usuario.

En cuanto a la gestión del acceso, el software debe tener:

1. Registro y almacenamiento en tiempo real de todos los intentos de acceso válidos y no válidos.
2. Control total de acceso y seguimiento de empleados, terceros, socios, candidatos y visitantes.

Definición y creación de políticas de seguridad, como días laborables y festivos, franjas horarias independientes para el control de acceso, registro horario y uso de comedores, incluida la gestión del crédito.

Trazabilidad con la gestión, el control de las rutas, los niveles de acceso y anti-pass-back.

Gestión de contratos de empresas subcontratadas, validando el acceso durante la vigencia del contrato y facilitando la recogida de credenciales en los molinetes al finalizar el contrato y el acceso de salida de los empleados de terceros - (empresas de seguridad, por ejemplo).

Ampliación de las franjas horarias para realizar la liberación de horas extras, autorizaciones de personas y salidas de visitantes.

Control de prestaciones, que permite gestionar la distribución de artículos como, por ejemplo, beneficios, bonos de transporte, premios, etc., incluyendo la carga y el control de los créditos a través de la tarjeta inteligente sin contacto.

Registro de control de persona no Grata lista negra, alertando en tiempo real, eventuales registros no deseados, por ej. Recibiendo el evento de un rostro o una chapa registrada en lista negra o una lista de seguimiento.

Gestión y distribución de los EPI para el control de las personas en áreas eventuales que deseen este tipo de control, bloquear el acceso de la persona en cualquier dispositivo cuando el EPI está vencido, proporcionando así una mayor gestión de la seguridad de la persona.

Sobre la gestión de flotas de vehículos, el software de control de acceso debe tener las opciones de:

Registro completo de vehículos, modelos, placas y otras opciones para controlar un vehículo.

Gestión del mantenimiento, seguro e historial de uso.

Flujo de trabajo para la solicitud de vehículos y cuando se aprueba, el usuario debe presentar su tarjeta y la tarjeta del vehículo para que la puerta se abra cuando se relacionan y se liberan.

Sobre la gestión de la identificación de las personas, el software de control de acceso debe tener:

Identificación biométrica: biometría dactilar, venas u otra en modo 1 a 1 o 1 a varios y la biometría de reconocimiento facial. El reconocimiento facial debe funcionar en modo 1: N (uno a muchos).

Más de un nivel de validación, en el propio controlador: Tarjeta de ID y contraseña.

Registro y contraseña. Credencial y biometría.

Credencial, biometría y contraseña.

Utilizando la tecnología de identificación de la tarjeta inteligente Mifare® tipo A4 Kb, tamiz de seguridad deben ser almacenadas en la tarjeta.



La gestión de las insignias físicas como tarjetas también debería permitir: Diseño de las insignias para su impresión.

Control de la ruta de la tarjeta. Insignias extraviadas.

Bloqueo y liberación de las tarjetas en línea.

Eliminación automática de las insignias a través del sistema o cuando el límite de tiempo expira.

En cuanto al uso de la biometría de las huellas dactilares, el software debe permitir:

Recoger y almacenar al menos dos dedos del usuario;

Biometría de la palma de la mano mediante la recogida y el almacenamiento de la geometría de la mano.

Biometría de la vena del usuario.

La biometría facial a través de la captura de rostros, su almacenamiento, comprobación e integración con el control de acceso, permite que un rostro registrado pueda ser comparado entre N otros en una base de datos y luego permitir la apertura o no de un controlador de acceso, deberá estar plenamente integrado al sistema de gestión de datos biométricos, su base de datos y como ya fue mencionado, de la API a la Plataforma LOW-CODE de multi integración y automatización de flujo de trabajo.

Módulo de control de doble factor de autenticación para entornos con un alto nivel de seguridad, tras la autenticación con tarjeta y/o biometría, el usuario debe introducir una clave y recibir una contra clave para confirmar en el controlador de acceso. Si hay coincidencia, el acceso será liberado.

Sobre el registro de visitantes debe tener el software de control de acceso:

Un módulo integrado y propio del sistema (no se aceptarán interfaces integradas de terceros u otro software que opere en paralelo), y el sistema debe permitir un número ilimitado de registros de puertas, todo vía web a través del navegador, sin que se cargue la tarea de solución para la administración de puertas de acceso de personas.

El módulo de portería tendrá las siguientes funciones, pero no se limitará a ellas:

Control, distribución e impresión de distintivos provisionales para empleados, terceros y otras clases de usuarios.

Control del material entrante y saliente de los empleados y visitantes. Control de guarda de equipaje y control de llaves.

Registro de ocurrencias.

Control de rutinas de revisión del personal de manera automática y automatizado de forma aleatoria a través de la programación realizada en los controladores de acceso y el software, mediante la generación de sirenas, lámparas o alarmas en el sistema.

Tarjetas de acceso para visitantes, acompañantes y grupos de visitantes.

La programación de las visitas puede ser realizada previamente por el propio visitado, garantizando una mayor agilidad a la hora de acreditar a un visitante o grupo de visitantes.

Seguimiento en línea del acceso de los visitantes.

Captura de la foto del visitante, anverso y reverso del documento a través de la webcam o dispositivo de captura KYC, posibilidad de integración automática con escáner para la captura de documentos.

Búsqueda en la base de datos de visitantes a través de múltiples documentos, CI, pasaporte, registro de conducir, tarjeta de entidad profesional, etc.

Control de la estancia del visitante por día, fecha y hora de validez con control de los lugares a los que puede acceder el visitante.

Definición de control de visitas, visitas especiales y visitas que deben introducir los distintivos en una posible caja fuerte (boca de lobo) para su recogida a la hora de salida.

Control de los EPI de los visitantes.

Impresión de insignias, según el diseño definido, así como código de barras

encriptado.

Registro de todos los accesos de los visitantes, intentos de acceso, válidos y no válidos.

Captura de la huella dactilar del visitante en el momento de la acreditación, si el visitante utiliza el acceso biométrico.

Tras el registro y/o la programación, el software debería enviar automáticamente un correo electrónico al visitante con la información de la visita y su QRcode de acceso.

En cuanto a la gestión de alarmas y plantas, el software debe permitir:

Utilizando el plano del lugar vigilado, el software debe gestionar los eventos de acceso y las alarmas de forma sencilla.

Manejo y reconocimiento de eventos de alarma y acceso.

Debe mostrar el vídeo en el momento de la ocurrencia permitiendo también la visualización en directo de la imagen de la escena.

Debe tener un sistema de sonido a través de archivos de onda pregrabados en el software.

Debería ser posible establecer la prioridad de visualización de las alarmas.

Debe ser posible enmascarar las alarmas no controladas definidas por franjas horarias.

Debe ser posible configurar reacciones automáticas a eventos de alarma y acceso, como la activación de la sirena o el envío de un correo electrónico.

Debe ser posible configurar la redirección y el zoom automático en la ubicación de la ocurrencia del evento en la planta.

Debe ser posible configurar la ejecución de comandos directamente desde la planta, como, por ejemplo, la liberación de controladores para abrir puertas o el desbloqueo de molinetes para situaciones de emergencia.

Debe ser posible reconocer y gestionar las alarmas de forma individual o por grupos.

Debe ser posible consultar e informar de las alarmas tratadas, reconocidas o no tratadas.

Deberá ser posible realizar consultas de acceso vinculadas con la hora del evento de acceso o de la alarma y mostrar la reproducción de vídeo. Dicho flujo de vídeo puede ser tomado en cualquiera de los siguientes 2 formatos de compresión, MPEG4, H.264, flujos de vídeo múltiples.

Debería ser posible vincular las cámaras a los controladores o dispositivos de alarma.

Debería ser posible identificar el último lugar donde entraron las personas.

Debe ser posible realizar consultas e informes de personas presentes y ausentes con detalles y totales.

Debe ser posible consultar e informar de los accesos válidos e inválidos de las personas, aunque cambien de placa en determinados periodos.

Debe posibilitar la realización de controles de accesos supervisados y simultáneos, es decir, para entrar en un determinado lugar sólo pueden acceder simultáneamente dos usuarios previamente registrados y autorizados.

Debe ser posible realizar el acceso con un número máximo y mínimo de usuarios, es decir, sólo se puede acceder a determinados lugares si un cierto número de usuarios, previamente determinado, entra y sale del respectivo nivel de control. Por lo tanto, si un lugar en particular se registra en el sistema para esta función, el mismo número de personas que entran en el sitio debe ser el mismo número de personas a salir, y la liberación de acceso tanto en la entrada y la salida se concede después de la verificación de la biometría y / o tarjeta de identificación, el número de usuarios definidos.

El software debe tener integración con el Active Directory de Windows y por tanto, cada usuario registrado para esta funcionalidad sólo puede entrar en su puesto de trabajo cuando haya superado el control de acceso o el nivel de control de acceso predeterminado en el sistema.

El software debe ser 100% tecnología web y ofrecer características como: Actualización centralizada de datos (Base de datos y aplicación).

No es necesario instalar el cliente en las estaciones de trabajo de operación, supervisión y administración.

Posibilidad de acceder al software en el lugar donde está instalado o, a distancia, desde un punto con conexión a Internet, siempre que el inicio de sesión se realice mediante ambiente seguro, uso autenticado y contraseña.

Utilización a través de Intranet y Extranet, VPN. Mantenimiento del sistema a distancia.

El software debe utilizar la protección de datos del cliente mediante certificado digital (HTTPS).

Debe utilizar un dispositivo de bloqueo hard lock como HASP (Hard lock o traba de Hardware) para proteger el sistema en versiones físicas o virtuales.

Instalación en servidor virtual.

Debería ser posible acceder a ello al menos a través de los navegadores Internet Explorer 8 o FireFox 1.5.0 o superior.

Debe utilizar las siguientes plataformas tecnológicas:

Servidor web: Apache. o similar

Servidores Linux o Windows: 2000/XP/2003 o superior. Base de datos: Oracle 9i o SQL 2000 o superior.

El software de grabación y gestión, integrado en la plataforma de seguridad, debe cumplir las siguientes especificaciones:

Debe ser de alto rendimiento, con un funcionamiento fácil de usar, con alarmas en la pantalla, y controles, menús y otras acciones a las que se accede a través del ratón.

Debe permitir la integración a través de la red TCP/IP con otros módulos de grabación en otras unidades y también permitir la visualización remota a través de Internet.

Debe contar con recursos de distribución y escalabilidad que garanticen que la comunicación con los controladores de acceso a puertas, torniquetes, puntos electrónicos y aparcamiento se realice en línea, de forma rápida, sin generar colas, pudiendo estar distribuida por regiones, sedes y/o otras formas de distribución.

Debe tener una interfaz para insertar planos o mapas de los lugares vigilados, con las respectivas cámaras posicionadas, para mayor facilidad y control de las funciones de gestión, aumentando la eficiencia y la respuesta con acciones de contingencia.

Debe presentar las alarmas de forma jerárquica al operador encargado de la supervisión, es decir, clasificando las alarmas en niveles de criticidad alta, media y baja. La asociación de los niveles de criticidad a cada evento relacionado con los puntos controlados se definirá en el proyecto ejecutivo y según las necesidades del Contratista.

Activará un evento de alarma, automáticamente, cuando:

Un objeto dejado en un punto de vigilancia de la cámara se identifica según un tiempo que puede parametrizarse en el software.

Intento de acceso indebido a través de barreras y cerco perimetral.

Además de generar el evento de alarma, el modo de grabación se activará a una velocidad máxima de 25 FPS.

Recursos de integración con las otras plataformas del Sistema Integral de Control Inteligente:

Debe tener un Webservice para la integración con el software heredado.

Debe tener la posibilidad de poder integrarse con la plataforma SAP sin necesidad de ninguna personalización, teniendo en cuenta las necesidades futuras, debe permitir acceso dúplex para la generación y ejecución de flujos de trabajo a través de la API a la Plataforma LOW-CODE de multi integración y automatización de flujo de trabajo, sin necesidad de programación.

Debe disponer de recursos para compartir la información de los registros de acceso y las alarmas sin necesidad de acceder directamente a la base de datos, de forma que el usuario pueda crear el diseño necesario del archivo y crear horarios a través de un software para exportar la información.

Funcionalidades de Sistema de alarma y detección de incendios de la plataforma S.D.A.I.

La plataforma debe tener integradas las funciones de detección y alarma de incendios, y debe estar integrada de tal manera que la detección de la presencia de llamas, humo o calor, por cualquiera de los módulos sensores existentes, debe permitir la apertura de puertas, molinetes, portones y otros dispositivos de control de acceso del sistema según la configuración realizada cumpliendo con la norma NFPA101 u otras .

La solución deberá interpretar los sensores, panel de control de incendios, teclados, disparadores manuales, luces de emergencia y otros dispositivos relacionados con el sistema.

La solución S.D.A.I debe proporcionar un módulo de detección y alarma de incendios basado en imágenes, aprobado y certificado por UL y FM, de acuerdo con las especificaciones mencionadas a continuación.

El sistema proporcionará una arquitectura digital, basada en microprocesadores, inteligente y modular, con verdadera comunicación entre pares para la alarma y el control de incendios.

Debe diseñarse con una amplia gama de variables parametrizables, permitir la transmisión casi instantánea de información y la capacidad de realizar tareas de gestión de procesos, como la evacuación por voz, la desconexión del sistema de aire acondicionado, el control de las compuertas, las puertas, los ascensores, la seguridad, la CCTV y la interfaz con los sistemas de gestión de edificios.

#### ITEM 15

#### Molinete Tipo 1, por Pasaje de Flujo Libre

Deberá ser un molinete de doble paso, fabricado para alto flujo de personas y trabajar en la modalidad de flujo libre, siempre abierto, en caso de intento de paso sin autenticar, el cierre será automático.

Pasillo de 90 a 110 cm (PNE).

Características  
Generales o  
equivalentes

Deberá funcionar en modalidad unidireccional y bidireccional con la posibilidad de bloquear una sola solapa o una doble solapa.

Deberá tener incorporado un lector integrado a la base de datos y facial para la validación del acceso y asociación con el rostro.

Compatible con los principales lectores del mercado. Tarjeta inteligente Proximidad.

Biometría facial - Biometría digital.

Código QR Bares, podrá trabajar en modo bloqueado (cerrado). Tiempo de apertura y cierre de 1s.

Función antideslizamiento.

Sensores infrarrojos para el control del flujo con aletas giratorias con solapas giratorias.

Alarma por intento de fraude y por hacer dedo.

Control de flujo por visión artificial, que permite bloquear a los usuarios no autorizados.

Interfaz para la integración con la central de incendios. Central de alarmas contra incendios.

Orientación mediante pictogramas luminosos en ambas direcciones. Aviso sonoro de acceso permitido y denegado.

Configuraciones del corredor PNE.

Memoria de almacenamiento 8GB. Sistema de protección contra la caída. No hay rotura integrada en el equipo.

Autonomía en caso de fallo de alimentación 4hs. Permitir la instalación de baterías externas adicionales.  
Comunicación

Interfaces ethernet 10/100 Mbps. Tipo de lectores compatibles

Tarjeta inteligente Mifare (sin contacto). Proximidad (ABA y Wiegand).

Biometría facial (externo). Código QR (opcional).

Biometría de dedo.

Características  
específicas o  
equivalentes

\* Huella dactilar. \* Resolución 500 dpi.

\* Tipo de consulta 1:1 y 1:N.

\* FRR (tasa de falsos rechazos) 0,001.

\* FAR (Tasa de falsa aceptación) 0,00001%. \* Número de usuarios 5000.

Opción para instalación de dispositivo de seguridad para la recogida de insignias.

Luces indicadoras Pictograma RGB. Indicador de sonido de audio.

Vigilancia del funcionamiento de WachtDoG. Operación

Modo de funcionamiento en línea y fuera de línea.

Mueble de acero inoxidable. Gabinete delgado.

Solapas de acrílico o policarbonato con personalización del logotipo del SNPP.

Características constructivas o equivalentes	Motor de bajo consumo, con velocidad programable, acelerando o desacelerando la apertura y el cierre de las solapas.
	Armario de acero inoxidable.
	Fuente de alimentación de 90 a 240 VAC.
	Dimensiones de altura X anchura X profundidad (mm) 990 x 180 x 1200.

## ITEM 16 Molinete Tipo 2.

Características Generales o equivalentes	Deberá ser un molinete de paso simple (una sola solapa) fabricado para alto flujo de personas y trabajar en la modalidad de flujo libre, siempre abierto, en caso de intentar pasar sin identificarse, el cierre será automático.
	Pasillo de 50 a 70 cm.
	Deberá funcionar en modalidad unidireccional y bidireccional con la posibilidad de bloquear la solapa.
	Deberá estar incorporado un lector de documentos con función OCR integrado a la base de datos y facial para la validación del acceso y asociación con el rostro.
	Compatible con los principales lectores del mercado. Tarjeta inteligente Proximidad.
	Biometría facial - Biometría digital. Código QR.
	Tiempo de apertura y cierre de 1 seg. Función antideslizamiento.
	Sensores infrarrojos para el control del flujo con aletas giratorias con solapas giratorias.
	Alarma por intento de fraude.
	Control de flujo por visión artificial, que permite bloquear a los usuarios no autorizados.
	Interfaz para la integración con la central de incendios, de alarmas contra incendios.
	Orientación mediante pictogramas luminosos en ambas direcciones. Aviso sonoro de acceso permitido y denegado.
	Configuraciones del corredor.
	Memoria de almacenamiento 8GB.
	Sistema de protección contra la caída de personas. Autonomía en caso de fallo de alimentación 4hs. Permitir la instalación de baterías externas adicionales. Comunicación
	Interfaces ethernet 10/100 Mbps. Tipo de lectores.
Características específicas o equivalentes	Tarjeta inteligente Mifare (sin contacto). Proximidad (ABA y Wiegand).
	Biometría facial (externa). Código QR (opcional).
	Biometría del dedo.
	* Huella dactilar. * Resolución 500 dpi.
	* Tipo de consulta 1:1 y 1: N.
	* FRR (tasa de falsos rechazos) 0,001.

	<p>* FAR (Tasa de falsa aceptación) 0,00001%. * Número de usuarios 5000.</p> <p>Opción para instalación de dispositivo de seguridad para la recogida de insignias.</p> <p>Luces indicadoras Pictograma RGB. Indicador de sonido Audio.</p> <p>Vigilancia del funcionamiento de WachtDoG Operación</p> <p>Modo de funcionamiento en línea y fuera de línea.</p> <p>Mueble de acero inoxidable, gabinete delgado.</p> <p>Solapa de acrílico o policarbonato con personalización del logotipo del SNPP.</p> <p>Motor de bajo consumo, con velocidad programable, acelerar y desacelerar la apertura y el cierre de la solapa.</p> <p>Fuente de alimentación de 90 a 240 VAC.</p> <p>Dimensiones de altura X anchura X profundidad (mm) 770 x 180 x 1200</p>
<b>ITEM 17</b>	<b>Barreras de Acceso Alto Flujo</b>
Características constructivas o equivalentes	<p>Dispositivos de bloqueo vehicular ultra rápido tipo barrera con brazo móvil.</p> <p>Deberá ser exclusivamente destinada al uso para el cual ha sido expresamente diseñado y fabricado. Cualquier uso diferente será considerado peligroso. La barrera automática deberá ser un equipo proyectado para ser utilizada en aparcamientos públicos o privados, o en zonas con mucho tránsito de vehículos.</p> <p>La seguridad del producto y por consiguiente su instalación correcta están supeditadas al respecto de las características técnicas y a las modalidades correctas de instalación con arreglo a la maestría, seguridad y conformidad de uso indicadas expresamente en la documentación técnica del fabricante y las respectivas integraciones en el uso de los componentes de automatización.</p> <p>Estar fabricada en concordancia a la norma de gestión de calidad, ISO 9001 y medioambiente ISO 14001, o similar.</p> <p>Este producto deberá cumplir con las normas vigentes mencionadas en la declaración de conformidad del fabricante.</p> <p>Eléctricas:</p> <p>Alimentación: (V - 50/60 Hz) 120 - 230 AC. Alimentación motora: (V) 24 DC. Absorción: (A) 15 máx.</p> <p>Potencia: (W) 300. Funcionamiento Par (Nm) :200.</p> <p>Tiempo de apertura: a 90° (s) 0,9 ultra rápido. Intermitencia/Funcionamiento: SERVICIO INTENSIVO. Temperatura de funcionamiento: (°C) -20 ÷ +55.</p> <p>Relación de reducción :(i) 1/202. Clase de aislamiento: I.</p> <p>La Central de mando de la barrera. Funciones mínimas necesarias.</p> <p>Función stop total (1-2).</p> <p>Función asociada con la entrada CX. Función asociada con la entrada CY. Función prueba de seguridad.</p> <p>Función acción mantenida. Modalidad de mando en 2-7.</p> <p>Función detección obstáculo con motor parado. Función luz testigo.</p>
Características Generales o equivalentes	

Características específicas o equivalentes

Función de parpadeo del cordón luminoso. Tiempo cierre automático.

Tiempo parpadeo previo. Tiempo de funcionamiento.

Regulación de la velocidad en apertura.

Regulación de la velocidad en cierre.

Regulación de la velocidad de ralentización en apertura. Regulación de la velocidad de ralentización en cierre.

Regulación de la velocidad de calibración. Sensibilidad durante el movimiento.

Sensibilidad durante la ralentización.

Regulación del punto inicial de ralentización en apertura. Regulación del punto inicial de ralentización en cierre.

Tipo de mando que asociar con el usuario mediante mando radio. Borrado de un usuario.

Borrar todos los usuarios. Prueba del motor.

Calibración de la carrera. Reseteo parámetros de fábrica.

Conteo del número de maniobras.

Ajuste de sensibilidad de los sensores por inducción de piso. Configuración del tipo de mástil.

La comunicación de la central de mando integradas a la barrera deberá ser directa con el bus de datos en full dúplex a los DISPOSITIVOS DE CONTROL DE ACCESO del ítem 18 (Control de Acceso IP Multi Tecnología), que a su vez se comunicaran por IP con el software control de acceso y credenciales con gestión integrada del ítem 14 (Sistema de Control de Acceso).

La Barrera deberá estar fabricada de acero galvanizado con pintura epoxi. Brazo de aluminio de 4 a 6 metros.

Peso aproximado 50 kg. Grado de protección: (IP) 54.

Apoyo fijo para el brazo: parte del kit 1.3 mts.

Características constructivas o equivalentes

Si los cables tienen una longitud distinta con respecto a la indicada por el fabricante, hay que determinar la sección de los cables con arreglo a la absorción efectiva de los dispositivos conectados y según lo establecido por la normativa PY. NP 2 028 13.

Instalación.

Preparar un encofrado de dimensiones mínimas 36x50x50cm para la base de la barrera.

Poner una rejilla de hierro dentro del encofrado para armar el cemento. Acoplar las cuatro grapas de anclaje a la placa de fijación.

#### ITEM 18

#### Control de Acceso IP Multi Tecnología.

##### DISPOSITIVOS DE CONTROL DE ACCESO

Características de los equipos de control de acceso IP Multi Tecnología:

Los dispositivos deben tener características de tecnología biométrica añadidas a los terminales.

El Gabinete debe estar protegido contra el acceso indebido, el vandalismo y estar provisto de tornillos de fijación resistentes. También debe contar con un sensor de apertura del armario, que debe generar un código de alarma



Características  
Generales o  
equivalentes

cuando se produzca un intento de apertura indebida de acceso interno al armario del equipo, no autorizado previamente.

El terminal debe tener la opción de instalarse en un armario de plástico u otro material con un simple cambio de caja, sin necesidad de cambiar los módulos internos.

El terminal dispositivo de datos también debe tener una aplicación para los sistemas de control de frecuencia, haciendo que los datos recolectados estén disponibles para las áreas de RRHH, como la hora de entrada, salida, almuerzo, horas extras, etc.

Su electrónica debe poder almacenar el software de su aplicación de forma segura e intacta, es decir, sin riesgo de perder información, descargar nuevas versiones o actualizaciones de su aplicación, y debe ser posible actualizarla a distancia.

Debe tener memoria para almacenar el registro de operaciones y/o transacciones gestionando los datos de forma inteligente, precisamente porque tiene toda la inteligencia integrada en un único armario. Toda la información que se almacenará en el equipo, debe hacerse de forma segura contra la pérdida por corte de energía, almacenando al menos 40.000 registros y las transferencias realizadas con la velocidad y la misma seguridad.

En la composición de la memoria del equipo, debe ser posible almacenar los registros de la bitácora de operaciones (40.000 registros) como se ha solicitado anteriormente, así como una copia de seguridad en caso de corte de energía y/o comunicación fuera de línea. Cuando se restablezca la comunicación, es decir, de fuera de línea a en línea, los registros deben ser enviados automáticamente a la base de datos sin ninguna intervención humana.

La recogida de información puede realizarse en línea o fuera de línea, según la mejor arquitectura definida para cada situación.

El dispositivo de datos debe disponer de un circuito de reloj preciso, con una alta fiabilidad en cuanto al registro de tiempos o épocas, con la función de eliminar los errores, los inconvenientes y la necesidad de ajustes manuales causados por problemas con la hora mostrada por el usuario y la hora realmente marcada en el software.

El sistema debe adaptarse a situaciones críticas de trabajo, es decir, lugares con temperaturas fluctuantes, humedad extrema, ambientes sujetos a condensación, es decir, donde se requieren soluciones robustas que puedan servir a la SNPP en un ambiente normal con condiciones normales de temperatura y presión o incluso en situaciones inesperadas o lugares con condiciones ambientales extremas.

El equipo debe poder configurarse para su instalación local o remota, con actualizaciones de firmware y aplicaciones.

El dispositivo debe poder instalarse en techos u otros lugares protegidos, dejando sólo visible el módulo de la interfaz de usuario, es decir, el módulo lector de tarjetas y el módulo biométrico, en su caso.

Debe poder interactuar con todos los tipos de soportes de tarjetas disponibles en el mercado para este tipo de aplicaciones, es decir, tarjetas de código de barras, tarjetas magnéticas, tarjetas inteligentes con o sin contacto, tarjetas de proximidad de 125 KHz, lectores biométricos y teclados, entre otros.

El equipo debe tener una interfaz RS 232 y una interfaz TCP-IP nativa, es decir, un puerto Ethernet directamente en la placa del equipo.

El equipo debe ser reversible, es decir, debe ser posible cambiar la placa de interfaz y el software para tener comunicación RS 485 o TCP-IP, para los casos en que la red TCP-IP no esté disponible.

El sistema de alimentación del dispositivo debe tener como objetivo proteger al usuario de los riesgos causados por los cortocircuitos, las

sobrecargas en la fuente o similares y también facilitando las características de instalación de las fuentes de alimentación (red y no ruptura). Por lo tanto, la fuente de alimentación debe ser externa a la unidad de dispositivo es separada de la unidad de control y procesamiento, precisamente para cumplir con los últimos requisitos y conceptos de seguridad a nivel mundial. La fuente de alimentación debe contar con medios de señalización visual que permitan identificar la fuente de alimentación activa, tanto en modo de CA como de CC. La fuente de alimentación debe contener una unidad sin ruptura con una autonomía mínima de 04 (cuatro) horas en funcionamiento continuo.

La fuente de alimentación debe estar en el rango completo de 90 ~ 240 VAC, entrada auxiliar de 12 VDC, entrada de batería de 12 VDC, y cuando haya un corte de energía el equipo funcionará con alimentación externa a través del módulo de fuente.

Datos técnicos

Gabinete: Acero inoxidable 304.

Visualización: LCD 2 x 16 con retroiluminación de alta intensidad con ajuste de contraste.

Teclado: Alta resistencia 12 teclas para la entrada de datos, selección de funciones, contraseñas, opción de configuración local para el administrador.

Pictograma: El equipo dispondrá de señalización visual mediante pictogramas orientativos que indiquen al usuario que su fichaje ha sido aceptado o no y los pictogramas tendrán al menos dos colores diferentes para indicar la actuación positiva y negativa, es decir, para la validación o rechazo de los fichajes o en su caso los eventos de acceso. De esta especificación, el empresario espera una solución de pictograma y no sólo una señalización mediante leds bicolor o incluso dos leds.

Estará equipado con dos lectores de tarjetas inteligentes mifare de 1 KB ISO 14443 tipo "A" y un lector biométrico. El lector biométrico será óptico y leerá en modo 1:1 y 1:N, según se seleccione por software y el tiempo de lectura en 1:1 será como máximo de 1s y en 1:N de 3s.

Comunicación: TCP-IP IPv6.

El equipo debe tener una memoria RAM y Flash de 512 Kb.

Debe estar equipado con un sensor biométrico con una resolución mínima de 500 ppp y un índice de falsa aceptación del 0,00001% y un índice de falso rechazo del 0,001%, permitiendo 9000 usuarios (sólo el modelo con biometría).

También debe ser capaz de almacenar datos durante un periodo superior a 120 horas.

Alimentación: Fuente de rango completo 90-240 Vac, 50-60 Hz - (POE). Consumo: Aproximadamente 10 VA.

Auxiliar: 12 Vdc 1 A.

Debe tener zumbador interno con ajuste.

Baterías: No hay kit de baterías de ruptura que permita el funcionamiento y la comunicación sin alimentación de la red principal Kit integrado en el equipo. No está permitido utilizarlo por separado.

Memoria protegida por super cápsula. Funcionamiento.

Puede funcionar on-line, off-line, Stand-alone o Cliente x Servidor.

Debe tener al menos 6 interfaces de E/S para comunicar y activar dispositivos y otros módulos mediante contacto seco, así como para recibir

información de los sensores mediante contacto seco y gestionar cada una de estas informaciones mediante el envío del software de gestión de accesos y seguridad.

Características  
específicas o  
equivalentes

Debe disponer de recursos de puesta en marcha a distancia con decisiones programadas en el propio controlador y/o recibir instrucciones de puesta en marcha desde el software de gestión de accesos para la eventual liberación/bloqueo de una puerta, portón del torniquete, etc. y recursos para la automatización como el encendido de una bombilla, aire acondicionado, activación de sensores, etc.

Características operativas

La placa lógica o placa electrónica principal del equipo, además de sus funciones de seguridad y acceso a los datos, debe albergar el procesador, las memorias, el circuito de reloj en tiempo real y todos los componentes del dispositivo, excepto la fuente de alimentación.

Cuando el empleado activa el lector de tarjetas, el dispositivo de datos debe verificar si es la tarjeta válida para ese sistema y proceder a la autorización, es decir, registra o no la hora de entrada/salida/comida del empleado, etc. mostrando en el pictograma de leds bicolor (verde/rojo) la señalización correspondiente como sigue:

Será imprescindible que el dispositivo tenga la funcionalidad de leer y escribir tarjetas inteligentes, operando en modo "on line" y "off line" de forma transparente para el usuario, siendo entonces necesario que las condiciones y reglas de cada empleado queden registradas en la memoria de la tarjeta.

Por lo tanto, en la acción de lectura del dispositivo también debe escribir en las tarjetas inteligentes sin contacto.

La señalización de los pictogramas debe cumplir, como mínimo, la norma que se indica a continuación.

Verde: Aceptado, tarjeta válida y datos registrados.

Rojo: Rechazada, tarjeta no válida para el sistema, o bloqueada por el administrador por razones predefinidas a través del software.

El administrador del sistema puede, si es necesario y conveniente, acceder a los parámetros de configuración de los dispositivos de datos a través de la tarjeta de administrador, lo que permite cambiar las condiciones de funcionamiento del equipo; sin embargo, estos cambios se pueden realizar a través del software de gestión suministrado con la solución.

Los dispositivos deben comunicarse en protocolo TCP-IP como se ha especificado anteriormente y deben ser compatibles con la base de datos ORACLE/SQL-SERVER. No se aceptarán soluciones que no sean compatibles con la plataforma mencionada, por lo que la SNPP exige en este pliego que sean compatibles con la plataforma de base de datos, en línea.

Comunicación

El dispositivo de datos estará equipado con comunicación TCP-IP, siendo aceptado sólo este tipo de interfaz nativa, pero también será posible, con el intercambio del módulo de interfaz, operar con red serial tipo RS 485 y también GPRS/3G/4G.

Como la comunicación estándar será del tipo TCP-IP, el dispositivo de esta manera equipado con una interfaz estándar Ethernet nativa, se debe considerar una comunicación half/full-duplex 10 BASE-T (10/100 Mbits/s), con una dirección de red MAC-ADDRESS fija guardada de fábrica en el dispositivo, garantizando una vez más la accesibilidad segura al equipo.

En modelos con comunicación GPRS debe estar preparada para cualquier operador del mercado. El dispositivo de datos debe tener su propia "cuna" en su placa electrónica interna donde se debe insertar el chip del operador, y no se aceptan soluciones con módems GPRS externos.

Cuando el proyecto aborda el controlador de la puerta basado únicamente en un lector de tarjetas inteligentes sin contacto, la solución se refiere a este mismo elemento, pero sin las características de cumplir las especificaciones biométricas.

Los lectores y controladores de los molinetes deben ser compatibles con el sistema de control de acceso y deben contar con la homologación de Anatel o similar.

Características constructivas o equivalentes	<p>El dispositivo debe tener una construcción tecnológica tal que tenga inteligencia distribuida, permitiendo la interconexión de los terminales del dispositivo en una sola red de equipos con comunicación en línea tanto con interfaces tipo TCP-IP como RS 485.</p> <p>Debe tener un gabinete de acero inoxidable 304, fabricado de acuerdo con la norma ABNT o similar, con clase de seguridad eléctrica y mecánica adecuada a la aplicación.</p>
--	--

#### ITEM 19 Sensor Sísmico IOT

Características Generales o equivalentes	<p>Los dispositivos de rastreo de activo con sensores múltiples.</p> <p>Deberán ser dispositivos pequeños de alta precisión, versátiles y confiables equipados con sensores múltiples que admiten hasta 50 configuraciones, firmware personalizable.</p> <p>Duración de la batería: 10 años *. Número de mensajes: 30.000.</p> <p>Grado de impermeabilidad: IP68. Batería 1500 mAh.</p> <p>Machine learning y mapeo de patrones.</p> <p>Detección de Wifi para seguimiento de ubicación precisa de Wifi. Multizona conmutable.</p>
Características específicas o equivalentes	<p>LED señalizador.</p> <p>Rango de medición de temperatura -40 a 60 ° C / <math>\pm 0,5</math> ° C. Barómetro.</p> <p>Giroscopio. Podómetro. Tiempo preciso. Acelerómetro. Magnetómetro. Luz ambiental. Anti- sabotaje. KEEP_ALIVE.</p> <p>Temperatura de funcionamiento -40 ° C a 60 ° C. Zonas de radio compatibles 1,2,3,4,5,6.</p> <p>Programación en línea, haga clic y seleccione. Lote a través de enlace descendente.</p> <p>Automatización y flujo de trabajo con integración.</p> <p>Firmware personalizable.</p>
Características constructivas o equivalentes	<p>Accesorios para tornillos perforados y bridas de cable de alta resistencia opcionales.</p> <p>Botón físico. Volumen 29 cm<sup>2</sup>.</p> <p>*La cantidad de mensajes y la longevidad de la batería en años están relacionados, considerar mínimo el envío de 2 eventos diarios.</p>

#### ITEM 20 Sensor de Presencia IOT.

Características Generales o equivalentes	<p>Dispositivos de sensor de alarma por presencia. Modos de operación.</p> <p>Detecta multi zonas en espacios internos, detección de intrusión en lugares restringidos.</p> <p>Basado en eventos: Detectar movimiento humano basado en tiempo, número de recuento de humanos.</p> <p>Tipo de sensor: Infra Rojo Pasivo.</p> <p>Temperatura de funcionamiento -20 ° C a 70 ° C. Ángulo de visión: 120°.</p>
Características específicas o equivalentes	<p>Distancia detección: hasta 10 m.</p> <p>Led indicador: aviso de envío de mensaje. Baterías: 3 años**.</p>

Características constructivas o equivalentes	KEEP_ALIVE.
	Agregación de datos: Reduzca el consumo de energía con menos enlaces ascendentes.
	Carcaza: Plástico ABS. Antena: interna.
Características constructivas o equivalentes	Tamaño aproximado: 32g / 88 (L) x 30 x 20 (H) mm.
	**La cantidad de mensajes y la longevidad de la batería en años están relacionados, considerar mínimo el envío de 10.000 mensajes.
ITEM 21	<b>Plataforma de Gestión de Alarmas Integrada al VMS y conectividad IOT hasta 20 dispositivos por 24 meses.</b>
Características Generales o equivalentes	Sistema de alarmas de alta seguridad y rastreo de activos en tiempo real conectados al sistema de monitoreo remoto integrado al VMS.
	La tecnología
	La tecnología de comunicación deberá ser en una red de área amplia de baja potencia inmune al jamming (bloquear e interferir en diferentes tipos de señales de comunicación).
	Seguridad de la RED de comunicación:
	El ecosistema de red deberá integrar la seguridad de forma predeterminada:
	Autenticación + integridad + anti- reproducción en mensajes propagados en la red.
	Criptografía basada en AES sin transmisión de clave OTA.
	Cifrado de carga útil como opción para garantizar la confidencialidad de los datos.
	Aislamiento de cada parte de la red. Inmune al jammer.
	El oferente deberá presentar en su oferta la tecnología de red que utilizará, cobertura y seguridad.
Características específicas o equivalentes	Dispositivos conectados a la RED
	Dispositivos de rastreo de activos en tiempo real contarán con información adicional de posición de los puntos de acceso Wi-Fi®.
	Dispositivos sensores de movimiento por presencia.
	Todos los dispositivos deberán contar con batería de larga duración, detectar eventos específicos de acuerdo con las especificaciones técnicas de cada elemento ofertado.
	El funcionamiento:
	El sistema deberá mantener seguro los activos asignados proporcionando un dato de geolocalización en tiempo real, detección de golpes bruscos, intentos de manipulación, explosivos, temperatura, salida del área de influencia, dispositivo presente/ausente.
	Deberá enviar al VMS todos los eventos y alarmas preconfigurados, con la información de posicionamiento, mapas, imagen de las cámaras asignadas al dispositivo u evento para la toma de decisiones.
	Eventos mínimos a ser enviados al centro de Monitoreo. El nombre del dispositivo con su Geolocalización.
	Eventos generados. Tipo de sensor.

	Nivel de batería. KEEP_ALIVE.
	Histórico de datos de mensajes y eventos de los dispositivos. Horario de última actividad.
	Indicación del recorrido (en caso del activo haya sido movido del lugar o al ambiente externo).
Características constructivas o equivalentes	Todo el sistema tendrá que funcionar en modalidad M2M (maquina a máquina o sea del dispositivo al VMS centralizado) enviando la información de cada dispositivo hasta la central de monitoreo.
<b>ITEM 22</b>	<b>Servicio de Integración de Sistema de Control Inteligente</b>
	Magnitud del Sistema Integral de Control Inteligente estará compuesto por hardware, software, infraestructura de red de datos y ciberseguridad IOT y sistema de misión crítica (Failover).
	Casa Central, centro operativo y monitoreo.
	Todo el sistema de video vigilancia, sus integraciones y controles centralizados de gestión de seguridad con las siguientes características y equipos:
Características Generales o equivalentes	<p>Todos los equipos deben contar con tecnología IP nativa, una red datos exclusiva y administrable, estar integrados nativos, vía API o Plataforma LOW-CODE y con comunicación y comandos directa por software y todas las instrucciones y flujos de trabajos deben ser recibidos y enviados directos de la plataforma de gestión de vigilancia unificada, no serán aceptados equipos adaptados o placas de contacto seco para esta finalidad cada equipo suministrado ya deberá contar con sus contactos de I/O para la gestión de sensores comandos y bloqueos necesarios en las respectivas integraciones.</p> <p>Funcionamiento</p> <p>Control de acceso por molinetes inteligentes de alto flujo de pase libre, deberá actuar siempre abierto para la rápida autenticación de los usuarios.</p> <p>Deberá contar con lector para autenticación , lo requerido para el registro de datos de los usuarios, se grabará en base de datos, por validación y asociación con el rostro del usuario. Esta función está asociada al método KYC (Know Your Customer) cuyo proceso fundamental define y permite las relaciones empresas/usuarios y que deberán estar integrados con el Sistema de Gestión Empresarial (ERP) (Sistemas, aplicaciones y productos para el procesamiento de datos.) del SNPP por API.</p> <p>Una vez que el método KYC sea validado, el control de acceso y seguimiento de los usuarios será por reconocimiento e identificación facial en todas las cámaras disponibles conectadas en el sistema.</p> <p>Conectividad:</p> <p>La infraestructura de red de datos deberá ser utilizada en su totalidad y actualizada para soportar los nuevos equipos, ancho de banda, seguridad IOT y el sistema de Failover (Conmutación por falla) configurado como misión crítica.</p> <p>Failover (Conmutación por falla) configurado de misión crítica -Replicación Remota en Tiempo Real.</p> <p>Considerando los factores externos de conectividad IoT, la modalidad y la ciberseguridad, el oferente deberá prever en la oferta, para la seguridad de los equipos en la solución Failover,y seguridad de la red</p> <p>Estas configuraciones y medidas de seguridad son las mínimas exigidas e indispensables para:</p> <p>Evitar que el personal no autorizado se infiltre en la red del sistema de seguridad; la asignación de puertos y el direccionamiento ofrece la posibilidad de limitar el rango de direcciones para cada área funcional.</p> <p>La administración de la red se vuelve una tarea más sencilla al poder controlar (habilitar o denegar) los servicios de red:</p>

Se reducen los dominios de broadcast, es decir, se limita el número de dispositivos conectados de acuerdo con el direccionamiento dinámico establecido.

Se evita la pérdida de información ya que la responsabilidad recae en los usuarios asignados a cada red virtual.

Se pueden compartir recursos de forma responsable asignados por área como pueden ser: Impresoras, servidores, equipos IoT etc.

Deberá justificar con su oferta cómo será la conexión, los equipos a ser utilizados, sistema de ciberseguridad, elementos físicos de red, fibra óptica (Intranet), enlaces y monitoreo, (arquitectura, diagrama, equipos, firewalls, proveedor del servicio, etc.) todo representado en el esquema de topología física de la RED que deberá acompañar a la oferta en formato tipo vision.

Observación:

Tener en cuenta al preparar la Oferta:

La configuración de Failover deberán estar disponibles mínimo por el periodo de 24 meses.

Considerar todos los costos necesarios al preparar la oferta. Infraestructura

El sistema de misión crítica Failover deberá contar con un servidor físico con la capacidad, licencias y recursos asignado en un DATACENTER que mínimo cumpla los estándares TIER3 y la norma ISO 27000 de seguridad de la información (con la respectiva declaración que el DC cumple con las normas).

Toda la implantación deberá contar con soporte local de rápida respuesta y asesoramiento al servicio de su actividad: atención 24 x 7 días a la semana durante el termino de 24 meses, sin costo adicional, todo lo cual deberá estar contemplado en la oferta. Además, justificará en su oferta la manera en que estará disponible el servicio de respuesta rápida.

Deberá tener en cuenta todos los costos necesarios al preparar la oferta en función de la solución propuesta.

Pasados los 24 meses del servicio de misión crítica incluido en la oferta, el sistema failover deberá seguir funcionando por un periodo de 2 meses más acompañado de todas las configuraciones del sistema de misión crítica ciberseguridad y conectividad IoT, durante este periodo el SNPP decidirá la renovación o no, del sistema de misión crítica.

Deberá contar con un técnico certificado en IT service managent (ITSM) Gestión de Servicios de Tecnología de Información.

2. Garantía integral en modalidad ILIMITADA de 2 años, otros datos requeridos y garantizados Todos los componentes del sistema deberán contar con garantía ilimitada de 2 años.

El proveedor deberá garantizar una garantía total ilimitada por un periodo mínimo de 24 meses de la solución ofertada, deberá contar con repuestos componentes del sistema disponible para reposición en un plazo no mayor a 48 horas desde el reclamo formal por mail o plataforma de reclamos.

La Garantía, está comprendida para todos los equipos que presenten defectos por cualquier desperfecto que ocurra en la instalación/montaje, independiente de la causa de manera ilimitada.

El proveedor deberá efectuar el cambio y pruebas del equipo en un plazo de 72 hs. posterior al reclamo correspondiente del SNPP.

En caso que se compruebe vandalismo o robo de equipos, el proveedor deberá efectuar el referido informe al Administrador del Contrato, a los efectos de establecer los costos de reposición de los equipos y su montaje correspondiente.

3. Sistema de vídeo vigilancia IP existente

Características  
Específicas o  
Equivalente

El sistema de video vigilancia existente en la, así como sus cámaras IP deberán ser migradas a la nueva plataforma de video vigilancia en su totalidad con las prestaciones, seguridad y funciones disponibles en cada dispositivo con su respectivo mantenimiento.

Prever en su totalidad el mantenimiento correctivo del sistema de videovigilancia del SNPP- Sede Central-Asunción con sus componentes.

El Servicio de mantenimiento contemplará: si necesario actualizar el software de gestión de video, y reemplazar las cámaras que actualmente presentan fallas y no se encuentran operativas (25, ya están en la lista de cámaras), así también, es necesario reemplazar 3 (tres) switches de comunicación Poe para la conectividad de las mismas, prever los cambios en caso

que también se detecten fallas en el cableado actual y, por tanto, necesiten ser modificados.

la Solución de videovigilancia existente a ser actualizada es un sistema Intelligent Security Systems (ISS), esta debe estar operativa y funcionando hasta la migración definitiva.

#### 4. Plataforma Abierta de video vigilancia basada en servidor dedicados escalable.

La nueva arquitectura de software de gestión de video integral deberá soportar todas las cámaras, dispositivos, componentes del proyecto y ser escalable para el crecimiento futuro.

La capacidad de grabación deberá ser de 60 días en la plataforma centralizada, considerando un mínimo de 100 cámaras activas y configuradas con estos parámetros:

- Sistema de discos -mínimo RAID 5.
- Detección de movimiento: Server-Side.
- Número de clientes remotos: 10.
- Clientes en transmisión: 16.
- Cámaras: 400 activas.
- Ancho de banda: 567 Mbps.
- Resolución: 2600x1950 (5 MP).
- Compresión de video: H.264-MediumQual.
- Flujo de bits: Tasa de bits variable (VBR).
- Tasa de bits (kb/s): 3097.
- Cuadros por segundo: 12 promedio.
- Periodo de grabación: 60 días.
- Escena: Moderate-30.
- % Diario de grabación: 40.
- Ancho de banda (Mbps): 567 Mbps.
- Storage: dimensionar.



Presentar cálculo técnico que justifique el hardware dimensionado, cantidad y modelo de discos duros presentados, deberá tener en cuenta el almacenamiento unificado y centralizado, rendimiento necesario, velocidad, tiempo de búsqueda de archivos, (no serán aceptados discos duros que no sean específicos para video vigilancia en función de la cantidad de cámaras y volumen de grabación) conforme a requisitos de exigencia y prestaciones de la plataforma ofertada en los ítems 10 y 11 (Licencias Tipo 1: Servidor Remoto,

Licencias Tipo 4: Servidor Centralizado). Los discos deben ser incluidos en el hardware y certificados por el fabricante y la plataforma VMS.

## 5. Distribución de Cámaras SNPP sede San Lorenzo

Ubicación	Subtotal Cámaras	Detalle Cámaras	Tipo Instalación	Planta
<b>Pabellón 1</b>	<b>2</b>			
Esquina Izquierda del Galpón radiando hacia la calle Destacamento Cazal	1		Perimetral	Interiores
A 20 metros del Galpón del lado derecho radiando hacia calle Destacamento Cazal	1		Perimetral	Exteriores
Pasillo entre salones 1201 y 1109 radiando hacia el corredor dirección salón 1207	1		Interior	planta alta
Salida de baño de hombres al lado del salón 1106	1		interior	planta baja
<b>Pabellon 2</b>	<b>4</b>			
Esquina lado derecho radiando hacia Viena	1		Perimetral	exteriores

Esquina lado izquierdo radiando hacia calle	1	Perimetral	exteriores
---	---	------------	------------

destacamento  
Cazal

Esquina lado izquierdo radiando hacia Galpón del	1	Perimetral	exteriores
--	---	------------	------------

Pabellón 3

Esquina lado derecho radiando entre Galpón	1	Perimetral	exteriores
--	---	------------	------------

pabellón 1 y  
calle Viena

**Pabellón 2      4**

pasillo radiando hacia salón 2204	1	Interior	Planta alta
-----------------------------------	---	----------	-------------

Pasillo a nivel del salón 2204 radiando hacia el salón	1	Interior	Planta alta
--	---	----------	-------------

2203

pasillo nivel entre 2203 y 2202 radiando hacia salón	1	Interior	Planta alta
--	---	----------	-------------

2201

interna en salón 2102	1	Interior	Planta baja
-----------------------	---	----------	-------------

**Pabellón 3      3**

A definir con el contratista	3	Perimetral	Exterior
------------------------------	---	------------	----------

**Pabellón 3      6**

Salón 3201 centro radiando hacia calle Viena	1	Interior	Planta alta
--	---	----------	-------------

Pasillo esquina salón 3202 a nivel de escaleras	1	Interior	Planta alta
radiando hacia destacamento casal			
Salón 3101 radiando hacia calle Viena	1	Interior	Planta baja
Taller de Heladeras radiando entre Pabellón 2 y	1	Interior	Planta Baja
Pabellón 5			
Perimetral Lado Izquierdo a nivel Taller de Soldadura	1	Perimetral	Planta baja
Radiando hacia Viena			
A definir con el contratista	1	Perimetral	Exterior

#### **Pabellón 4 4**

Desde el Archivo hacia las Escaleras dirección		Interior	Planta alta
Limpieza	1		
Puerta de Salón 4202 radiando hacia escaleras	1	Interior	Planta alta
Pasillo esquina del 4105 hacia dirección del corredor	1	Interior	Planta baja
entre 4103 y 4102			
Esquina del Salón Laboratorio Mantenimiento	1	Interior	Planta baja
Industrial			

#### **Pabellón 5 3**

Salón de Auditorio radiando hacia Destacamento	1	Interiores	Planta alta
Cazal			
Salón 5201 Radiando hacia calle destacamento Cazal	1	Interiores	Planta alta
Salón 5202 radiando hacia la calle destacamento Cazal	1	Interiores	Planta alta
<b>Pabellón 5</b>	<b>1</b>		
A definir con el contratista	1	Perimetral	Exterior
<b>Pabellón Admin</b>	<b>1</b>		
A definir con el contratista	1	Perimetral	Interiores
<b>Pabellón Admin</b>	<b>3</b>		
Informaciones Radiando hacia secretaria de	1	Interiores	Planta baja
Academia Técnica			
Esquina de Seguridad y Vigilancia radiando hacia	1	Interiores	Planta alta
Deposito			
Dirección radiando hacia Dpto. Académico	1	Interiores	Planta alta

#### 6 Tiempo de Plazo del Proyecto

El proyecto tendrá 30 días corridos desde su planificación, ejecución e implementación.

#### 7 Materiales

Los suministros deberán incluir, sin estar limitados, a las siguientes partidas:

Todos los equipos, dispositivos y elementos necesarios, de manera que permitan el funcionamiento del Sistema integrado de Video Vigilancia IP.

El contratista prever todos los equipos y accesorios para el completo funcionamiento del sistema Como ser:

Los Racks, Ups 1KVA, patcheras, fichas RJ45 CAT6 Switch Core, Switch PoE o no cuando necesarios en cada punto o nudo con su respectivo número de puertos, cableado de datos UTP CAT. 6 que cumpla la norma EIA/TIA 568-C., así como el de alimentación, cajas de paso, canalizaciones y ductos adecuadas a cada punto a ser instalado, protecciones contra descargas para por cada elemento del sistema y los mismos deberán estar conectada a tierra, la interconexión de los Switches será a través de fibra óptica

proveerá dos ejemplares de un Manual de Operación y Mantenimiento del Sistema de Video Vigilancia.

#### 8 Mano de Obra:

El oferente deberá de prever en su oferta la mano de obra para la puesta en marcha de todo el sistema.

Deben considerar para el diseño, implementación y puesta en marcha de la plataforma de Video Seguridad Integrada. Deberá prever todos los trabajos necesarios, de manera que permitan el funcionamiento del Sistema de Video Vigilancia IP.

#### 9 INSPECCIONES Y PRUEBAS

La Contratante por su administrador de contrato será la máxima autoridad para verificar que la instalación se efectué de acuerdo a estas especificaciones.

Ninguna comunicación verbal tendrá validez para justificar cambios en el proyecto.

#### 10 Entrenamiento

El entrenamiento de uso, gestión y administración de la nueva solución de gestión de video deberá ser de un mínimo de 100 horas para el personal designado por el Administrador del Contrato. Las horas de entrenamiento serán computadas una vez que el sistema este instalado e integrado en su totalidad.

#### 11 Manuales y Licencias

El Contratista deberá entregar manuales completos y adecuados de la operación. Estos manuales deberán ser en español y deben contener una descripción de funcionamiento y operación individual e integral, y no limitarse a la entrega de catálogos y especificaciones del fabricante, los cuales también deben ser entregados, pudiendo ser los documentos originales del proveedor. El proveedor deberá entregar las licencias originales de todos los softwares instalados.

#### 12 Sala de Control, Muebles y Accesorios

Sera suministrada por la Sede del SNPP San Lorenzo, en su totalidad. El cual quedara en custodia el servidore de Video remoto y todos sus accesorios.

#### 13 Generalidades

El alcance del proyecto para los sistemas antes mencionados considera el suministro, montaje, pruebas, puesta en servicio.

Es de responsabilidad del oferente reconocer los puntos de instalación e identificar los materiales y accesorios necesarios para la correcta instalación y funcionamiento de estos equipos.

Los trabajos deben contemplar el desarrollo complementario de la Ingeniería necesaria para el montaje, incluido planos, cortes, elevaciones, detalles, suministro de materiales y equipos, mano de obra calificada y especializada, y todo lo que resulte necesario para la provisión, montaje y puesta en servicio del Sistema de Video Seguridad Integrado.

Durante todo el curso de los trabajos el Contratista deberá mantener una persona en el lugar de la obra, quien estará en condiciones de suministrar la información relativa a los trabajos y recibir las indicaciones del Contratante.

La omisión o no inclusión de algún ítem necesario y esencial para el buen funcionamiento de la solución no exime al Contratista de la responsabilidad de presentar una solución de conjunto que permita el funcionamiento integral de la misma, con desempeño satisfactorio y un máximo nivel de confianza.

Quedará a cargo del oferente todos los trabajos para el montaje y puesta en funcionamiento del sistema, por lo que para la cotización deberá tener en cuenta los siguientes ítems:

- \* Los equipos y componentes con las características básicas obligatorias, conforme a lo especificado y las cantidades definidas
- \* Accesorios para la instalación de todo el sistema (conductores, ductos, soportes, etc.).
- \* Instalación, configuración y puesta en servicio de todo el Sistema de Video Seguridad Integrado.
- \* Tendido de cableado e interconexión entre los Switches
- \* Licencia legal del software proveído.
- \* Soporte técnico tanto de hardware como de software

**SE PRORROGAN LAS FECHAS DE CONSULTA, RESPUESTA, INICIO Y FIN DE PROPUESTA, ETAPA COMPETITIVA, ENTREGA Y APERTURA DE SOBRES DE OFERTAS PARA EL PRESENTE LLAMADO, QUEDANDO CONFORME A LO INDICADO EN EL SICP.**

**TODAS LAS DEMÁS CONDICIONES ESTABLECIDAS EN EL PLIEGO DE BASES Y CONDICIONES Y SUS ADENDAS PERMANECEN VIGENTES, INVARIABLES E INALTERABLES.**

Se detectaron modificaciones en las siguientes cláusulas:

Sección: Suministros requeridos - especificaciones técnicas

- Detalle de los productos con las respectivas especificaciones técnicas

Se puede realizar una comparación de esta versión del pliego con la versión anterior en el siguiente enlace:

<https://www.contrataciones.gov.py/licitaciones/convocatoria/392088-adquisicion-e-instalacion-sistema-cctv-snpp-1/pliego/10/diferencias/9.html?seccion=adenda>

La adenda es el documento emitido por la convocante, mediante la cual se modifican aspectos establecidos en la convocatoria y/o en las bases de la licitación y/o en los contratos suscriptos. La adenda será considerada parte integrante del documento cuyo contenido modifique.

# DATOS DE LA LICITACIÓN

Los Datos de la Licitación constituye la información proporcionada por la convocante para establecer las condiciones a considerar del proceso particular, y que sirvan de base para la elaboración de las ofertas por parte de los potenciales oferentes.

## Contratación Pública Sostenibles - CPS

Las compras públicas juegan un papel fundamental en el desarrollo sostenible, así como en la promoción de estilos de vida sostenibles.

El Estado, por medio de las actividades de compra de bienes y servicios sostenibles, busca incentivar la generación de nuevos emprendimientos, modelos de negocios innovadores y el consumo sostenible. La introducción de criterios y especificaciones técnicas con consideraciones sociales, ambientales y económicas tiene como fin contribuir con el Desarrollo Sostenible en sus tres dimensiones.

El símbolo “CPS” en este pliego de bases y condiciones, es utilizado para indicar criterios o especificaciones sostenibles.

Criterios sociales y económicos:

- Los oferentes deberán indicar bajo declaración jurada el pago del salario mínimo a sus colaboradores, además de garantizar la no contratación de menores.
- Los oferentes deberán dar cumplimiento a las disposiciones legales vigentes asegurando a los trabajadores dependientes condiciones de trabajo dignas y justas en lo referente al salario, cargas sociales, provisión de uniformes, provisión de equipos de protección individual, bonificación familiar, jornada laboral, asegurar condiciones especiales a trabajadores expuestos a trabajos insalubres y peligrosos, remuneración por jornada nocturna.
- Las deducciones al salario, anticipos y préstamos a los trabajadores no podrán exceder los límites legales. Los términos y condiciones relacionados a los mismos deberán comunicarse de manera clara, para que los trabajadores los entiendan.
- Los oferentes adjudicados deberán fomentar en la medida de lo posible, la creación de empleo local y el uso de suministros locales.

Criterios ambientales:

- El oferente adjudicado deberá utilizar en la medida de lo posible, insumos cuyo embalaje pueda ser reutilizado o reciclado.
- El oferente adjudicado deberá cumplir con los lineamientos ambientales, incluidos en el ordenamiento jurídico o dictado por la institución, tales como: cooperación en acciones de recolección, separación de residuos sólidos, disposición adecuada de los residuos, participación del personal en actividades de capacitación impartidas por la institución, entre otros.
- El oferente adjudicado deberá asegurar que todos los residuos generados por sus actividades sean adecuadamente gestionados (identificados, segregados y destinados) y buscar su reducción o eliminación en la fuente, por medio de prácticas como la modificación de los procesos de producción, manutención y de las instalaciones utilizadas, además de la sustitución, conservación, reciclaje o reutilización de materiales.

Conducta empresarial responsable:

Los oferentes deberán observar los más altos niveles de integridad, así como altos estándares de conducta de negocios, ya sea durante el procedimiento de licitación o la ejecución de un contrato. Asimismo, se comprometen a:

- No ofrecer, prometer, dar ni solicitar, directa o indirectamente, pagos ilícitos u otras ventajas indebidas para obtener o conservar un contrato u otra ventaja ilegítima.
- No ofrecer, prometer o conceder ventajas indebidas, pecuniarias o de otro tipo a funcionarios públicos. Tampoco deberán solicitar, recibir o aceptar ventajas indebidas, pecuniarias o de otro tipo, de funcionarios públicos o empleados de sus socios comerciales.
- Introducir políticas y programas contra la corrupción e implementarlas dentro de sus operaciones.
- Garantizar que todos los recursos a ser empleados en la ejecución de un contrato público sean de origen lícito.
- Garantizar que los fondos obtenidos de una licitación pública no sean destinados a fines ilícitos.

## Difusión de los documentos de la licitación

Todos los datos y documentos de esta licitación deben ser obtenidos directamente del Sistema de Información de Contrataciones Públicas (SICP). Es responsabilidad del oferente examinar todos los documentos y la información de la licitación que obren en el mismo.

## Aclaración de los documentos de la licitación

Todo oferente potencial que necesite alguna aclaración del pliego de bases y condiciones podrá solicitarla a la convocante. El medio por el cual se recibirán las consultas es el Sistema de Información de Contrataciones Públicas (SICP), y/o si es el caso, en la Junta de Aclaraciones que se realice en la fecha, hora y dirección indicados por la convocante.

La convocante responderá por escrito a toda solicitud de aclaración del pliego de bases y condiciones que reciba dentro del plazo establecido o que se derive de la Junta de Aclaraciones.

La convocante publicará una copia de su respuesta, incluida una explicación de la consulta, pero sin identificar su procedencia, a través del Sistema de Información de Contrataciones Públicas (SICP), dentro del plazo tope.

La inasistencia a la Junta de Aclaraciones no será motivo de descalificación de la oferta.

La convocante podrá optar por responder las consultas en la Junta de Aclaraciones o podrá diferirlas, para que sean respondidas conforme con los plazos de respuestas o emisión de adendas. En todos los casos se deberá levantar acta circunstanciada.

## Documentos de la oferta

El pliego, sus adendas y aclaraciones no forman parte de la oferta, por lo que no se exigirá la presentación de copias de los mismos con la oferta.

Los oferentes inscriptos en el Sistema de Información de Proveedores del Estado (SIPE) de la DNCP, podrán presentar con su oferta, la constancia firmada emitida a través del SIPE, que reemplazará a los documentos solicitados por la convocante en el anexo pertinente del presente pliego.

Los oferentes deberán indicar en su oferta, que documentos que forman parte de la misma son de carácter confidencial e invocar la norma que ampara dicha reserva, para así dar cumplimiento a lo estipulado en la Ley N° 5282/14 "DE LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL". Si el oferente no hace pronunciamiento expreso amparado en la Ley, se entenderá que toda su oferta y documentación es pública.

## Oferentes en consorcio

Dos o más interesados que no se encuentren comprendidos en las inhabilidades para presentar ofertas o contratar, podrán unirse temporalmente para presentar una oferta sin crear una persona jurídica.

Para ello deberán presentar escritura pública de constitución del consorcio o un acuerdo con el compromiso de formalizar el consorcio por escritura pública en caso de resultar adjudicados, antes de la firma del contrato.

Los integrantes de un consorcio no podrán presentar ofertas individuales ni conformar más de un consorcio en un mismo lote o ítem, lo que no impide que puedan presentarse individualmente o conformar otro consorcio que participe en diferentes partidas.



---

## **Aclaración de las ofertas**

Con el objeto de facilitar el proceso de revisión, evaluación, comparación y posterior calificación de ofertas, el Comité de Evaluación solicitará a los oferentes, aclaraciones respecto de sus ofertas, dichas solicitudes y las respuestas de los oferentes se realizarán por escrito.

A los efectos de confirmar la información o documentación suministrada por el oferente, el Comité de Evaluación, podrá solicitar aclaraciones a cualquier fuente pública o privada de información.

Las aclaraciones de los oferentes que no sean en respuesta a aquellas solicitadas por la convocante, no serán consideradas.

No se solicitará, ofrecerá, ni permitirá ninguna modificación a los precios ni a la sustancia de la oferta, excepto para confirmar la corrección de errores aritméticos.

---

## **Disconformidad, errores y omisiones**

Siempre y cuando una oferta se ajuste sustancialmente al pliego de bases y condiciones, el Comité de Evaluación, requerirá que cualquier disconformidad u omisión que no constituya una desviación significativa, sea subsanada en cuanto a la información o documentación que permita al Comité de Evaluación realizar la calificación de la oferta.

A tal efecto, el Comité de Evaluación emplazará por escrito al oferente a que presente la información o documentación necesaria, dentro de un plazo razonable establecido por el mismo, bajo apercibimiento de rechazo de la oferta. El Comité de Evaluación, podrá reiterar el pedido cuando la respuesta no resulte satisfactoria, toda vez que no viole el principio de igualdad.

Con la condición de que la oferta cumpla sustancialmente con los Documentos de la Licitación, la Convocante corregirá errores aritméticos de la siguiente manera y notificará al oferente para su aceptación:

1. Si hay una discrepancia entre un precio unitario y el precio total obtenido al multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio total y el precio unitario será corregido.
2. Los precios subtotales podrán ser corregidos siempre que se mantenga inalterable el precio total obtenido en la SBE.
3. En ambos casos, los precios unitarios modificados no podrán ser superiores a los precios unitarios iniciales que figuran en el Acta de Sesión Pública Virtual de la SBE.
4. En caso de que el oferente haya cotizado su precio en guaraníes con décimos y céntimos, la convocante procederá a realizar el redondeo hacia abajo, aun cuando el resultado varíe del precio total que se encuentra en el Acta de Sesión Pública Virtual de la SBE como precio final.
5. Si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras a menos que la cantidad expresada en palabras corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras de conformidad con los párrafos (1) y (2) mencionados.

---

## **Idioma de la oferta**

La oferta deberá ser presentada en idioma castellano o en su defecto acompañado de su traducción oficial, realizada por un traductor público matriculado en la República del Paraguay.

La convocante permitirá con la oferta, la presentación de catálogos, anexos técnicos o folletos en idioma distinto al castellano y sin traducción:

No Aplica

---

## Idioma del contrato

El contrato, así como toda la correspondencia y documentos relativos al Contrato, deberán ser escritos en idioma castellano. Los documentos de sustento y material impreso que formen parte del contrato, pueden estar redactados en otro idioma siempre que estén acompañados de una traducción realizada por traductor matriculado en la República del Paraguay, en sus partes pertinentes al idioma castellano y, en tal caso, dicha traducción prevalecerá para efectos de interpretación del contrato.

El proveedor correrá con todos los costos relativos a las traducciones, así como todos los riesgos derivados de la exactitud de dicha traducción.

---

## Moneda de la oferta y pago

La moneda de la oferta y pago será:

En Guaraníes para todos los oferentes

La cotización en moneda diferente de la indicada en este apartado será causal de rechazo de la oferta. Si la oferta seleccionada es en Guaraníes, la oferta se deberá expresar en números enteros, no se aceptarán cotizaciones en decimos y céntimos.

---

## Visita al sitio de ejecución del contrato

La convocante dispone la realización de una visita al sitio con las siguientes indicaciones:

fecha: 29 de octubre de 2021

lugar: *Molas Lopez N° 480 e/ Tte. Cirilo Gill Edificio del SNPP*

hora: 09:00 hs Sede Central SNPP y a las 13:00 hs. CCP - PJ -San Lorenzo

procedimiento: *En el sitio Molas Lopez N° 480 e/ Tte. Cirilo Gill Sede Central del SNPP Dpto. Informática; con funcionarios del Departamento de Informática*

Nombre del funcionario responsable de guiar la visita: *Funcionarios del Departamento de Informática*

participación Obligatoria: SI

Al culminar la o las visitas, se labrará acta en la cual conste, la fecha, lugar y hora de realización, en la cual se identifique el nombre de las personas que asistieron en calidad de potenciales oferentes, así como del funcionario encargado de dicho acto.

Los gastos relacionados con dicha visita correrán por cuenta del oferente.

Cuando la convocante haya establecido que no será requisito de participación, el oferente podrá declarar bajo fe de juramento conocer el sitio y que cuenta con la información suficiente para preparar la oferta y ejecutar el contrato.

## **Precio y formulario de la oferta**

El oferente indicará el precio total de su oferta y los precios unitarios de los bienes que se propone suministrar, utilizando para ello el formulario de oferta y lista de precios, disponibles para su descarga a través del SICP, formando ambos un único documento.

1. Para la cotización el oferente deberá ajustarse a los requerimientos que se indican a continuación:

a) El precio cotizado deberá ser el mejor precio posible, considerando que en la oferta no se aceptará la inclusión de descuentos de ningún tipo.

b) En el caso del sistema de adjudicación por la totalidad de los bienes requeridos, el oferente deberá cotizar en la lista de precios todos los ítems, con sus precios unitarios y totales correspondientes.

c) En el caso del sistema de adjudicación por lotes, el oferente cotizará en la lista de precios uno o más lotes, e indicará todos los ítems del lote ofertado con sus precios unitarios y totales correspondientes. En caso de no cotizar uno o más lotes, los lotes no cotizados no requieren ser incorporados a la planilla de precios.

d) En el caso del sistema de adjudicación por ítems, el oferente podrá ofertar por uno o más ítems, en cuyo caso deberá cotizar el precio unitario y total de cada uno o más ítems, los ítems no cotizados no requieren ser incorporados a la planilla de precios.

2. En caso de que se establezca en las bases y condiciones, los precios indicados en la lista de precios serán consignados separadamente de la siguiente manera:

a) El precio de bienes cotizados, incluidos todos los derechos de aduana, los impuestos al valor agregado o de otro tipo pagados o por pagar sobre los componentes y materia prima utilizada en la fabricación o ensamblaje de los bienes;

b) Todo impuesto al valor agregado u otro tipo de impuesto que obligue la República del Paraguay a pagar sobre los bienes en caso de ser adjudicado el contrato; y

c) El precio de otros servicios conexos (incluyendo su impuesto al valor agregado), si lo hubiere, enumerados en los datos de la licitación.

3. En caso de indicarse en el SICP, que se utilizará la modalidad de contrato abierto, cuando se realice por montos mínimos y máximos deberán indicarse el precio unitario de los bienes ofertados; y en caso de realizarse por cantidades mínimas y máximas, deberán cotizarse los precios unitarios y los totales se calcularán multiplicando los precios unitarios por la cantidad máxima correspondiente.

4. El precio del contrato que cobre el proveedor por los bienes suministrados en virtud del contrato no podrá ser diferente a los precios unitarios cotizados en su oferta, excepto por cualquier ajuste previsto en el mismo.

5. En caso que se requiera el desglose de los componentes de los precios será con el propósito de facilitar a la convocante la comparación de las ofertas.

## **Abastecimiento simultáneo**

El sistema de abastecimiento simultáneo para esta licitación será:

No Aplica

## **Incoterms**

La edición de incoterms para esta licitación será:

No Aplica

Las expresiones DDP, CIP, FCA, CPT y otros términos afines, se regirán por las normas prescriptas en la edición vigente de los Incoterms publicada por la Cámara de Comercio Internacional.

Durante la ejecución contractual, el significado de cualquier término comercial, así como los derechos y obligaciones de las partes serán los prescritos en los Incoterms, a menos que sea inconsistente con alguna disposición del Contrato.

## **Autorización del Fabricante**

Los productos a los cuales se le requerirá Autorización del Fabricante son los indicados a continuación:

*Si se requiere autorización del Fabricante*

Cuando la convocante lo requiera, el oferente deberá acreditar la cadena de autorizaciones, hasta el fabricante o productor.

## **Muestras**

Se requerirá la presentación de muestras de los siguientes productos y en las siguientes condiciones:

No Aplica

En caso de ser solicitadas, las muestras deberán ser presentadas junto con la oferta, o bien en el plazo fijado por la convocante en este apartado, la cual será considerada requisito indispensable para la evaluación de la oferta. La falta de presentación en la forma y plazo establecido por la convocante será causal de descalificación de la oferta.

## **Copias de la oferta - CPS**

El oferente presentará su oferta original. En caso de que la convocante requiera la presentación de copias lo deberá indicar en este apartado, las copias deberán estar identificadas como tales.

Cuando la presentación de ofertas se realice a través del sistema de Oferta Electrónica, la convocante no requerirá de copias.

Cantidad de copias requeridas:

0 copias

## **Formato y firma de la oferta**

1. El formulario de oferta y la lista de precios serán firmados, física o electrónicamente, según corresponda por el oferente o por las personas debidamente facultadas para firmar en nombre del oferente.
2. No serán descalificadas las ofertas que no hayan sido firmadas en documentos considerados no sustanciales.
3. Los textos entre líneas, tachaduras o palabras superpuestas serán válidos solamente si llevan la firma de la persona que firma la Oferta.
4. La falta de foliatura no podrá ser considerada como motivo de descalificación de las ofertas.

## **Periodo de validez de las ofertas**

Las ofertas deberán mantenerse válidas (en días calendarios) por:

88

Las ofertas se deberán mantener válidas por el periodo indicado en el presente apartado, que se computará a partir del inicio de la etapa competitiva. Toda oferta con un periodo menor será rechazada.

La convocante en circunstancias excepcionales podrá solicitar, por escrito, al oferente que extienda el periodo de validez de la oferta, por lo tanto la Garantía de Mantenimiento de la Oferta deberá ser también prorrogada.

El oferente puede rehusarse a tal solicitud sin que se le haga efectiva su Garantía de Mantenimiento de Oferta. A los oferentes que acepten la solicitud de prórroga no se les pedirá ni permitirá que modifiquen sus ofertas.

## **Garantías: instrumentación, plazos y ejecución.**

1. La garantía de mantenimiento de oferta deberá expedirse en un monto en guaraníes que no deberá ser inferior al porcentaje especificado en el SICP. El oferente puede adoptar cualquiera de las formas de instrumentación de las garantías dispuestas por las normativas vigentes.
2. La garantía de mantenimiento de ofertas presentada en los términos del párrafo anterior, deberá cubrir el precio total de la oferta en la etapa de recepción de propuestas.
3. En los contratos abiertos, el porcentaje de las garantías a ser presentado por los oferentes que participen, deberá ser aplicado sobre el monto máximo del llamado; si la adjudicación fuese por lote o ítem ofertado, deberán sumarse los valores máximos de cada lote o ítem ofertado, a fin de obtener el monto sobre el cual se aplicará el porcentaje de la citada garantía.
4. En caso de instrumentarse a través de Garantía Bancaria, deberá estar sustancialmente de acuerdo con el formulario de Garantía de Mantenimiento de oferta incluido en la Sección "Formularios".
5. La garantía de mantenimiento de oferta en caso de oferentes en consorcio deberá ser presentado de la siguiente manera:
  - Consorcio constituido por escritura pública: deberán emitir a nombre del consorcio legalmente constituido por escritura pública, del líder del consorcio o de todos los socios que la integran;
  - Consorcio en proceso de formación con acuerdo de intención: deberán emitir a nombre del líder del consorcio en proceso de formación con acuerdo de intención o de todos los miembros que la integran.
6. La garantía de mantenimiento de ofertas podrá ser ejecutada:
  - a) Si el oferente altera las condiciones de su oferta,
  - b) Si el oferente retira su oferta durante el período de validez de la oferta,
  - c) Si no acepta la corrección aritmética del precio de su oferta, en caso de existir,

- d) Si el oferente no presentare su oferta en la fecha y hora señaladas, previo requerimiento por parte de la convocante,
- e) Si el adjudicatario no procede, por causa imputable al mismo a:
- e.1. suministrar los documentos indicados en el pliego de bases y condiciones para la firma del contrato,
  - e.2. firmar el contrato,
  - e.3. suministrar en tiempo y forma la garantía de cumplimiento de contrato,
  - e.4. se comprobare que las declaraciones juradas presentadas por el oferente adjudicado con su oferta sean falsas,
  - e.5. el adjudicatario no presentare las legalizaciones correspondientes para la firma del contrato, cuando éstas sean requeridas, o
  - e.6. no se formaliza el consorcio por escritura pública, antes de la firma del contrato.
7. Las garantías tanto de Mantenimiento de Oferta, Cumplimiento de Contrato o de Anticipo, sea cual fuere la forma de instrumentación adoptada, deberá ser pagadera ante solicitud escrita de la convocante donde se haga constar el monto reclamado, cuando se tenga acreditada una de las causales de ejecución de la póliza. En estos casos será requisito que previamente el oferente sea notificado del incumplimiento y la intimación de que se hará efectiva la ejecución del monto asegurado.
8. Si la entrega de los bienes o la prestación de los servicios se realizare en un plazo menor o igual a diez (10) días calendario, posteriores a la firma del contrato, la garantía de cumplimiento deberá ser entregada antes del cumplimiento de la prestación.
9. La garantía de Fiel Cumplimiento de Contrato será liberada 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 de contrato, incluyendo cualquier obligación relativa a la garantía de los bienes.

## **Periodo de Validez de la Garantía de Mantenimiento de Oferta**

El plazo de validez de la Garantía de Mantenimiento de Oferta (en días calendario) será de:

120

El oferente deberá presentar como parte de su oferta una Garantía de Mantenimiento de acuerdo al porcentaje indicado para ello en el SICP y por el plazo indicado en este apartado. Cuando la competencia se desarrolle por más de un día, la garantía de mantenimiento de oferta deberá cubrir a partir del primer día del inicio de la etapa competitiva.

## **Porcentaje de Garantía de Fiel Cumplimiento de Contrato**

El Porcentaje de Garantía de Fiel Cumplimiento de Contrato es de:

10,00 %

La garantía de Cumplimiento de Contrato deberá ser presentada por el proveedor, dentro de los 10 días calendarios siguientes a partir de la fecha de suscripción del contrato, de conformidad con lo dispuesto en el artículo 39 de la Ley N° 2051/2003.

## **Periodo de validez de la Garantía de Cumplimiento de Contrato**

El plazo de vigencia de la Garantía de Fiel Cumplimiento de Contrato será de:

*El plazo de vigencia de esta garantía deberá cubrir por lo menos de 30 días posteriores al plazo de ejecución o vigencia del contrato, según sea el caso*

---

## Periodo de validez de la Garantía de los bienes

El periodo de validez de la Garantía de los bienes será el siguiente:

*Según Especificaciones Técnicas*

---

## Tiempo de funcionamiento de los bienes

El periodo de tiempo estimado de funcionamiento de los bienes, para los efectos de repuestos será de:

*12 MESES*

---

## Plazo de reposición de bienes

El plazo de reposición de bienes para reparar o reemplazar será de:

10 (diez) días hábiles a partir de la notificación recibida por parte del administrador del contrato

El proveedor garantiza que todos los bienes suministrados están libres de defectos derivados de actos y omisiones que este hubiera incurrido, o derivados del diseño, materiales o manufactura, durante el uso normal de los bienes en las condiciones que imperen en la República del Paraguay.

1. La Contratante comunicará al proveedor la naturaleza de los defectos y proporcionará toda evidencia disponible, inmediatamente después de haberlos descubierto. La contratante otorgará al proveedor facilidades razonables para inspeccionar tales defectos.

Tan pronto reciba ésta comunicación, y dentro del plazo establecido en este apartado, deberá reparar o reemplazar los bienes defectuosos, o sus partes sin ningún costo para la contratante.

2. Si el proveedor después de haber sido notificado, no cumple dentro del plazo establecido, la contratante, procederá a tomar medidas necesarias para remediar la situación, por cuenta y riesgo del proveedor y sin perjuicio de otros derechos que la contratante pueda ejercer contra el proveedor en virtud del contrato.

## **Cobertura de Seguro de los bienes**

La cobertura de seguro requerida a los bienes será:

No Aplica

A menos que se disponga otra cosa en este apartado, los bienes suministrados deberán estar completamente asegurados en guaraníes, contra riesgo de extravío o daños incidentales ocurridos durante la fabricación, adquisición, transporte, almacenamiento y entrega, de acuerdo a los incoterms aplicables.

## **Sistema de presentación de ofertas**

Las ofertas serán presentadas en un solo sobre y deberán:

1. Indicar el nombre y la dirección del oferente;
2. Estar dirigidos a la convocante;
3. Llevar la identificación específica del proceso de licitación indicado en el SICP;
4. Llevar una advertencia de no abrir antes de la hora y fecha de apertura de ofertas.

Si los sobres no están cerrados e identificados como se requiere, la convocante no se responsabilizará en caso de que la oferta se extravíe o sea abierta prematuramente.

## **Plazo para presentar las ofertas**

Culminada la etapa competitiva, presentarán las ofertas físicas en la dirección y hasta la fecha y hora que se indican en el SICP, los siguientes participantes requeridos:

los ubicados en 1°, 2° y 3° lugar

Las ofertas deberán ser recibidas por la convocante en la dirección y hasta la fecha y hora que se indican en el SICP.

La convocante podrá a su discreción, extender el plazo originalmente establecido para la presentación de ofertas mediante una adenda. En este caso todos los derechos y obligaciones de la convocante y de los oferentes previamente sujetos a la fecha límite original para presentar las ofertas quedarán sujetos a la nueva fecha prorrogada.

Cuando la presentación de oferta sea electrónica la misma deberá sujetarse a la reglamentación vigente.

## **Retiro, sustitución y modificación de las ofertas**



1. Un Oferente podrá retirar, sustituir o modificar su oferta después de presentada mediante el envío de una comunicación por escrito, debidamente firmada por el representante autorizado. La sustitución o modificación correspondiente de la oferta deberá acompañar dicha comunicación por escrito.

2. Todas las comunicaciones deberán ser:

- a) presentadas conforme a la forma de presentación e identificación de las ofertas y además los respectivos sobres deberán estar marcados "RETIRO", "SUSTITUCION" o "MODIFICACION";
- b) recibidas por la Convocante antes del plazo límite establecido para la presentación de las ofertas;

Las ofertas cuyo retiro, sustitución o modificación fuere solicitada serán devueltas sin abrir a los oferentes remitentes, durante el acto de apertura de ofertas.

3. Ninguna oferta podrá ser retirada, sustituida o modificada durante el intervalo comprendido entre la fecha límite para presentar ofertas y la expiración del período de validez de las ofertas indicado en el Formulario de Oferta, o cualquier extensión si la hubiere, caso contrario, se hará efectiva la Garantía de Mantenimiento de Oferta.

---

## Apertura de ofertas

1. La convocante abrirá las ofertas y en caso de que hubiere notificaciones de retiro, sustitución y modificación de ofertas presentadas, las leerá en el acto público con la presencia de los oferentes o sus representantes a la hora, en la fecha y el lugar establecidos en el SICP.

2. Cuando la presentación de oferta sea electrónica, el acto de apertura deberá sujetarse a la reglamentación vigente.

3. Primero se procederá a verificar de entre las ofertas recibidas por courier o entregadas personalmente, los sobres marcados como:

a) "RETIRO". Se leerán en voz alta y el sobre con la oferta correspondiente no será abierto sino devuelto al oferente remitente. No se permitirá el retiro de ninguna oferta a menos que la comunicación de retiro pertinente contenga la autorización válida para solicitar el retiro y sea leída en voz alta en el acto de apertura de las ofertas.

b) "SUSTITUCION" se leerán en voz alta y se intercambiará con la oferta correspondiente que está siendo sustituida; la oferta sustituida no se abrirá y se devolverá al oferente remitente. No se permitirá ninguna sustitución a menos que la comunicación de sustitución correspondiente contenga una autorización válida para solicitar la sustitución y sea leída en voz alta en el acto de apertura de las ofertas.

c) "MODIFICACION" se abrirán y leerán en voz alta con la oferta correspondiente. No se permitirá ninguna modificación a las ofertas a menos que la comunicación de modificación correspondiente contenga la autorización válida para solicitar la modificación y sea leída en voz alta en el acto de apertura de las ofertas. Solamente se considerarán en la evaluación los sobres que se abren y leen en voz alta durante el Acto de Apertura de las Ofertas.

4. Los representantes de los oferentes que participen en la apertura de las ofertas deberán contar con autorización suficiente para suscribir el acta y los documentos que soliciten, bastando para ello la presentación de una autorización escrita del firmante de la oferta, esta autorización podrá ser incluida en el sobre oferta o ser portado por el representante.

5. Se solicitará a los representantes de los oferentes que estén presentes que firmen el acta. La omisión de la firma por parte de un Oferente no invalidará el contenido y efecto del acta. Se distribuirá una copia del acta a todos los presentes.

6. Las ofertas sustituidas y modificadas presentadas, que no sean abiertas y leídas en voz alta durante el acto de apertura no podrán ser consideradas para la evaluación sin importar las circunstancias y serán devueltas sin abrir a los oferentes remitentes.

7. La falta de firma en un documento sustancial, es considerada una omisión sustancial que no podrá ser subsanada en ninguna oportunidad una vez abiertas las ofertas.

8. El acta de apertura deberá ser comunicada al Sistema de Información de Contrataciones Públicas para su difusión, dentro de los dos (02) días hábiles de la realización del acto de apertura.

# REQUISITOS DE CALIFICACIÓN Y CRITERIOS DE EVALUACIÓN

Esta sección contiene los criterios que la convocante utilizará para evaluar la oferta y determinar si un oferente cuenta con las calificaciones requeridas. Ningún otro factor, método o criterio será utilizado.

## Condición de Participación

Podrán participar de ésta licitación, individualmente o en forma conjunta (consorcio), los oferentes domiciliados en la República del Paraguay, que no se encuentren comprendidos en las prohibiciones o limitaciones para presentar propuestas y contratar con el Estado, establecidas en la Ley N° 2051/03 "De Contrataciones Públicas".

Adicionalmente a lo establecido en el párrafo anterior el oferente deberá considerar las siguientes condiciones de participación:

Que se encuentren registrados/as en el Sistema de Información de Proveedores del Estado (SIPE), debiendo suscribir ante el mismo una Declaración Jurada en la cual manifiesta que tiene pleno conocimiento y acepta las reglas del proceso para su activación como oferente. La Declaración Jurada referida, podrá ser descargada desde el SICP, módulo del SIPE.

Que activados/as conforme al SIPE posean su Usuario y Contraseña, personal e intransferible, salvo que los mismos hayan sido cancelados por el Sistema, de conformidad a la reglamentación específica. La pérdida del usuario y contraseña deberá ser comunicada a la DNCP para que, a través del Sistema, sea bloqueado el acceso inmediatamente; y

Como requisito para la participación en la Subasta a la Baja Electrónica, el oferente deberá manifestar en el campo previsto en el Sistema Electrónico, que cumple plenamente los requisitos de habilitación y que su propuesta de precios está conforme con las exigencias del pliego de bases y condiciones.

## Requisitos de Calificación

### Capacidad Legal

Los oferentes deberán declarar que no se encuentran comprendidos en las limitaciones o prohibiciones para contratar con el Estado, contempladas en el artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, declaración que forma parte del formulario de oferta.

Serán desechadas las ofertas de los oferentes que se encuentren comprendidos en las prohibiciones o limitaciones para contratar a la hora y fecha límite de presentación de ofertas o a la fecha de firma del contrato.

A los efectos de la verificación de la existencia de prohibiciones o limitaciones contenidas en los incisos a) y b), m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, el comité de evaluación realizará el siguiente análisis:

1. Verificará que el oferente haya proporcionado el formulario de ofertas que incluye la declaratoria debidamente firmada.
2. 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 de la Ley N° 2051/03, modificado por Ley N° 6716/2021.
3. Verificará por los medios disponibles, si el oferente y los demás sujetos individualizados en las prohibiciones o limitaciones contenidas en los incisos a) y b), m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, aparecen en la base de datos del SINARH o de la Secretaría de la Función Pública.
4. Si se constatará que alguno de las personas mencionadas en el párrafo anterior figura en la base de datos del SINARH o de la Secretaría de la Función Pública, el comité analizará acabadamente si tal situación le impedirá ejecutar el contrato, exponiendo los motivos para aceptar o rechazar la oferta, según sea el caso.
5. Verificará que el oferente haya proporcionado el formulario de Declaración de Miembros, de conformidad a estándar debidamente firmado en su oferta y cotejará los datos con las personas físicas inhabilitadas que constan en el registro de "Sanciones a Proveedores" del SICP a fin de detectar si directores, gerentes, socios gerentes, quienes ejerzan la administración, accionistas, cuotapartistas o propietarios se hallan comprendidos en el presupuesto del inciso m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021.

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

6. 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.

## **Análisis de precios ofertados**

Durante la evaluación de ofertas, luego de haber realizado la corrección de errores aritméticos y de ordenar las ofertas presentadas de menor a mayor, el Comité de Evaluación procederá a solicitar a los oferentes una explicación detallada de la composición del precio ofertado de cada ítem, rubro o partida adjudicable, conforme a los siguientes parámetros:

1. En contrataciones en general: cuando la diferencia entre el precio ofertado y el precio referencial sea superior al 25% para ofertas por debajo del precio referencial y del 15% para ofertas que se encuentren por encima del referencial establecido por la convocante y difundido con el llamado a contratación.

Si el oferente no respondiese la solicitud, o la respuesta no sea suficiente para justificar el precio ofertado del bien, el precio será declarado inaceptable y la oferta rechazada.

El análisis de los precios, con esta metodología, será aplicado a cada ítem, rubro o partida que componga la oferta y en cada caso deberá ser debidamente fundada la decisión adoptada por la Convocante en el ejercicio de su facultad discrecional.

## **Certificado de Producto y Empleo Nacional - CPS**

A los efectos de acogerse al beneficio de la aplicación del margen de preferencia, el oferente deberá contar con el Certificado de Producto y Empleo Nacional (CPEN). El certificado debe ser emitido como máximo a la fecha y hora de la etapa competitiva.

La falta del CPEN no será motivo de descalificación de la oferta, sin embargo, el oferente no podrá acogerse al beneficio.

El comité de evaluación verificará en el portal oficial indicado por el Ministerio de Industria y Comercio (MIC) la emisión en tiempo y forma del CPEN declarado por los oferentes. No será necesaria la presentación física del Certificado de Producto y Empleo Nacional.

Independientemente al sistema de adjudicación, el margen de preferencia será aplicado a cada bien o servicio objeto de contratación que se encuentre indicado en la planilla de precios.

### **a) Consorcios:**

#### **a.1. Provisión de Bienes**

El CPEN debe ser expedido a nombre del oferente que fabrique o produzca los bienes objeto de la contratación. En el caso que ninguno de los oferentes consorciados fabrique o produzca los bienes ofrecidos, el consorcio deberá contar con el CPEN correspondiente al bien ofertado, debiendo encontrarse debidamente autorizado por el fabricante. Esta autorización podrá ser emitida a nombre del consorcio o de cualquiera de los integrantes del mismo.

## **Margen de preferencia local - CPS**

Para contrataciones realizadas por Unidades Operativas que se encuentren conformadas dentro de un municipio o departamento se deberá considerar que, si la oferta evaluada como la más baja pertenece a una firma u empresa domiciliada

fuera del territorio departamental de la convocante, ésta será comparada con la oferta más baja de la firma u empresa domiciliada dentro del territorio de la convocante, agregándole al precio total de la oferta propuesta por la primera una suma del diez por ciento (10%) del precio. Si en dicha comparación adicional la oferta de la firma u empresa domiciliada dentro del territorio departamental de la convocante resultare ser la más baja, se la seleccionará para la adjudicación; en caso contrario se seleccionará la oferta de servicios de la firma u empresa domiciliada fuera del territorio departamental de la convocante.

En el caso de que el oferente, sea de la zona y además cuente con margen de preferencia, se le aplicará únicamente el margen de este último.

Las convocatorias deberán acogerse a las condiciones específicas para la aplicación del Margen de Preferencia Local establecidas en la reglamentación emitida por la DNCP.

## Requisitos documentales para evaluación de las condiciones de participación

<b>1. Formulario de Oferta (*)</b> [El formulario de oferta y lista de precios, generados electrónicamente a través del SICP, deben ser completados y firmados por el oferente.]
<b>2. Garantía de Mantenimiento de Oferta (*)</b> La garantía de mantenimiento de oferta debe ser extendida, bajo la forma de una garantía bancaria o póliza de seguro de caución.
<b>3. Certificado de Cumplimiento con la Seguridad Social. (**)</b>
<b>4. Certificado de Producto y Empleo Nacional, emitido por el MIC, en caso de contar. (**)</b>
<b>5. Constancia de presentación de la Declaración Jurada de bienes y rentas, activos y pasivos ante la Contraloría General de la República, para los sujetos obligados según los incisos a) y b) del numeral 2 del art. 1 de la Ley N° 6355/19. (**)</b>
<b>6. Declaración Jurada de Declaración de Miembros, de conformidad con el formulario estándar Sección Formularios (**)</b>
<b>7. Certificado de Cumplimiento Tributario (**)</b>
<b>8. Patente Comercial del municipio en donde esté asentado el establecimiento principal del oferente. (**)</b>
<b>9. Documentos legales</b>
<b>9.1. Oferentes Individuales. Personas Físicas.</b>
<ul style="list-style-type: none"><li>Fotocopia simple de la Cédula de Identidad del firmante de la oferta. (*)</li></ul>
<ul style="list-style-type: none"><li>Constancia de inscripción en el Registro Único de Contribuyentes - RUC. (*)</li></ul>

- 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. (\*)

## 9.2. Oferentes Individuales. Personas Jurídicas.

- 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. (\*)

- Constancia de inscripción en el Registro Único de Contribuyentes y fotocopia simple de los documentos de identidad de los representantes o apoderados de la sociedad.

- 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); o 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. (\*)

## 9.3. 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 Oferentes individuales. Personas Físicas. Cada integrante del consorcio que sea una persona jurídica domiciliada en Paraguay deberá presentar los documentos requeridos para Oferentes Individuales Personas Jurídicas. (\*)

2. Original o fotocopia del consorcio constituido o del acuerdo de intención de constituir el consorcio por escritura pública en caso de resultar adjudicados y antes de la firma del contrato. Las formalidades de los acuerdos de intención y de los consorcios serán determinadas por la Dirección Nacional de Contrataciones Públicas (DNCP). (\*)

3. Fotocopia simple de los documentos que acrediten las facultades de los firmantes del acuerdo de intención de consorciarse. Estos documentos pueden consistir en (\*):

- Un poder suficiente otorgado por escritura pública por cada miembro del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o
- 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 (\*):

1. 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
2. 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.

Los documentos indicados con asterisco (\*) son considerados documentos sustanciales a ser presentados con la oferta.

Los documentos indicados con doble asterisco (\*\*) deberán estar vigentes al inicio de la etapa competitiva.

---

## Capacidad Financiera

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

*a) Contribuyentes IRE con su Régimen correspondiente.*

*Deberán cumplir con el siguiente parámetro:*

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

*Deberá ser igual o mayor que 1, en promedio, en los [2018, 2019, 2020].*

*2. Endeudamiento: pasivo total / activo total*

*No deberá ser mayor a 0,80 en promedio, en los [2018, 2019, 2020]*

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

*El promedio en los años [2018, 2019, 2020], no deberá ser negativo.*

*Copia autenticada del Balance General Impositivo en formato clasificado, años [2018, 2019, 2020], que contendrá el resumen de cada uno de los balances. Los mismos deberán estar firmados por el Contador y Representante Legal de la Empresa. Deberá ir acompañado con la copia autenticada del Formulario de liquidación del Impuesto del ejercicio correspondiente.*

*b) Para contribuyente 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 últimos años [2018, 2019 y 2020]*

*a. Endeudamiento: pasivo total / activo total*

*No deberá ser mayor a 0,80 en promedio, en los últimos años [2018, 2019 y 2020]*

*b. Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital. El promedio en los años 2018, 2019 y 2020], no deberá ser negativo.*

*c) Para contribuyentes de IRPC*

*Deberán cumplir el siguiente parámetro:*

*Eficiencia: (Ingreso/Egreso).*

*Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales 2018, 2019 y 2020.*

*d) Para contribuyentes de IRP*

*Deberán cumplir el siguiente parámetro:*

*Eficiencia: (Ingreso/Egreso).*

*Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales 2018, 2019 y 2020.*

*f) Para contribuyentes de exclusivamente IVA General*

*Deberá cumplir el siguiente parámetro:*

*Eficiencia: (Ingreso/Egreso).*

*Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales 2018, 2019 y 2020.*

## Requisitos documentales para la evaluación de la capacidad financiera

- a) Copia autenticada del Balance General Impositivo en formato clasificado, años [2018, 2019, 2020]
- b) Certificado de Cumplimiento Tributario vigente a la fecha de apertura o al inicio de la carga de propuestas para procesos de SBE.
- b) Balance General y Cuadro de Estado de Resultados de los años 2018, 2019 y 2020 para contribuyente de IRACIS.
- c) IVA General de los últimos 2018, 2019 y 2020 años, para contribuyentes sólo del IVA General
- d) Formulario 106 de los últimos 2018, 2019 y 2020 años para contribuyentes del IRPC
- e) Formulario 104 de los últimos 2018, 2019 y 2020 años para contribuyentes de Renta Personal.

## Experiencia requerida

Con el objetivo de calificar la experiencia del oferente, se considerarán los siguientes índices:

Demostrar la experiencia en **Provisión e instalación de equipos de CCTV IP** con facturaciones de venta y/o recepciones finales por un monto equivalente al **50 %** como mínimo del monto total ofertado en la presente licitación, de los: **los últimos 3 años. 2018, 2019 y 2020**

El oferente deberá a tener experiencia comprobada y certificada por los clientes, en la provisión e instalación de equipos de CCTV en por lo menos 2 (dos) proyectos.

## Requisitos documentales para la evaluación de la experiencia

1. Copia de facturaciones y/o recepciones finales que avalen la experiencia requerida

*2. Patente y Licencia Comercial vigente a la fecha de la etapa competitiva*

## Capacidad Técnica

El oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de capacidad técnica:

- a) El oferente deberá presentar Carta o Documento de autorización del fabricante
- b) El oferente deberá prever un soporte de atención ante fallas, repuestos, mano de obra y mantenimiento de rutina a cargo del oferente por un periodo de 24 (veinticuatro) meses
- c) Tener domicilio en Paraguay
- d) Existencia Legal de por lo menos cinco (5) años de antigüedad, contados a partir de la fecha de la habilitación de la empresa. Copia de Constitución de Sociedad.
- e) Presentar catálogos técnicos del fabricante que contengan las informaciones relativas al modelo de equipo ofertado, o capacidad de entrega de información técnica en formato digital, en forma inviolable (ej. Acrobat Reader).
- f) El oferente deberá contar con técnicos (al menos 1) certificado por el fabricante de la marca ofertada.
- g) Todos los equipos deberán contar con al menos 2 años de garantía
- h) Será fundamental y obligatoria la presentación de Planillas de Cumplimiento de Especificaciones en forma de Declaración Jurada, en la que el oferente deberá expresar de manera explícita si el bien o servicio ofertado CUMPLE o NO CUMPLE con las especificaciones técnicas.

## Requisito documental para evaluar la capacidad técnica

- a. Carta o documento de autorización del Fabricante
- b. Presentar Garantía en forma de Declaración Jurada a través de la cual se comprometa a proveer un soporte de atención ante fallas, repuestos, mano de obra y mantenimientos de rutina a cargo del Oferente por un periodo de 24 (veinticuatro) meses
- c. Tener domicilio en Paraguay en forma de declaración jurada
- d. Existencia Legal de por lo menos cinco (5) años de antigüedad, contados a partir de la fecha de la habilitación de la empresa. Copia de Constitución de Sociedad.
- e. Presentar catálogos técnicos del fabricante que contengan las informaciones relativas al modelo de equipo ofertado, o capacidad de entrega de información técnica en formato digital, en forma inviolable (ej. Acrobat Reader).
- f. El oferente deberá contar con técnicos (al menos 1) certificado por el fabricante de la marca ofertada.
- g. Todos los equipos deberán contar con al menos 2 años de garantía
- h. Será fundamental y obligatoria la presentación de Planillas de Cumplimiento de Especificaciones en forma de Declaración Jurada, en la que el oferente deberá expresar de manera explícita si el bien o servicio ofertado CUMPLE o NO CUMPLE con las especificaciones técnicas



## Otros criterios que la convocante requiera

Otros criterios para la evaluación de las ofertas a ser considerados en ésta contratación serán:

El SNPP se reserva el derecho de realizar las verificaciones con el fabricante de las informaciones presentadas en las ofertas

## Criterio de desempate de ofertas

El vencedor de cada grupo subastado será el oferente que ingresó el menor precio. En los casos de igualdad de precios, queda como vencedor el que lo haya ingresado primero.

Siempre que el criterio de desempate establecido, no sea aplicable, el comité de evaluación determinará cuál de ellas es la mejor calificada para ejecutar el contrato utilizando los criterios dispuestos para el efecto por la DNCP.

**Nota1:** Conforme a lo previsto en el Decreto reglamentario de la Ley de Contrataciones los adjudicatarios de los contratos resultantes de los procesos licitatorios, deberán inscribirse en el Sistema de Información de Proveedores del Estado - SIPE, como requisito previo a la emisión del Código de Contratación respectivo, no siendo la inscripción una exigencia para participar en el proceso tradicional.

# SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS

Esta sección constituye el detalle de los bienes con sus respectivas especificaciones técnicas - EETT, de manera clara y precisa para que el oferente elabore su oferta. Salvo aquellas EETT de productos ya determinados por plantillas aprobadas por la DNCP.

## Suministros y Especificaciones técnicas

El Suministro deberá incluir todos aquellos ítems que no hubiesen sido expresamente indicados en la presente sección, pero que pueda inferirse razonablemente que son necesarios para satisfacer el requisito de suministro indicado, por lo tanto, dichos bienes serán suministrados por el Proveedor como si hubiesen sido expresamente mencionados, salvo disposición contraria en el Contrato.

Los bienes suministrados deberán ajustarse a las especificaciones técnicas y las normas estipuladas en este apartado. En caso de que no se haga referencia a una norma aplicable, la norma será aquella que resulte equivalente o superior a las normas oficiales de la República del Paraguay. Cualquier cambio de dichos códigos o normas durante la ejecución del contrato se aplicará solamente con la aprobación de la contratante y dicho cambio se registrará de conformidad a la cláusula de adendas y cambios.

El Proveedor tendrá derecho a rehusar responsabilidad por cualquier diseño, dato, plano, especificación u otro documento, o por cualquier modificación proporcionada o diseñada por o en nombre de la Contratante, mediante notificación a la misma de dicho rechazo.

## Detalle de los productos con las respectivas especificaciones técnicas

Los productos a ser requeridos cuentan con las siguientes especificaciones técnicas:

ITEM	CODIGO DE CATALOGO	DESCRIPCIÓN	DESCRIPCIÓN ESPECIFICACIONES TECNICAS MINIMAS REQUERIDAS	CANTIDAD	UNIDAD DE MEDIDA	PRESENTACIÓN
1	46171619-9999	Sistema de circuito cerrado de video vigilancia	Según especificaciones tecnicas	1	unidad	unidad
Sub Items						

1.1	camara tipo 1: procesador de captura y procesamiento de imagen preparada para integración, inteligencia artificial e Depp Learning en el borde	según especificaciones tecnicas	2	unidad	unidad
1.2	camara tipo 2: domo 5 mpx	según especificaciones tecnicas	28	unidad	unidad
1.3	camara tipo 3: bullet 5 mpx	según especificaciones tecnicas	28	unidad	unidad
1.4	camara tipo 4: speed dome 5 mpx	según especificaciones tecnicas	1	unidad	unidad
1.5	tipo 1: servidor de gestión	según especificaciones tecnicas	1	unidad	kit
1.6	tipo 2 : servidor para sitio centralizado	según especificaciones tecnicas	1	unidad	kit
1.7	tipo 3: servidor de video wall	según especificaciones tecnicas	1	unidad	kit
1.8	tipo 4: servidor de video remoto	según especificaciones tecnicas	1	unidad	kit
1.9	tipo 5: servidor de aplicaciones y virtualización	según especificaciones tecnicas	1	unidad	kit
1,10	licencias tipo 1: servidor remoto	según especificaciones tecnicas	33	unidad	unidad
1.11	licencias tipo 4: servidor centralizado	según especificaciones tecnicas	70	unidad	unidad
1.12	biometria facial, registro de licencia perpetua, pago unico ilimitadas camaras de analitica facial	según especificaciones tecnicas	1000	unidad	unidad
1.13	licencias de integración y automatización de flujos modalidad instalación	según especificaciones tecnicas	1	unidad	unidad

1.14	sistema de control de acceso	según especificaciones técnicas	1	unidad	unidad
1.15	molinete tipo 1 por pasaje flujo libre	según especificaciones técnicas	1	unidad	kit
1.16	molinete tipo 2	según especificaciones técnicas	1	unidad	kit
1.17	barreras de acceso alto flujo	según especificaciones técnicas	1	unidad	kit
1.18	control de acceso IP multi tecnología	según especificaciones técnicas	3	unidad	kit
1.19	sensor de presencia IOT	según especificaciones técnicas	2	unidad	kit
1.20	sensor de presencia IOT	según especificaciones técnicas	2	unidad	kit
1.21	Plataforma de gestión de alarmas integrada al VMS y conectividad IOT hasta 20 dispositivos por 24 meses	según especificaciones técnicas	1	unidad	unidad
1.22	servicio de integración de sistema de control inteligente	según especificaciones técnicas	1	unidad	global

Las características técnicas se describen en el numeral 3 de la presente Especificación Técnica y según cantidades indicadas en la Lista Equipos requeridos a ser suministrados.

Los equipos correspondientes detallados en alcance del suministro, deberá incluir la provisión, montaje y puesta en servicio de todos los componentes sea hardware y software con sus accesorios necesarios para optimizar su uso, los cuales se detallan en cada ítem respectivo.

### 3. Características Técnicas

3.1 Los equipos y sus respectivos componentes con sus características básicas específicas y licencias legales se detallarán a continuación

<b>ITEM 1</b>	<b>Cámara Tipo 1: Procesador de captura y procesamiento de imagen preparada para integración, Inteligencia Artificial y Deep Learning en el borde</b>
---------------	---

Características  
Generales

Es un equipo de captura y procesamiento de imagen que por medio de reconocimiento óptico de caracteres (OCR), realiza la (LPR). El equipo actúa como una plataforma abierta que permite introducir aplicaciones de terceros para reducir las necesidades de equipamientos adicionales, con acelerador de Red Neural (NPU) compatible con soluciones de visión computacional

Conformidad con las normas FCC, CE Compliance y homologación Anatel o normas similares y equivalentes

Deberá disponer capacidad superior de procesamiento de analíticos, brinda el poder de las características deep learning, que sumada a la conectividad móvil, arroja una cámara inteligente.

Resolución  
(Tamaño en  
píxeles del  
Sensor): 1636 x  
1220 px. Tamaño  
Físico del Sensor:  
1/1.8" o similar

Sistema de Captura de Imagen: Global Shutter. Lente: CS Mount 13-55 mm o similar

Shutter Mínimo | Máximo: 1/12500 (80 us) a 1/15.6 (64 ms) o similar

Tipo de Sensor de Imagen: CCD Tasa de Frames (Interna) :15 cps.o similar

Tasa de Cuadros (Transmisión): hasta 15 cps. o similar

Tensión de Alimentación: 9 ~ 32 VDC.

Tipo de Conectores: 2 LAN| USB A 2.0| Microfit 16 vías| Slot para SIM Card, |Slot para Micro SD| conector AUTO ÍRIS  
|Conectores SMA con sus respectivas antenas GPS, Wi-Fi, 4G/3G. o equivalentes

Potencia Mínima | Máxima: 8.5 ~ 12 W o equivalente.

Peso sin lente: aproximado 875 g

Dimensiones aproximadas: (A) x (L) x (C) - (mm) 75x74x189. Grado de protección IP: mínimo IP40.

Temperatura de operación: '-10 a 65 °C con humedad relativa del aire de 5% a 95% y sin condensación, cumpliendo en conformidad con la IEC 60068-2-2 o similar.

Entradas y Salidas (I/O): 4 puertas digitales bidireccionales individualmente programable con entradas con salidas opto-aisladas para conexión de señal de disparo o/u integración a otros dispositivos del sistema de integrado.

Características  
Específicas

Interfaz de Red: 2 interfaces 10/100/1000 Mbps (Gigabit). Formato de Imagen: JPEG.

Formato de Vídeos H.264, H.265 e MJPEG. Protocolos de Comunicación 'RTSP y FTP. O equivalente

APIs (Application Programming Interface): REST O equivalente para integración con el sistema.

Capacidad de Almacenamiento Externo: Tarjeta de memoria microSD hasta 128GB o equivalente

Memoria RAM: 2GB LPDDR4 (2100 Mbps e 1050 MHz).

LPR incorporado.

Perfiles de Configuración de la Cámara: mínimo 4.

Múltiples exposiciones de 2 a 8 imágenes por disparo con distintas opciones de configuración de parámetros.

	<p>Función HDR (alto rango dinámico).</p> <p>GPS para evidencia de imagen: Gen8C Lite Multi-constellation Glonass  BeiDou/Compass  Galileo e QZSS  Antena Externa 2 dBic típico o similar.</p> <p>Wifi: IEEE 802.11 bandas b/g/n 2.4 GHz  Antena Externa 2.8 dBi típico,</p> <p>4G: LTE-FDD/LTE-TDD/WCDMA/GSM  Antena Externa (1.42 dBi, 1.91 dBi  2.51 dBi  3.23 dBi 2.89 dBi) o similar.</p> <p>Módulo eSIM para comunicación celular o similar.</p> <p>CPU mínimo: Quad-core 1.2 GHz, con soporte a tecnología ARM y NEON o compatible</p> <p>Software libre incorporado (ej: Linux) opción de cargar software analítico en la propia cámara a través de contenedores Docker. Utilizando a API REST, para las funciones de captura de imágenes y acceso a los analíticos   SDK y ejemplos de aplicaciones deberán estar disponibles O equivalente , software libre.</p>
Características constructivas	Aluminio anodizado y panel frontal en policarbonato O equivalente en proteccion
<b>ITEM 2</b>	<b>Cámara Tipo 2: domo 5 mpx.</b>
Características Generales o equivalentes	<p>Deberá ser una cámara IP que proporciona resolución de mínimo 5 MP en tiempo real a 24 cps. con una lente vari-focal de enfoque automático teniendo como referencia la distancia focal de 2.7~13.5mm con lente motorizado simultáneo y tecnología de color en la oscuridad para video de calidad en cualquier condición de iluminación, debe cumplir con los requisitos ONVIF-S (Opcional) facilitando su integración exitosa con cualquier solución de plataforma abierta en el mercado.</p> <p><b>IMAGEN</b></p> <p>Sensor de imagen CMOS de mínimo 5 MP de 1/2.8" cantidad total de píxeles 2592</p> <p>(H) x 1944 (V), relación de aspecto 4:3.</p> <p><b>LENTE</b></p> <p>Distancia focal de 2.7 13.5 mm, F1.4, tipo P-iris vari-focal con enfoque automático y zoom motorizado, campo de visión (FoV, Campo de visión) 85° ~ 31°, distancia Infra roja con un rango de alcance de 30.48 m, zoom óptico digital siendo x 5 E/S.</p> <p><b>OPERACIONALES</b></p> <p>Modo del obturador: automático, manual, anti parpadeo, obturador lento</p> <p>velocidad del obturador:1/15 ~ 1/32000, obturador lento: 1/2, 1/3, 1/5, 1/6, 1/7.5, 1/10</p> <p>Día (Color), Noche (Blanco y negro), reducción de ruido digital con función 3D, reducción de ruido digital 3D, rango dinámico amplio (WDR, Rango dinámico amplio) WDR real (WDR) dB120 dB.</p> <p><b>Zona de Privacidad</b></p> <p>Mínimo 16 máscaras de privacidad programables, compensación de luz de fondo (BLC), capacidad de voltear de forma horizontal y vertical, notificaciones de alarma, correo electrónico, FTP, salida de alarma y grabación de tarjeta SD.</p> <p><b>RED</b></p>
Características específicas o	Puerto LAN 10/100Base-T, tipo de compresión de video

equivalente

H.265, H.264, MJPEG, resolución H.265: 2592x1944, 2304x1296, 2.1 MP/1080p, 720p, VGA, D1, CIF H.264: 2592x1944, 2304x1296, 2.1 MP/1080p, 720p, VGA, D1, CIF MJPEG: 2.1 MP/1080p, 720p, 800x600, VGA, 768x432, D1, CIF, velocidad de

fotogramas, hasta 24 cps en todas las resoluciones, velocidad de bits de video H.264/H.265: 32 Kbps ~ 14 Mbps MJPEG: 1 Mbps ~ 40 Mbps, doble control de uso de bits, H.265 o H.265/H.264/MJPEG simultáneo, capacidad de flujo de transmisión doble a diferentes velocidades y resoluciones.

#### Norma IP .

IPv4, IPv6

#### Protocolo

TCP/IP, UDP, AutoIP, RTP(UDP/TCP), RTSP, NTP, HTTP, HTTPS, SSL, DNS, DDNS, DHCP, FTP, SMTP, ICMP, SNMPv1/v2/v3 (MIB-2), ONVIF-S.

#### Seguridad

HTTPS(SSL), filtro IP, 802.1x, Autenticación implícita (ID/PW), que cumple con las normas del ONVIF, visualizador web en los SO: Sistema operativo Windows®, Mac®, Linux®, Navegador: Internet Explorer®, Google Chrome®, Mozilla Firefox®, Safari® y Software de gestión de video.

#### AMBIENTALES Y ELECTRICAS

Temperatura operativa -20 °C ~ 50 °C, humedad durante la operación relativa 10- 90 % (sin condensación), grado de protección IP Certificación IP66 Otras certificaciones o similares CE, FCC, RoHS

CC de 12 V, PoE (IEEE802.3af, clase 3), 12 V CC: máx. 7.4 W-PoE: máx. 8.7 W.

Características constructivas o equivalentes

Deberá ser una carcasa tipo mini-dome (DOMO) de policarbonato clasificación IP66 antivandálica y IK-10 resistente a impactos mínimamente una ranura para tarjeta de memoria compatible con los estándares Micro SD/SDHC/SDXC Clase 10. Garantía de fábrica mínima 5 años.

#### ITEM 3

#### Cámara Tipo 3: Bullet 5 mpx

Características Generales o equivalentes

Deberá ser una cámara IP que proporciona resolución de mínimo 5 MP en tiempo real a 24 cps, con una lente vari-focal de enfoque automático teniendo como referencia la distancia focal de 2.7~13.5 mm con zoom motorizado, que soporte códec H.265/H.264/MJPEG simultáneo y tecnología de color en la oscuridad para video de calidad en cualquier condición de iluminación, que cumplen los requisitos ONVIF-S facilitando su integración exitosa con cualquier solución de plataforma abierta en el mercado, entrada de sensor de alarma, salida de relé, servidor Web integrado, capacidad de arranque en frío a -40°C.

#### IMAGEN

Sensor de imagen CMOS de mínimo 5 MP de 1/2.8", cantidad total de píxeles 2592

(H) x 1944 (V), iluminación de escena relación de aspecto 4:3.

#### LENTE

Distancia focal de 2.7~13.5 mm, F1.4, tipo de lente P-iris vari-focal con enfoque automático y zoom motorizado, campo de visión (FoV, Campo de visión) 85° ~ 31°, distancia infra roja con un rango de alcance de 42.67 m,

zoom óptico siendo x 5, E/S, entrada/salida de audio 1/1, compresión de audio: G.711, entrada/salida de alarma: 1/1.

#### OPERACIONALES

Modo del obturador en automático o manual, anti parpadeo, obturador lento.

Velocidad del obturador de 1/15 ~ 1/32000, obturador lento de 1/2, 1/3, 1/5, 1/6, 1/7.5, 1/10, control automático de mejoras (AGC) en automático día y noche, automático día (Color), noche (Blanco y negro), reducción de ruido digital con función 3D, rango dinámico amplio (WDR, Rango Dinámico Amplio) siendo WDR real (WDR) dB120 dB.

#### Zona de Privacidad

Mínimo 16 máscaras de privacidad programables, compensación de luz de fondo (BLC), capacidad de voltear de forma horizontal y vertical, función de notificaciones de alarma, correo electrónico, FTP, salida de alarma y grabación de tarjeta SD.

#### RED

Características específicas o equivalente

Puerto LAN 10/100 Base-T, tipo de compresión de video H.265, H.264, MJPEG, resolución H.265: 2592x1944, 2304x1296, 2.1 MP/1080p, 720p, VGA, D1, CIF H.264: 2592x1944, 2304x1296, 2.1 MP/1080p, 720p, VGA, D1, CIF MJPEG: 2.1 MP/1080p,

720p, 800x600, VGA, 768x432, D1, CIF ,velocidad de fotogramas, hasta 24 cps en todas las resoluciones, velocidad de bits de video H.264/H.265: 32 Kbps ~ 14 Mbps MJPEG: 1 Mbps ~ 40 Mbps, doble control de uso de bits, H.265 o H.265/H.264/MJPEG simultáneo, capacidad de flujo de transmisión doble a diferentes velocidades y resoluciones.

#### Normas IP

IPv4, IPv6.

#### Protocolo

TCP/IP, UDP, Auto IP, RTP(UDP/TCP), RTSP, NTP, HTTP, HTTPS, SSL, DNS, DDNS, DHCP, FTP, SMTP, ICMP, SNMPv1/v2/v3 (MIB-2), ONVIF.

#### Seguridad

HTTPS (SSL), filtro IP, 802.1x, Autenticación implícita (ID/PW).

Visualizador web en las plataformas: sistema operativo Windows®, Mac®, Linux® con los navegadores: Internet Explorer®, Google Chrome®, Mozilla Firefox®, Safari® y Software de gestión de video.

#### AMBIENTALES Y ELECTRICAS

Temperatura operativa -40 °C ~ 50 °C, humedad durante la operación relativa 10- 90 % (sin condensación), grado de protección IP con Certificación IP66, otras certificaciones CE, FCC, RoHS o similares

CC de 12 V, PoE (IEEE802.3af, clase 3), 12 V CC: máx. 9 W, PoE: máx. 10.5 W.

Características constructivas o equivalentes

Deberá ser una carcasa tipo bala (Bullet) clasificación IP66 y resistente a la intemperie para cumplir con la Certificación IP66, mínimamente una ranura para tarjeta de memoria compatible con los estándares Micro SD/SDHC/SDXC. Garantía de fábrica mínima 5 años.

#### ITEM 4

#### Cámara Tipo 4: Sped Dome 5 mpx.

Características Generales o equivalentes

Deberá ser una cámara tipo PTZ con movimiento horizontal 0 a 360°, vertical -10 ~ 190° a una velocidad máxima de 380°/seg. y un zoom de 30x para proporcionar imágenes claras a una resolución de hasta 4 K en tiempo real de 24 cps, con tecnología todo color, para lograr un color sorprendente en la oscuridad, el zoom debe ser óptico de 30x e infra rojo de alta potencia con un alcance de hasta 350 m

#### IMAGEN

Deberá ser una cámara IP que proporciona resolución de mínimo de hasta 4 K, sensor de imagen CMOS de 1/1.7 de 4 K, cantidad total de píxeles 4168 x 3062, Píxeles activos 3840 x 2160, sistema de escaneo progresivo, iluminación de escena mínima 0.75 lux (color), 0 Lux (blanco y negro).



## LENTE

Distancia focal 6 ~ 180 mm, lente tipo PTZ con zoom motorizado 30x, distancia del IR 350 m de alcance, ángulo de visión de 55.4 ~ 2.7°, zoom digital/óptico de 30x E/S, entrada/salida de audio 1/1 Compresión de audio G.711, alerta audible de mínimo 3 archivos de audio definidos por el usuario entrada/salida de alarma 4/1, activación manual 4 activaciones programables

## OPERACIONALES

El modo del obturador debe ser automático, anti parpadeo, velocidad del obturador de 1/10,000 ~ 1 seg., contraluz, anti neblina, rango dinámico amplio (WDR) real de 120 dB, reducción de ruido digital, balance de blancos automático o manual, día y noche, Día (Color), Noche (Blanco y negro), con funciones de espejo y volcado, zonas de privacidad mínimo 16 máscaras programables, detección de movimiento 16 zonas programables siendo 8 áreas incluidas y 8 áreas excluidas, modo de grabación en tarjeta SD (grabación de evento y continua), almacenamiento de eventos en memoria intermedia FTP Anterior: 30 seg., Posterior: 30 seg., tarjeta SD Anterior: 10 seg., Posterior: 60 seg., notificaciones de alarma por correo electrónico, servidor FTP, activación de salida de alarma, activación de salida de audio, activación preprogramada, servidor de notificaciones, notificaciones XML o grabación en tarjeta SD.

## FUNCIÓN PTZ

Alcance de movimiento horizontal 360° sin fin, velocidad de movimiento horizontal Máx. 380°/seg. (preprogramado), alcance de movimiento vertical -10 ~ 190°, velocidad de movimiento vertical Máx. 380°/seg. (preprogramado), preprogramado 256 recorrido 8 Patrón 8, con funciona inicial.

## RED

Características  
específicas o  
equivalente

LAN RJ-45 (10/100 Base-T), tipo de compresión de video H.265 (perfil principal),

H.264 (perfil de línea base, perfil principal, perfil alto), MJPEG, resolución 3840x2160, 3072x2048, 2592x1944/1520, 2560x1440, 1920x1080, 1440x1080, 1280x1024/720, 1024x768, 800x600/480, D1, 640x480, 400x240, CIF, velocidad de bits de video flujo Cuádruple (H.265x3/H.264, MJPEGx1), códec inteligente de alta transmisión, control de uso de bits, transmisión múltiple CVBR/VBR a H.265,

H.264 (velocidad de fotogramas y ancho de banda controlables), velocidad de fotogramas Hasta 24 fps en todas las resoluciones, capacidad de flujo de transmisión, transmisión doble a diferentes velocidades y resoluciones

## Normas IP:

IPv4, IPv6

## Protocolo

TCP/IP, UDP, HTTP, HTTPS, QoS, FTP, UPnP, RTP, RTSP, RTCP,

DHCP, ARP, Zeroconf, Bonjour. Seguridad y autenticación de contraseña, autoridad multiusuario, filtrado IP, HTTPS (SSL), acceso máximo de usuarios :10 usuarios en vivo, 3 en reproducción, cumple con las normas ONVIF.

Visualizador web SO: Sistema operativo Windows®, Mac®, Linux®

Navegador: Internet Explorer®, Sincronización con el tiempo de red Servidor NTP, aceptar actualización remota respaldo y restablecimiento

## Operación y eléctrica:

Temperatura operativa -30 °C ~ 55 °C, humedad durante la operación Humedad relativa 0 ~ 90 % (sin condensación) otras certificaciones CE, FCC, RoHS, PoE (UPoE, Clase 4), 12 V CC. Consumo de energía PoE: 28 W, 500 mA, 12 V CC: 28 W, 2.3 A

Características constructivas o equivalentes

Dentro de una carcasa de aluminio para el conjunto PTZ, domo de policarbonato con clasificación IK-10 resistente a impactos. Grado de protección IP: Clasificación IP66.

#### ITEM 5

##### Tipo 1: Servidor de Gestión

Construido con propósito de gestión con SQL STD. Solución escalable, desarrollado e ideal para análisis. Aceleración de GPU.

Características Generales

Arquitectura flexible.

VMS optimizado y certificado. Probado en laboratorio.

Garantía 5 años de fábrica.

Procesador: Familia de procesadores específicos para servidores hasta 8 núcleos, frecuencia básica de 1.8 Ghz hasta 3.2, cache de 11mb hasta 16.5mb compatible con la carga de trabajo del sistema ofertado. Sistema operativo: IOT integrado (OEM) precargados con su Hardware, Núcleo híbrido (Kernel), con soporte al menos hasta 2027

Características Específicas o Equivalente

Memoria	Opción predeterminada de 32 GB Almacenamiento máximo de datos	Hasta 128 Salidas de video VGA
---------	---	--------------------------------

GPU: placa grafica Redes 1 x 1GbE

USB Delantero: 2 x USB 2.0

Trasero: 2 x USB 3.0

Sistema operativo RAID: 2 SSD de hasta 240 GB (RAID 1) Monitoreo de hardware preinstalado.

Características constructivas o equivalentes

Formato 2 U

Dimensiones del producto (métrico) (H x B x T)44,55 x 73,03 x 8,74 cm

#### ITEM 6

##### Tipo 2: Servidor para sitio centralizado

Dispositivo de almacenamiento de video comercial empresarial . El servidor deberá estar especialmente diseñado para instalaciones de video vigilancia de nivel empresarial. Desde el transporte hasta las instalaciones gubernamentales y cualquier lugar intermedio.

El servidor debe ser un equipo de ingeniería avanzada que pueda transformar un práctico servidor, en una máquina de rendimiento mejorado/optimo.

Deberá estar preparado para una gran cantidad de cámaras, soportar como mínimo 200 camaras 5MP y las aplicaciones de gran retención, proporcionando un rendimiento de velocidad de grabación de 400-600 Mbps y potencialmente superior en la aplicación VMS.

Características Generales o equivalentes

Deberá estar preparado para instalaciones de nivel empresarial, entorno de misión crítica y soporte técnico. Estar optimizado, certificado y garantizado, con la marca del VMS ofertado en el ítem 11 (Licencias Tipo 4: Servidor Centralizado). Preinstalado de fábrica una herramienta de monitoreo de hardware diseñada para monitorear, informar y administrar el entorno y el rendimiento del hardware de los servidores lo que garantiza el máximo tiempo de actividad, para el control total del hardware de seguridad con un panel de control fácil de usar que le permita evaluar, administrar y hacer cambios de forma remota. Las alertas instantáneas reportan problemas antes que los operadores lo hagan, haciendo que el TI sea más proactivo.

	Preinstalado un sistema de optimización de transferencia de datos de alto rendimiento desde discos duros externos. Garantía 5 años de fábrica	
	Procesador: Familia de procesadores específicos para servidores hasta 8 núcleos, frecuencia básica de 1.8 Ghz hasta 3.2, cache de 11mb hasta 16.5mb compatible con la carga de trabajo del sistema ofertado Sistema operativo: Para servidor mínimamente 2019, específico para servidores, soporte hasta 2024, núcleo híbrido, arquitectura x86-64, Infraestructura Hiper-Convergente, Acceso al dispositivo de alojamiento para contenedores, incluye protección contra amenazas avanzadas, que permita ejecutar. Deberá contar con una interface para administración unificada, donde desde una única consola se pueda administrar sistemas externos y servidores remotos, sino también otras herramientas de línea de comando como PowerShell	
Características específicas o equivalente	Memoria	Opción predeterminada de 32 GB hasta 64 GB Almacenamiento máximo de datos Hasta 384TB RAW
	Salidas de video VGA en GPU	
	Redes 4 x 1GbE (opcional + 2x 10GbE SFP + Configuración) USB	Delantero: 2 x USB 2.0
	Trasero: 2 x USB 3.0	
	Sistema operativo RAID: 2 SSD de 240 GB (RAID 1) Nivel de RAID de datos: PERC H740P JBOD, 0, 1, 5, 6, 10 Monitoreo de hardware NVR	Preinstalado
Características constructivas o equivalentes	Factor de Forma 2 U	
	Bahías de Unidades del sistema Operativo 2 x M.2 BOSS PCIe Card Bahías de Unidades de los Datos Up to 18 x 3.5 Data Drives (14 Hot	
	Swappable, 4 Fixed). Fuente de Alimentación 1+1 750W cambio en caliente	
	Humedad de Funcionamiento 5% ~ 90% non-condensing Dimensiones 17.08 x 3.4 x 28.16 in / 434 x 86 x 715 mm	
ITEM 7	Tipo 3: Servidor de Video Wall	
Características Generales	Sistema de Video Wall (muralla de video)	
	Todos los monitores existentes deben ser compatibles con los equipos y servidores de la central de monitoreo.	
	Se debe prever un hardware de video Wall con configuración mínima en matrix 2x4, compatible con los servidores de video y debe estar con la solución embarcada y totalmente compatible con solución de video vigilancia propuesta.	
	Deberá ser de la misma marca/proveedor,	
	Los equipos tienen que tener un servidor nativo y un software nativo para la instalación y puesta en funcionamiento de lo que es el SO y el VMS dentro del propio equipo y finalmente debe tener una herramienta tal que permita tener la imagen completa de un equipo a la hora de una falla, para poder restaurarlo de manera intuitiva. Estos equipos deben estar en red.	

	<p>Plataforma de gestión de video:</p> <p>Software preinstalado de fábrica para el monitoreo del hardware:</p> <p>Monitoreo intuitivo del sistema: monitorear la información del sistema o la señal de estado de los elementos clave de los dispositivos desde un solo panel.</p> <p>Gestión sencilla del ecosistema: desde un único menú desplegable, puede navegar para gestionar clientes, usuarios, puertas de enlace y dispositivos.</p> <p>El sistema deberá detectar problemas de índole técnico que permita al TI reportar dichos eventos a través de un informe directamente a la fábrica.</p> <p>Procesador: Familia de procesadores específicos para servidores hasta 8 núcleos, frecuencia básica de 1.8 Ghz hasta 3.2, cache de 11mb hasta 16.5mb compatible con la carga de trabajo del sistema ofertado</p> <p>Sistema operativo: IOT integrado (OEM) precargados con su Hardware, Núcleo híbrido (Kernel), con soporte al menos hasta 2027</p>
Características específicas o equivalente	<p>Hasta 64 GB DDR4 2666MHz Almacenamiento hasta 2 SSD de 256 GB (RAID 1)</p> <p>Gráficos: hasta 2 x (Memoria de GPU 4 GB GDDR5 - Interfaz de Memoria 128-bit - Ancho de Banda de Memoria Hasta 80 GB/s) - Unidad óptica CD / DVD / RW óptico de línea delgada</p> <p>Conectividad 2 x 1 GbE</p> <p>Puertos de E / S traseros 6 puertos USB 3.1</p> <p>Gabinete: Torre</p>
Características constructivas aproximadas	<p>Fuente de alimentación: 950W 80PLUS Gold Certified Power Supply Disco interno Drives 2 TB Data Drive</p> <p>Front I/O Ports 2 x USB 3.1 Type-A 2 x USB 3.1 Type-C</p>
<b>ITEM 8</b>	<b>Tipo 4: Servidor de Video Remoto</b>
Características Generales o equivalentes	<p>Compatibilidad con cámaras ampliadas acepta más de 10.000 dispositivos a su VMS.</p> <p>Un único punto de contacto para la asistencia del VMS y de los dispositivos, posibilidad de realizar intervenciones de asistencia sobre el terreno para sustituciones y reparaciones de hardware.</p> <p>Deberá ser un sistema servidor de video de bastidor pequeño, pero también flexible para crecer dentro de la infraestructura de TI existente.</p> <p>Tamaño: Montaje en bastidor 1U , CPU: de 4 nucleos, 4 subprocesos, de 3.2 a 4.2 Ghz, cache 6mb, velocidad de bus 8Gt/s compatible con 64-bit</p> <p>GPU: Placa grafica ultra HD , frecuencia base 350 Mhz, secuencia de gráficos hasta 1.2Ghz, memoria de gráficos gata 64Gb, que soporte hasta 4k @ 60Hz, resolución máxima, 4096x2304 @ 24Hz o compatible</p> <p>RAM:mínimo 16 GB DDR4</p> <p>RAM:16 GB DDR4</p> <p>Sistema operativo: IOT integrado (OEM) precargados con su Hardware, Núcleo híbrido (Kernel), con soporte al menos hasta 2027. Almacenamiento VMS/OS:1 x 256 GB (M.2 PCIe NVMe)</p> <p>Número de discos duros: 2 x 3.5 (accesibles desde el exterior)</p>

Características específicas o equivalente	<p>Almacenamiento en bruto: de 4/8/16/24 hasta 32 TB (unidades tipo empresarial 24/7) Controlador y compatibilidad RAID, controlador Intel® Rapid Storage o similar, RAID 0,1 (Software RAID) o similar Puertos de visualización 2 x USB 3.1 tipo C/puerto de visualización iGFX, adaptador de USB-C a video VGA incluido Interfaz de red 1x 1 GbE (RJ45).</p> <p>1x 1/2.5/5/10 GbE (RJ45).</p> <p>Ranuras PCIe disponibles: Una ranura PCI Express® x16 Gen 3 de anchura doble y altura completa.</p> <p>Una ranura PCI Express x4 Gen 3 de altura completa Archivado a NAS externo, a través de puerto LAN Credencial y cifrado de clave</p> <p>Módulo de plataforma segura (TPM 2.0) Información de hardware:</p> <p>Garantía de hardware: 5 años de garantía de fabrica para todo el sistema. Alimentación:100~240 V, 50/60 Hz</p> <p>Consumo máximo:550 W con hasta un 94 % de eficiencia Protección</p> <p>OVP (exceso de tensión), OCP (exceso de corriente), OTP (exceso de temperatura), SCP (cortocircuito).</p> <p>Estándares sobre emisiones y seguridad, CE (clase A), UKCA, FCC, RCM, UL, México (NOM), VCCI, conformidad con disposiciones comerciales, conforme a NDAA o normas similares.</p>
Características constructivas o equivalentes	<p>Humedad 10-85 % de humedad relativa (sin condensación)</p>

#### ITEM 9 Tipo 5: Servidor de Aplicaciones y Virtualización

Características generales o equivalentes	<p>Servidor para aplicaciones y analítica con un procesador de hasta 16 GB de memoria de rango dual, controlador de almacenamiento con 2 MB de caché y batería de almacenamiento inteligente, 2 bahías de unidades de factor formato reducido, un adaptador Ethernet de 1 Gb y 1 puertos, un kit de rieles SFF fáciles de instalar, un kit de brazo para gestionar cables, una fuente de 500 W. Garantía de fábrica de 3 años.</p> <p>Procesador: Familia de procesadores específicos para servidores hasta 8 núcleos, frecuencia básica de 1.8 Ghz hasta 3.2, cache de 11mb hasta 16.5mb compatible con la carga de trabajo del sistema ofertado. Memoria: hasta 32GB (2 x 16GB) PC4-2666V-R DDR4 RDIMM</p>
Características específicas o equivalente	<p>2 x Hot Plug 3.5in Large Form Factor Smart Carrier Smart Array E208i-a SR</p> <p>Fuente 500W Ethernet 1Gb</p> <p>Garantía de fábrica de 3 años.</p>
Características constructivas	<p>Formato 2 U</p>

#### ITEM 10 Licencias Tipo 1: Servidor Remoto

Características generales	<p>Deberá posibilitar la integración con otros sistemas y aplicaciones, periodo de retención ilimitado, para tener acceso a las grabaciones de vídeo siempre que las necesite. Deberá ser practico y fácil de actualizar.</p> <p><b>Herramientas de búsqueda</b></p> <p>Cifrado basado en certificados para proteger el tráfico de datos (vídeo, audio, metadatos), originado en el servidor de grabación y recuperado por los com-ponentes conectados.</p> <p>Protección mediante contraseña, aceleración por hardware, almacenamiento Edge y servidores failover, mapas con múltiples capas, autenticación doble, gestor de alarmas, metadatos, mapas y alarmas.</p>
---------------------------	--

Características  
específicas o  
equivalente

Licencias perpetuas, hasta 48 cámaras por servidor de grabación. 1 servidor de grabación por sistema para esta licencia.

Motor de reglas flexible. Rendimiento y escalabilidad. Gestión centralizada.

Microsoft Active Directory. Buffering pregrabación en RAM.

Descodificación acelerada por hardware (Quick Sync) Quality Recording  
**Integración**

Integración de aplicaciones de terceros, screen recorder, metadatos, Add-on

**Ciberseguridad y derechos de usuario** Autenticación Kerberos

Cifrado de comunicación (grabación, gestión y servidor móvil) Acceso restringido de usuario por tipo de cliente

**Doble autorización** Monitorización e investigación Función de mapa

Búsqueda centralizada Máscara de privacidad Notificación push Gestor de alarmas Panel de usuario

Failover y redundancia Servidor de eventos failover Servidor failover de gestión

#### ITEM 11

#### Licencias Tipo 4: Servidor Centralizado

Características mínimas del sistema de gestión de video vigilancia confiable.

El SNPP necesita una vigilancia constante y fiable durante las 24 horas y los 7 días de la semana y 365 días del año.

La plataforma debe ser altamente personalizable, ofreciendo múltiples funciones de acuerdo a las necesidades de la Institución.

Considerando que no existe una solución única para todos los escenarios de video vigilancia y que cada operación es diferente, este concepto de plataforma debe ser abierta a las necesidades de la Institución, permitiendo la compatibilidad con varias marcas, modelos de cámaras y dispositivos.

Además, la plataforma de poseer la capacidad de incrementar equipos a gran escala. Deberá admitir un número ilimitado de servidores de grabación para que pueda ampliar el sistema sin problemas. Deberá conectar varios sitios con una arquitectura de infraestructura abierta y flexible, que permite conectar los sistemas individuales multimarca en una jerarquía padre/hijo de sitios federados, Gestionando de manera centralizada la video vigilancia distribuida en varias instalaciones.

El sistema integral de vigilancia, debe ser abierta y con capacidad de aprovechar la innovación de toda una industria, siendo compatible el 100% con otras marcas y dispositivos, que permita la posibilidad de agregar nuevas tecnologías a medida que se desarrollan, lo que facilite actualizar y mejorar continuamente el sistema de seguridad.

Interfaz gráfica fácil de utilizar, amigable.

El diseño deberá combinar simplicidad, sofisticación y ofrecer a los operadores la posibilidad de tener el control absoluto de cualquier situación al instante. Esto deberá garantizar un aprendizaje sencillo y una gran facilidad de uso, sin renunciar a prestaciones avanzadas.

Interfaces fáciles de utilizar que se deben ajustar a usuarios individuales en función de los niveles de seguridad y las áreas de responsabilidad.

Mapas interactivos que le ofrecen una completa panorámica general de la instalación local y remotas completas.

Búsqueda centralizada para que pueda buscar secuencias de vídeo, alarmas, eventos, marcadores y movimiento en un mismo sitio.

Características  
Generales o  
equivalentes

	<p>Sin brechas de seguridad,</p> <p>Toda la plataforma deberá estar en un entorno estructurado: seguridad en el diseño, seguridad por defecto y seguridad en la implementación, diferentes mecanismos de seguridad que mantienen su sistema y sus datos protegidos contra amenazas internas y externas y en cumplimiento a la ley de datos.</p> <p>Sistema</p> <p>Tipo de implementación Gestionado centralmente, multiservidor. Licencias perpetuas.</p> <p>Número de cámaras por servidor de grabación ilimitada. Número de servidores de grabación por sistema ilimitado. Motor de reglas flexible.</p> <p>Rendimiento y escalabilidad Gestión centralizada.</p> <p>Microsoft Active Directory. Buffering pregrabación en RAM.</p> <p>Decodificación acelerada por hardware (Quick Sync). Almacenamiento Edge.</p> <p>Scalable Video. Quality Recording.</p> <p>Decodificación de vídeo acelerada por hardware (GPU). Monitor del sistema.</p> <p>Integración.</p> <p>Integración de aplicaciones de terceros Screen Recorder.</p>
Características específicas o equivalente	<p>Metadatos. Add-on .</p> <p>Video Wall. Interoperabilidad</p> <p>Interconnect ubicación central/remota. Federated Architecture ubicación central/remota. Ciberseguridad y derechos de usuario Autenticación Kerberos.</p> <p>Cifrado de comunicación (grabación, gestión y servidor móvil). Acceso restringido de usuario por tipo de cliente.</p> <p>Doble autorización.</p> <p>Cifrado base de datos de medios y firma digital. Derechos de gestión por niveles.</p> <p>Verificación en dos pasos. Monitorización e investigación Función de mapa.</p> <p>Búsqueda centralizada. Máscara de privacidad. Notificación push.</p> <p>Gestor de alarmas. Panel de usuario. Marcador manual.</p> <p>Marcadores basados en reglas. Plano inteligente.</p> <p>Bloqueo de evidencias. Failover y redundancia Servidor de eventos failover. Servidor failover de gestión.</p> <p>Servidor de grabación failover (activo/pasivo).</p>
ITEM 12	<p><b>Biometría Facial, registro de Licencia Perpetua, único pago, ilimitadas cámaras de analítica facial</b></p> <p>Deberá ser un motor de reconocimiento facial puro que permite el procesamiento eficiente y preciso de rostros en imágenes y transmisión de video en vivo y puede ejecutarse en una amplia gama de dispositivos.</p> <p>La identificación sin contacto para fines de seguridad y control de acceso que agrega las funciones de extracción y coincidencia del descriptor facial.</p>

Características Generales o equivalentes	<p>Un descriptor de rostro es un conjunto de características que describen el rostro, invariante para la transformación del rostro, el tamaño u otros parámetros. La coincidencia de descriptores faciales permite juzgar con cierta probabilidad si dos imágenes faciales recibidas pertenecen a la misma persona.</p>
	<p>Contar con la opción de uso típicos para 68 puntos de referencia para la segmentación y la estimación de la postura de la cabeza.</p>
	<p>Deberá contar con una precisión de la estimación de género del 99,8%.</p>
	<p>Interpretación amplia de la manifestación de ciertas emociones: Enfado, asco, temor, felicidad, sorpresa, tristeza y neutral.</p>
	<p>Deberá ser una exclusiva arquitectura modular unificada que permitan el alojamiento y la gestión simultánea de casos de reconocimiento e identificación de rostros de uso múltiple en prácticamente cualquier Framework.</p>
	<p>Capacidad para la recopilación de datos sobre el tráfico de clientes, ingreso, edad, sexo e incluso el estado emocional permiten detectar y segmentar la tendencia del publico visitante.</p>
	<p>El algoritmo de analítica de reconocimiento facial también deberá ser instalado en el ítem 1 (Cámara Tipo 1: Procesador de captura y procesamiento de imagen preparada para integración, Inteligencia Artificial y Deep Learning) en un contenedor tipo Docker en el propio hardware para lograr el procesamiento en el borde.</p>
	<p>El sistema de biometría facial, detección de rostro y reconocimiento deben estar integrados nativamente en la plataforma de gestión de video solicitada en los ítems 10 y 11(Licencias Tipo 1: Servidor Remoto, Licencias Tipo 4: Servidor Centralizado). deberá estar integrado por API con el sistema de KYC de lectura de cedulas de identidad y/o documento equivalente, también deberá estar integrado por API con el sistema de gestión de control de acceso de los molinetes de flujo rápido, para que de esta manera, una vez registrado en el sistema, las autenticaciones serán por el hardware de procesamiento de imagen ítem 1 (Cámara Tipo 1: Procesador de captura y procesamiento de imagen preparada para integración, Inteligencia Artificial y Deep Learning) 1:N liberando o no el acceso o generando alarmas de acuerdo a los registros en la base de datos e inteligencia.</p>
	<p>El procesamiento de la analítica Facial no debe usar GPU (no hacer uso o trabajar por el procesador GPU de la placa de video).</p>
	<p>Para cámaras remotas no deberá usar más de 0.5 mb x cámara.</p>
Características específicas o equivalente	<p>Deberán ser licencias de único pago, perpetua e ilimitada para la cantidad de cámaras instaladas y conectadas al sistema.</p>
	<p>Sin limitación de cámara para el reconocimiento facial (la limitación esta únicamente por la capacidad del hardware). Integración nativa con el sistema de video y sistema de control de acceso.</p>
	<p>La plataforma deberá asentar 1.000 registros de reconocimiento facial en la base de datos del servidor, valido para todas las camaras activas del sistema.</p>
	<p>La tecnología de reconocimiento facial ofertada deberá contar con aprobación del NIST (National Institute of Standards and Technology) (FRVT), precisión superior al 99% o norma similar y equivalente o.</p>
	<p>El servidor de gestión de datos biométricos deberá estar disponible en todas las cámaras del alcance de este proyecto con las siguientes prestaciones:</p>
	<p>Identificar grupos de visitantes. Identificar ruta de los visitantes. Identificar tiempo de espera.</p> <p>Estimar la edad, género, emociones. Detección de rostro.</p> <p>Extracción de descriptores faciales.</p> <p>Almacenamiento de descriptores faciales y búsqueda rápida. Agrupación lógica del descriptor facial.</p> <p>Descriptor facial 1: 1, 1: N y N: N coincidencia.</p>



Estimación de atributos faciales (por ejemplo, género, edad y emociones).

Registro de eventos de coincidencia de rostros y generación de notificaciones.

Deberá contar con herramienta para la detección y el seguimiento de rostros en múltiples fuentes. Permite al usuario elegir las imágenes faciales más adecuadas para reconocimiento facial de una secuencia de fotogramas de vídeo.

Características constructivas o equivalentes

API tiene la capacidad de integrarse a cualquier software y hardware de Video Vigilancia modernizándolo con Algoritmos de Inteligencia Artificial.

#### ITEM 13

#### Licencias de Integración y Automatización de Flujos Modalidad instalación

Características Generales o equivalentes

La plataforma LOW-CODE de multi integración y automatización de flujo de trabajo deberá ser una herramienta basada en nodos, distribuida bajo el modelo de software libre y abierta (Commons Clause) de código justo.

La herramienta deberá dar opciones de mover y transformar datos entre diferentes aplicaciones y bases de datos de manera rápida, sencilla y sin quedar atrapado en documentos API y solucionar errores de C.O.R.S. (Cross-Origin Resource Sharing).

Descripción general del nodo

Los nodos son los componentes básicos de los flujos de trabajo de la herramienta. Son un punto de entrada para recuperar datos, una función para procesarlos o una salida para enviarlos. El proceso de datos incluye filtrar, recomponer y cambiarlos. Puede haber uno o varios nodos para cada API, servicio o aplicación. Puede conectar varios nodos, lo que permitirá crear con ellos, flujos de trabajo simples y complejos de forma intuitiva.

Características específicas o equivalente

Integraciones

Deberá estar disponible para más de 200 integraciones (nodos) diferentes que le permitirá conectar varios servicios existentes y crear nuestros flujos de trabajo de automatización entre aplicaciones o dentro de la misma aplicación, además deberá contar con ejemplos de flujos de trabajo automatizado.

Prestaciones de esta herramienta

Nuevas u todas las integraciones que no sean nativas entre sistemas, se deberán hacer a través de esta herramienta.

Deberá ser auto hospedado, fácilmente ampliable e incluso utilizable con herramientas internas.

La herramienta LOW-CODE de integración y automatización de flujo de trabajo deberá ser ejecutada en un servidor local.

El oferente deberá proveer toda la documentación para la creación de nuevas integraciones (nodos) personalizados.

Características constructivas o equivalentes

La plataforma deberá ser instalada, configurada y mantenida para su instancia de operación.

OAuth administrado para autenticación.

La herramienta contará con actualizaciones sencillas a las versiones más recientes sin costos adicionales. (Commons Clause) de código justo

La modalidad de entrega de esta herramienta será: licencia Commons Clause de código justo, la instalación, documentación y su respectivo entrenamiento.

#### ITEM 14

#### Sistema de Control de Acceso

Características  
Generales o  
equivalentes

Sistema de control de acceso y credenciales con gestión integrada en una única plataforma, con las siguientes prestaciones:

Multi-Idioma: en español como lengua principal. Capacidad de Gestionar de Acceso y Seguridad. Capacidad de Gestionar Porterías y Visitantes. Capacidad de Gestionar Tercerizados y Aliados.

Capacidad de Control de EPI para Colaboradores, Visitantes y Tercerizados. Capacidad de Gestionar el Control de la Flota de Vehículos.

Deberá estar integrado con la plataforma de gestión de videovigilancia ofertada en el ítem 10 y 11 (Licencias Tipo 1: Servidor Remoto, Licencias Tipo 4: Servidor Centralizado).

Con capacidad de controlar registros de tarjetas y biometría.

Deberá estar integrado con la plataforma de gestión de biometría facial ofertada en el ítem 12 (Biometría Facial, registro de Licencia Perpetua, pago único, ilimitadas cámaras de analítica facial).

Capacidad de Monitoreo y prevención de salud por Reconocimiento Facial: Temperatura, el uso de Mascaras.

Deberá ser Arquitectura 100% Web.

Contar con transmisión segura de datos Http sobre SSL.O Transmisión de Datos y páginas encriptadas.

Rastreo y auditoría con logs protegidos. Gestión de Usuarios vía Active Directory.

Disponible para servidores dedicados con opción de Cloud. Uso de Token para ambientes críticos conformidad con las leyes vigentes que reguan el manejo de datos y LGPD

Capacidad de Integración con Sistema de Gestión Empresarial (ERP) del SNPP (Sistemas, aplicaciones y productos para el procesamiento de datos.) por API.

Sistema de control de acceso y credenciales con gestión integrada

La solución de seguridad integrada deberá cumplir los siguientes criterios:

El software debe ser compatible con varias tecnologías de seguridad, como ser: Subsistema de control de acceso, subsistema de supervisión por imágenes, subsistema de detección de incendios, gestión de la identificación, gestión de alarmas, gestión de las puertas de entrada, control de los activos, gestión de la frecuencia, gestión y supervisión de los vehículos, reconocimiento facial, lectura e identificación de las matrículas de los vehículos, automatización y gestión de los servicios públicos.

El sistema debe ser una solución de seguridad con recursos avanzados que garanticen la asistencia, el apoyo operativo y estadístico a todas y cada una de las situaciones, en áreas internas, externas o remotas (en cualquiera de las sedes del SNPP establecidas a nivel Nacional), supervisadas en tiempo real o no, localmente y a distancia. Otro aspecto importante que deben observar los oferentes es, que la solución tendrá que ser integrada con las tecnologías disponibles en nuestros subsistemas, es decir, que las soluciones establecidas como el Sistema de Monitoreo de Vídeo Vigilancia, entradas, alarmas, intrusión e incendio, tengan una estrecha interrelación y puedan intercambiar información entre sí de forma totalmente full dúplex,

permitiendo generar acciones y reacciones instantáneas y coordinadas, proporcionando información correcta y eficaz a los administradores de la solución y dentro del marco de la observancia y el cumplimiento de las normas y reglamentos técnicos necesarios para el correcto y fiel cumplimiento de este objetivo.

En particular, con respecto a las características del software destinadas al control de acceso, así como toda la línea de dispositivos de control debe ser ofertado para leer y escribir tarjetas inteligentes - Mifare®, sin contacto, ISO 14443A, que permite la inserción de datos biométricos (huella digital) para la validación positiva en los puntos de control considerados de alta seguridad, lo que permite una ganancia en la flexibilidad en la operación, sin degradar el rendimiento y el bajo costo de la gestión de la información.

Los dispositivos para la lectura de tarjetas deben funcionar sin necesidad de realizar consultas al servidor para validar la información leída, por lo que las tarjetas de identificación deben llevar toda la información necesaria para validar el acceso. La solución ofertada deberá ser potente, es decir, tanto el hardware como el software de control de accesos deben soportar tarjetas de las siguientes tecnologías:

\* tarjeta de código de barras, \* código de barras 2D, \* bandas magnéticas, \* Qrcode,

\* RFID 125 Khz abatrack y wiegand de proximidad, \* tarjetas inteligentes Mifare®,

\* tarjetas inteligentes de contacto, \* tarjetas inductivas,

\* también activaciones por contraseña numérica, y cada tecnología puede o no combinarse con validación biométrica en la forma 1:1 o 1: N.

La solución también debe soportar la lectura y escritura en tarjetas de tipo PKI las tarjetas con triple tecnología, es decir, tarjeta inteligente Mifare®, tarjeta inteligente con chip de contacto y RFID 125 Khz.

Para las tarjetas PKI, debería ser posible leer los datos biométricos en los dispositivos AFIS. (Sistema de Identificación Automática por Huellas Digitales -AFIS - Automated Fingerprint Identification Systems por sus siglas en inglés).

Funciones de los dispositivos de control de acceso a la plataforma

Para cumplir con el sistema propuesto el software, entre otras características específicas, debe disponer, ya en su versión nativa, cuanto sigue:

Debe presentarse en un menú con funciones y subfunciones por ítems cuya finalidad será incorporar datos para que el sistema pueda alimentarse de todo tipo de información posible y necesaria, y a partir de esta información, proveer el monitoreo y la gestión de acceso y seguridad;

La solución debe ser completamente jerárquica, permitiendo la creación de perfiles de acceso para cada tipo de usuario, es decir, operador de conserjería, administradores, operador de registro, operador de seguridad, operador de CCTV, etc.

El administrador principal de la solución podrá restringir los elementos accesibles en el menú de cada usuario, aunque pertenezcan a la misma clase, sin embargo, cualquier liberación o restricción debe ser almacenada en un registro de auditoría para ser recuperada a través de perfiles de filtro e informes.

Además de los registros relacionados con los cambios en los perfiles de acceso al sistema, el software debe contar con registros de auditoría de las acciones realizadas en el sistema por los usuarios registrados, y se puedan

emitir informes a través de filtros específicos.

Debe trabajar en diferentes frentes de seguridad, como el monitoreo de alarmas de incendio, la gestión de imágenes, la gestión de flotas, el control georreferenciado de personas, el control de accesos, la RFID, el monitoreo web móvil, la manipulación y la intrusión, así como la gestión de estas alarmas en modo manual y automático.

Permitir la visualización de imágenes en tiempo real de las zonas controladas. Obtener grabaciones de los momentos desencadenantes de los sucesos.

Ajustes de la cámara controlados según las necesidades de la imagen (zoom y dirección).

En este caso, al buscar un acceso concreto, el software debe traer el clip de vídeo asociado a él, lo que debe permitir ver la imagen de quién ha accedido a un punto de control determinado, ya sea una puerta, un molinete o una barrera vial.

El software debe disponer de recursos para controlar el tiempo de apertura de la puerta, generando alarmas cuando el tiempo de apertura es superior al establecido, intentos de robo e intentos de acceso indebidos.

El software debe permitir verificar la fecha/hora y el lugar del acceso realizado por el propietario de una tarjeta de identificación o registro biométrico - registro de auditoría (log Eventos).

También debe interactuar con el subsistema de CCTV ofertado en los ítems

10 y 11 (Licencias Tipo 1: Servidor Remoto, Licencias Tipo 4: Servidor Centralizado) para la recuperación de las imágenes correspondientes a cada evento de acceso generado, de las alarmas relacionadas con la detección de imágenes y también de las alarmas relacionadas con la intrusión de acceso.

Debe permitir el registro, en una base de datos para su auditoría, de "todos los eventos", a saber: eventos de control de apertura de puertas autorizados, no autorizados, y eventos administrativos (como la creación de un nuevo usuario, por ejemplo, operador, etc.);

Según el nivel de seguridad, debe ser posible, en determinados puntos de acceso restringido, operar con doble tecnología: - identificación y/o validación positiva (mediante la lectura de la tarjeta de identificación y la biometría de las huellas dactilares o facial).

La tecnología dual, no debería interferir en los tiempos de respuesta del sistema ya que los datos de validación biométrica formarán parte de los datos incorporados en las tarjetas de identificación "Smart Card".

Los datos biométricos estarán nativos o integrados a la base de datos del sistema de gestión de biometría facial ofertado en el ítem 12 (Biometría Facial, registro de Licencia perpetua, único pago, ilimitadas cámaras de analítica facial) recibiendo mínimamente estos datos:

Detección de rostro.

Extracción de descriptores faciales.

Almacenamiento de descriptores faciales y búsqueda rápida. Agrupación lógica del descriptor facial.

Descriptor facial 1: 1, 1: N y N: N coincidencia.

Estimación de atributos faciales (por ejemplo, género, edad y emociones).

Función de pánico o coacción

Los puntos de acceso bajo control de identificación biométrica deben prever la implementación de la función "biometría de pánico";

La Biometría del Pánico" se configura en la opción de utilizar una biometría alternativa a la normal para el acceso, pero en este caso generando un evento como alarma de pánico al centro de monitoreo, movilizándolo el protocolo de seguridad y consecuentemente el equipo de seguridad para

que acudan al lugar donde se encuentra el usuario bajo coacción, pero aun liberando el acceso a la puerta.

La ejecución de esta compleja función, el sistema de gestión de datos biométricos deberá contar con estimación de atributos faciales precisamente interpretaciones amplias de emociones, en la práctica es entrenar una expresión facial de la manifestación que corresponde a una emoción (el pánico) previamente entrenada y envía como evento al sistema de gestión de acceso.

Cada imagen debe ser registrada con fecha, hora y lugar de origen.

Las imágenes deben localizarse a través de una búsqueda con parámetros de fecha, hora o lugar y enviarse por correo electrónico a un destinatario registrado.

Debe permitir la importación y exportación de datos de sistemas heredados con procesos automáticos configurados en la aplicación a través de archivos con interfaces definidas.

Además de los datos personales, el SOFTWARE debe ser capaz de exportar datos para controlar los horarios de trabajo, las tolerancias de tiempo de acceso.

Debe utilizar la tecnología TCP-IP para controlar a las personas en las zonas supervisadas y restringidas al acceso común.

Para equipos integrados, en una sola terminal de control debe ser posible controlar hasta 24 sensores (de presencia, activos, pasivos, magnéticos y de vibración) y 1 Mb de memoria total.

Con los equipos integrados al sistema en caso de fallo de la comunicación (en la red de datos o en la red eléctrica), los terminales deben funcionar sin conexión y en este modo deben disponer de inteligencia distribuida que trabaje con listas de liberación o bloqueo, garantizando el acceso seguro de las personas autorizadas.

La seguridad interna del sistema (datos e información) debe mantenerse mediante perfiles de acceso y contraseñas y credenciales configurados durante la instalación del producto.

El software debe ser inmune al fraude, ya que la información debe estar encriptada en la base de datos, que se suministrará junto con el software de control.

El software debe tener una interfaz intuitiva y amigable, con excelente navegabilidad y presentación, y el monitoreo de eventos no autorizados con generación de alarmas en una pantalla gráfica, a través de mapas gráficos de las instalaciones de la SNPP, debe ser parte integral de la solución ofertada.

El software debe tener archivos de ayuda individuales dentro de cada aplicación que informen sobre el funcionamiento específico de cada pantalla. Estas ayudas deben ser accesibles en todo momento cuando surjan preguntas sobre el registro, en la barra de navegación principal del sistema. (deberán estar en idioma español).

Como elemento de seguridad de la solución, el SNPP solicita, como requisito indispensable, que el software esté protegido contra copias indebidas a través de un dispositivo físico, y que disponga de una herramienta web para el control de versiones, emisión de actualizaciones y cuestiones relacionadas.

Debe ser posible registrar varias clases de usuarios, nuevos empleados, aprendices, visitantes, terceros, visitantes especiales (con largos periodos de acceso frecuente y consecutivo), pudiendo registrarse unitariamente y/o en grupos, incluso mediante rutinas específicas de importación de datos vía XML, CSV, archivos txt y vía base de datos o de la API a la Plataforma LOW- CODE de multi integración y automatización de flujo de trabajo.

Emitir informes de acceso, utilizar planos de las áreas del SNPP (que se

implementarán en el sistema) para monitorear los ambientes, etc.

El software debe tener un módulo de gestión para ser utilizado por el administrador del sistema, que podrá supervisar el acceso a las instalaciones del SNPP, así como extraer informes y configurar los equipos a través de su interfaz.

Debe tener el reconocimiento facial integrado con el sistema de control de acceso, lo que permite activar el dispositivo de control de la puerta a través de la biometría facial del usuario o recibir algún evento como el pánico biométrico u otros.

Como condición fundamental para las integraciones, las bases de datos de los dos sistemas (control de acceso y gestión de datos biométricos) deben permitir acceso total a la Plataforma LOW-CODE de multi integración y automatización de flujo de trabajo lo que dará total autonomía a la SNPP para crear nuevas integraciones y flujos de trabajo personalizables de acuerdo a las necesidades y las prestaciones de cada sistema u otros a futuro.

Debe conservar los historiales de toda la información de los empleados, manteniendo un registro desde la contratación hasta el despido de ese empleado.

Del mismo modo, debe mantener registros de todas las acciones realizadas en el sistema en las áreas de control que impactan en el proceso de configuración corporativa (reglas de negocio).

La seguridad interna del sistema (datos e información) debe mantenerse mediante perfiles de acceso y contraseñas (credenciales), configurados en la instalación del producto. Esta información debe ser encriptada antes de ser almacenada en la base de datos, para garantizar la seguridad de la información.

El sistema debe tener una interfaz intuitiva y amigable, con una navegabilidad y presentación óptimas.

El software debe ser una herramienta de trabajo que supervise los eventos en tiempo real.

El sistema debe utilizar tecnología y entorno 100% web, siendo necesario para su uso desde cualquier puesto de trabajo, únicamente un navegador.

Debe ser posible insertar planos de los lugares con los dispositivos de control colocados en ellos para una supervisión fácil e intuitiva, pudiendo interactuar con estos dispositivos.

Debe ser posible en la misma planta activar, desactivar, configurar, comprobar si está en línea o fuera de línea, insertar y quitar, etc. todos los dispositivos que son controlados por el software a través de las plantas.

El software debe tener una interfaz para el registro de usuarios, nuevos usuarios, visitantes y vehículos.

Debe permitir la programación de visitas a través del sistema vía web, es decir, sin necesidad de utilizar un software cliente, con opciones de reprogramación, rescate de vistas anteriores y módulo de visualización y control de vistas programadas.

Debe tener un módulo compatible con tótem de autoservicio, para generar tarjetas de visita, emitir QRcode, asignar credencial al rostro, emitir tarjetas temporales para empleados, servidores, terceros o cualquier otro tipo de personas gestionadas por el sistema. También debe tener recursos para comprobar la foto de la persona y comprobar el QRcode recibido por correo electrónico por el usuario.

En cuanto a la gestión del acceso, el software debe tener:

1. Registro y almacenamiento en tiempo real de todos los intentos de acceso válidos y no válidos.
2. Control total de acceso y seguimiento de empleados, terceros, socios, candidatos y visitantes.

Definición y creación de políticas de seguridad, como días laborables y festivos, franjas horarias independientes para el control de acceso, registro horario y uso de comedores, incluida la gestión del crédito.

Trazabilidad con la gestión, el control de las rutas, los niveles de acceso y anti-pass-back.

Gestión de contratos de empresas subcontratadas, validando el acceso durante la vigencia del contrato y facilitando la recogida de credenciales en los molinetes al finalizar el contrato y el acceso de salida de los empleados de terceros - (empresas de seguridad, por ejemplo).

Ampliación de las franjas horarias para realizar la liberación de horas extras, autorizaciones de personas y salidas de visitantes.

Control de prestaciones, que permite gestionar la distribución de artículos como, por ejemplo, beneficios, bonos de transporte, premios, etc., incluyendo la carga y el control de los créditos a través de la tarjeta inteligente sin contacto.

Registro de control de persona no Grata lista negra, alertando en tiempo real, eventuales registros no deseados, por ej. Recibiendo el evento de un rostro o una chapa registrada en lista negra o una lista de seguimiento.

Gestión y distribución de los EPI para el control de las personas en áreas eventuales que deseen este tipo de control, bloquear el acceso de la persona en cualquier dispositivo cuando el EPI está vencido, proporcionando así una mayor gestión de la seguridad de la persona.

Sobre la gestión de flotas de vehículos, el software de control de acceso debe tener las opciones de:

Registro completo de vehículos, modelos, placas y otras opciones para controlar un vehículo.

Gestión del mantenimiento, seguro e historial de uso.

Flujo de trabajo para la solicitud de vehículos y cuando se aprueba, el usuario debe presentar su tarjeta y la tarjeta del vehículo para que la puerta se abra cuando se relacionan y se liberan.

Sobre la gestión de la identificación de las personas, el software de control de acceso debe tener:

Identificación biométrica: biometría dactilar, venas u otra en modo 1 a 1 o 1 a varios y la biometría de reconocimiento facial. El reconocimiento facial debe funcionar en modo 1: N (uno a muchos).

Más de un nivel de validación, en el propio controlador: Tarjeta de ID y contraseña.

Registro y contraseña. Credencial y biometría.

Credencial, biometría y contraseña.

Utilizando la tecnología de identificación de la tarjeta inteligente Mifare® tipo A4 Kb, tamiz de seguridad deben ser almacenadas en la tarjeta.

La gestión de las insignias físicas como tarjetas también debería permitir: Diseño de las insignias para su impresión.

Control de la ruta de la tarjeta. Insignias extraviadas.

Bloqueo y liberación de las tarjetas en línea.

Eliminación automática de las insignias a través del sistema o cuando el límite de tiempo expira.

En cuanto al uso de la biometría de las huellas dactilares, el software debe permitir:

Recoger y almacenar al menos dos dedos del usuario;

Biometría de la palma de la mano mediante la recogida y el almacenamiento de la geometría de la mano.

Biometría de la vena del usuario.

La biometría facial a través de la captura de rostros, su almacenamiento, comprobación e integración con el control de acceso, permite que un rostro registrado pueda ser comparado entre N otros en una base de datos y luego permitir la apertura o no de un controlador de acceso, deberá estar plenamente integrado al sistema de gestión de datos biométricos, su base de datos y como ya fue mencionado, de la API a la Plataforma LOW-CODE de multi integración y automatización de flujo de trabajo.

Módulo de control de doble factor de autenticación para entornos con un alto nivel de seguridad, tras la autenticación con tarjeta y/o biometría, el usuario debe introducir una clave y recibir una contra clave para confirmar en el controlador de acceso. Si hay coincidencia, el acceso será liberado.

Sobre el registro de visitantes debe tener el software de control de acceso:

Un módulo integrado y propio del sistema (no se aceptarán interfaces integradas de terceros u otro software que opere en paralelo), y el sistema debe permitir un número ilimitado de registros de puertas, todo vía web a través del navegador, sin que se cargue la tarea de solución para la administración de puertas de acceso de personas.

El módulo de portería tendrá las siguientes funciones, pero no se limitará a ellas:

Control, distribución e impresión de distintivos provisionales para empleados, terceros y otras clases de usuarios.

Control del material entrante y saliente de los empleados y visitantes. Control de guarda de equipaje y control de llaves.

Registro de ocurrencias.

Control de rutinas de revisión del personal de manera automática y automatizado de forma aleatoria a través de la programación realizada en los controladores de acceso y el software, mediante la generación de sirenas, lámparas o alarmas en el sistema.

Tarjetas de acceso para visitantes, acompañantes y grupos de visitantes.

La programación de las visitas puede ser realizada previamente por el propio visitado, garantizando una mayor agilidad a la hora de acreditar a un visitante o grupo de visitantes.

Seguimiento en línea del acceso de los visitantes.

Captura de la foto del visitante, anverso y reverso del documento a través de la webcam o dispositivo de captura KYC, posibilidad de integración automática con escáner para la captura de documentos.

Búsqueda en la base de datos de visitantes a través de múltiples documentos, CI, pasaporte, registro de conducir, tarjeta de entidad profesional, etc.

Control de la estancia del visitante por día, fecha y hora de validez con control de los lugares a los que puede acceder el visitante.

Definición de control de visitas, visitas especiales y visitas que deben introducir los distintivos en una posible caja fuerte (boca de lobo) para su recogida a la hora de salida.

Control de los EPI de los visitantes.

Impresión de insignias, según el diseño definido, así como código de barras

encriptado.

Registro de todos los accesos de los visitantes, intentos de acceso, válidos y no válidos.

Captura de la huella dactilar del visitante en el momento de la acreditación, si el visitante utiliza el acceso biométrico.

Tras el registro y/o la programación, el software debería enviar automáticamente un correo electrónico al visitante con la información de la visita y su QRcode de acceso.

En cuanto a la gestión de alarmas y plantas, el software debe permitir:

Utilizando el plano del lugar vigilado, el software debe gestionar los eventos de acceso y las alarmas de forma sencilla.

Manejo y reconocimiento de eventos de alarma y acceso.

Debe mostrar el vídeo en el momento de la ocurrencia permitiendo también la visualización en directo de la imagen de la escena.

Debe tener un sistema de sonido a través de archivos de onda pregrabados en el software.

Debería ser posible establecer la prioridad de visualización de las alarmas.

Debe ser posible enmascarar las alarmas no controladas definidas por franjas horarias.

Debe ser posible configurar reacciones automáticas a eventos de alarma y acceso, como la activación de la sirena o el envío de un correo electrónico.



Debe ser posible configurar la redirección y el zoom automático en la ubicación de la ocurrencia del evento en la planta.

Debe ser posible configurar la ejecución de comandos directamente desde la planta, como, por ejemplo, la liberación de controladores para abrir puertas o el desbloqueo de molinetes para situaciones de emergencia.

Debe ser posible reconocer y gestionar las alarmas de forma individual o por grupos.

Debe ser posible consultar e informar de las alarmas tratadas, reconocidas o no tratadas.

Deberá ser posible realizar consultas de acceso vinculadas con la hora del evento de acceso o de la alarma y mostrar la reproducción de vídeo. Dicho flujo de vídeo puede ser tomado en cualquiera de los siguientes 2 formatos de compresión, MPEG4, H.264, flujos de vídeo múltiples.

Debería ser posible vincular las cámaras a los controladores o dispositivos de alarma.

Debería ser posible identificar el último lugar donde entraron las personas.

Debe ser posible realizar consultas e informes de personas presentes y ausentes con detalles y totales.

Debe ser posible consultar e informar de los accesos válidos e inválidos de las personas, aunque cambien de placa en determinados periodos.

Debe posibilitar la realización de controles de accesos supervisados y simultáneos, es decir, para entrar en un determinado lugar sólo pueden acceder simultáneamente dos usuarios previamente registrados y autorizados.

Debe ser posible realizar el acceso con un número máximo y mínimo de usuarios, es decir, sólo se puede acceder a determinados lugares si un cierto número de usuarios, previamente determinado, entra y sale del respectivo nivel de control. Por lo tanto, si un lugar en particular se registra en el sistema para esta función, el mismo número de personas que entran en el sitio debe ser el mismo número de personas a salir, y la liberación de acceso tanto en la entrada y la salida se concede después de la verificación de la biometría y / o tarjeta de identificación, el número de usuarios definidos.

El software debe tener integración con el Active Directory de Windows y por tanto, cada usuario registrado para esta funcionalidad sólo puede entrar en su puesto de trabajo cuando haya superado el control de acceso o el nivel de control de acceso predeterminado en el sistema.

El software debe ser 100% tecnología web y ofrecer características como: Actualización centralizada de datos (Base de datos y aplicación).

No es necesario instalar el cliente en las estaciones de trabajo de operación, supervisión y administración.

Posibilidad de acceder al software en el lugar donde está instalado o, a distancia, desde un punto con conexión a Internet, siempre que el inicio de sesión se realice mediante ambiente seguro, uso autenticado y contraseña.

Utilización a través de Intranet y Extranet, VPN. Mantenimiento del sistema a distancia.

El software debe utilizar la protección de datos del cliente mediante certificado digital (HTTPs).

Debe utilizar un dispositivo de bloqueo hard lock como HASP (Hard lock o traba de Hardware) para proteger el sistema en versiones físicas o virtuales.

Instalación en servidor virtual.

Debería ser posible acceder a ello al menos a través de los navegadores Internet Explorer 8 o FireFox 1.5.0 o superior.

Debe utilizar las siguientes plataformas tecnológicas:

Servidor web: Apache. o similar

Servidores Linux o Windows: 2000/XP/2003 o superior. Base de datos: Oracle 9i o SQL 2000 o superior.

El software de grabación y gestión, integrado en la plataforma de seguridad, debe cumplir las siguientes especificaciones:

Debe ser de alto rendimiento, con un funcionamiento fácil de usar, con alarmas en la pantalla, y controles, menús y otras acciones a las que se accede a través del ratón.

Debe permitir la integración a través de la red TCP/IP con otros módulos de grabación en otras unidades y también permitir la visualización remota a través de Internet.

Debe contar con recursos de distribución y escalabilidad que garanticen que la comunicación con los controladores de acceso a puertas, torniquetes, puntos electrónicos y aparcamiento se realice en línea, de forma rápida, sin generar colas, pudiendo estar distribuida por regiones, sedes y/o otras formas de distribución.

Debe tener una interfaz para insertar planos o mapas de los lugares vigilados, con las respectivas cámaras posicionadas, para mayor facilidad y control de las funciones de gestión, aumentando la eficiencia y la respuesta con acciones de contingencia.

Debe presentar las alarmas de forma jerárquica al operador encargado de la supervisión, es decir, clasificando las alarmas en niveles de criticidad alta, media y baja. La asociación de los niveles de criticidad a cada evento relacionado con los puntos controlados se definirá en el proyecto ejecutivo y según las necesidades del Contratista.

Activará un evento de alarma, automáticamente, cuando:

Un objeto dejado en un punto de vigilancia de la cámara se identifica según un tiempo que puede parametrizarse en el software.

Intento de acceso indebido a través de barreras y cerco perimetral.

Además de generar el evento de alarma, el modo de grabación se activará a una velocidad máxima de 25 FPS.

Recursos de integración con las otras plataformas del Sistema Integral de Control Inteligente:

Debe tener un WebService para la integración con el software heredado.

Debe tener la posibilidad de poder integrarse con la plataforma SAP sin necesidad de ninguna personalización, teniendo en cuenta las necesidades futuras, debe permitir acceso dúplex para la generación y ejecución de flujos de trabajo a través de la API a la Plataforma LOW-CODE de multi integración y automatización de flujo de trabajo, sin necesidad de programación.

Debe disponer de recursos para compartir la información de los registros de acceso y las alarmas sin necesidad de acceder directamente a la base de datos, de forma que el usuario pueda crear el diseño necesario del archivo y crear horarios a través de un software para exportar la información.

Funcionalidades de Sistema de alarma y detección de incendios de la plataforma S.D.A.I.

La plataforma debe tener integradas las funciones de detección y alarma de incendios, y debe estar integrada de tal manera que la detección de la presencia de llamas, humo o calor, por cualquiera de los módulos sensores existentes, debe permitir la apertura de puertas, molinetes, portones y otros dispositivos de control de acceso del sistema según la configuración realizada cumpliendo con la norma NFPA101 u otras .

La solución deberá interpretar los sensores, panel de control de incendios, teclados, disparadores manuales, luces de emergencia y otros dispositivos relacionados con el sistema.

La solución S.D.A.I debe proporcionar un módulo de detección y alarma de incendios basado en imágenes, aprobado y certificado por UL y FM, de acuerdo con las especificaciones mencionadas a continuación.

El sistema proporcionará una arquitectura digital, basada en microprocesadores, inteligente y modular, con verdadera comunicación entre pares para la alarma y el control de incendios.

Debe diseñarse con una amplia gama de variables parametrizables, permitir la transmisión casi instantánea de información y la capacidad de realizar tareas de gestión de procesos, como la evacuación por voz, la desconexión del sistema de aire acondicionado, el control de las compuertas, las puertas, los ascensores, la seguridad, la CCTV y la interfaz con los sistemas de gestión de edificios.

#### ITEM 15 Molinete Tipo 1, por Pasaje de Flujo Libre

Deberá ser un molinete de doble paso, fabricado para alto flujo de personas y trabajar en la modalidad de flujo libre, siempre abierto, en caso de intento de paso sin autenticar, el cierre será automático.

Pasillo de 90 a 110 cm (PNE).

Deberá funcionar en modalidad unidireccional y bidireccional con la posibilidad de bloquear una sola solapa o una doble solapa.

Deberá tener incorporado un lector integrado a la base de datos y facial para la validación del acceso y asociación con el rostro.

Compatible con los principales lectores del mercado. Tarjeta inteligente Proximidad.

Biometría facial - Biometría digital.

Código QR Bares, podrá trabajar en modo bloqueado (cerrado). Tiempo de apertura y cierre de 1s.

Función antideslizamiento.

Sensores infrarrojos para el control del flujo con aletas giratorias con solapas giratorias.

Alarma por intento de fraude y por hacer dedo.

Control de flujo por visión artificial, que permite bloquear a los usuarios no autorizados.

Interfaz para la integración con la central de incendios. Central de alarmas contra incendios.

Orientación mediante pictogramas luminosos en ambas direcciones. Aviso sonoro de acceso permitido y denegado.

Configuraciones del corredor PNE.

Memoria de almacenamiento 8GB. Sistema de protección contra la caída. No hay rotura integrada en el equipo.

Autonomía en caso de fallo de alimentación 4hs. Permitir la instalación de baterías externas adicionales. Comunicación

Interfaces ethernet 10/100 Mbps. Tipo de lectores compatibles

Tarjeta inteligente Mifare (sin contacto). Proximidad (ABA y Wiegand).

Biometría facial (externo). Código QR (opcional).

Biometría de dedo.

\* Huella dactilar. \* Resolución 500 dpi.

\* Tipo de consulta 1:1 y 1:N.

Características  
Generales o  
equivalentes

Características  
específicas o  
equivalentes

Características constructivas o equivalentes	* FRR (tasa de falsos rechazos) 0,001.
	* FAR (Tasa de falsa aceptación) 0,00001%. * Número de usuarios 5000.
	Opción para instalación de dispositivo de seguridad para la recogida de insignias.
	Luces indicadoras Pictograma RGB. Indicador de sonido de audio.
	Vigilancia del funcionamiento de WachtDoG. Operación
	Modo de funcionamiento en línea y fuera de línea.
	Mueble de acero inoxidable. Gabinete delgado.
	Solapas de acrílico o policarbonato con personalización del logotipo del SNPP.
	Motor de bajo consumo, con velocidad programable, acelerando o desacelerando la apertura y el cierre de las solapas.
	Armario de acero inoxidable.
ITEM 16	Fuente de alimentación de 90 a 240 VAC.
	Dimensiones de altura X anchura X profundidad (mm) 990 x 180 x 1200.
	<b>Molinete Tipo 2.</b>
	Deberá ser un molinete de paso simple (una sola solapa) fabricado para alto flujo de personas y trabajar en la modalidad de flujo libre, siempre abierto, en caso de intentar pasar sin identificarse, el cierre será automático.
	Pasillo de 50 a 70 cm.
	Deberá funcionar en modalidad unidireccional y bidireccional con la posibilidad de bloquear la solapa.
	Deberá estar incorporado un lector de documentos con función OCR integrado a la base de datos y facial para la validación del acceso y asociación con el rostro.
	Compatible con los principales lectores del mercado. Tarjeta inteligente Proximidad.
	Biometría facial - Biometría digital. Código QR.
	Tiempo de apertura y cierre de 1 seg. Función antideslizamiento.
Características Generales o equivalentes	Sensores infrarrojos para el control del flujo con aletas giratorias con solapas giratorias.
	Alarma por intento de fraude.
	Control de flujo por visión artificial, que permite bloquear a los usuarios no autorizados.
	Interfaz para la integración con la central de incendios, de alarmas contra incendios.
	Orientación mediante pictogramas luminosos en ambas direcciones. Aviso sonoro de acceso permitido y denegado.
	Configuraciones del corredor.
	Memoria de almacenamiento 8GB.

Características específicas o equivalentes	Sistema de protección contra la caída de personas. Autonomía en caso de fallo de alimentación 4hs. Permitir la instalación de baterías externas adicionales. Comunicación
	Interfaces ethernet 10/100 Mbps. Tipo de lectores.
	Tarjeta inteligente Mifare (sin contacto). Proximidad (ABA y Wiegand).
	Biometría facial (externa). Código QR (opcional).
	Biometría del dedo.
	* Huella dactilar. * Resolución 500 dpi.
	* Tipo de consulta 1:1 y 1: N.
	* FRR (tasa de falsos rechazos) 0,001.
	* FAR (Tasa de falsa aceptación) 0,00001%. * Número de usuarios 5000.
	Opción para instalación de dispositivo de seguridad para la recogida de insignias.
Características constructivas o equivalentes	Luces indicadoras Pictograma RGB. Indicador de sonido Audio.
	Vigilancia del funcionamiento de WachtDoG Operación
	Modo de funcionamiento en línea y fuera de línea.
	Mueble de acero inoxidable, gabinete delgado.
	Solapa de acrílico o policarbonato con personalización del logotipo del SNPP.
	Motor de bajo consumo, con velocidad programable, acelerar y desacelerar la apertura y el cierre de la solapa.
	Fuente de alimentación de 90 a 240 VAC.
	Dimensiones de altura X anchura X profundidad (mm) 770 x 180 x 1200

#### ITEM 17 Barreras de Acceso Alto Flujo

Características Generales o equivalentes	Dispositivos de bloqueo vehicular ultra rápido tipo barrera con brazo móvil.
	Deberá ser exclusivamente destinada al uso para el cual ha sido expresamente diseñado y fabricado. Cualquier uso diferente será considerado peligroso. La barrera automática deberá ser un equipo proyectado para ser utilizada en aparcamientos públicos o privados, o en zonas con mucho tránsito de vehículos.
	La seguridad del producto y por consiguiente su instalación correcta están supeditadas al respecto de las características técnicas y a las modalidades correctas de instalación con arreglo a la maestría, seguridad y conformidad de uso indicadas expresamente en la documentación técnica del fabricante y las respectivas integraciones en el uso de los componentes de automatización.
	Estar fabricada en concordancia a la norma de gestión de calidad, ISO 9001 y medioambiente ISO 14001, o similar.
	Este producto deberá cumplir con las normas vigentes mencionadas en la declaración de conformidad del fabricante.
	Eléctricas:
	Alimentación: (V - 50/60 Hz) 120 - 230 AC. Alimentación motora: (V) 24 DC. Absorción: (A) 15 máx.

	Potencia: (W) 300. Funcionamiento Par (Nm) :200.
	Tiempo de apertura: a 90° (s) 0,9 ultra rápido. Intermitencia/Funcionamiento: SERVICIO INTENSIVO. Temperatura de funcionamiento: (°C) -20 ÷ +55.
	Relación de reducción :(i) 1/202. Clase de aislamiento: I.
	La Central de mando de la barrera. Funciones mínimas necesarias.
	Función stop total (1-2).
	Función asociada con la entrada CX. Función asociada con la entrada CY. Función prueba de seguridad.
	Función acción mantenida. Modalidad de mando en 2-7.
	Función detección obstáculo con motor parado. Función luz testigo.
Características específicas o equivalentes	Función de parpadeo del cordón luminoso. Tiempo cierre automático.
	Tiempo parpadeo previo. Tiempo de funcionamiento.
	Regulación de la velocidad en apertura.
	Regulación de la velocidad en cierre.
	Regulación de la velocidad de ralentización en apertura. Regulación de la velocidad de ralentización en cierre.
	Regulación de la velocidad de calibración. Sensibilidad durante el movimiento.
	Sensibilidad durante la ralentización.
	Regulación del punto inicial de ralentización en apertura. Regulación del punto inicial de ralentización en cierre.
	Tipo de mando que asociar con el usuario mediante mando radio. Borrado de un usuario.
	Borrar todos los usuarios. Prueba del motor.
	Calibración de la carrera. Reseteo parámetros de fábrica.
	Conteo del número de maniobras.
	Ajuste de sensibilidad de los sensores por inducción de piso. Configuración del tipo de mástil.
	La comunicación de la central de mando integradas a la barrera deberá ser directa con el bus de datos en full dúplex a los DISPOSITIVOS DE CONTROL DE ACCESO del ítem 18 (Control de Acceso IP Multi Tecnología), que a su vez se comunicaran por IP con el software control de acceso y credenciales con gestión integrada del ítem 14 (Sistema de Control de Acceso).
Características constructivas o equivalentes	La Barrera deberá estar fabricada de acero galvanizado con pintura epoxi. Brazo de aluminio de 4 a 6 metros.
	Peso aproximado 50 kg. Grado de protección: (IP) 54.
	Apoyo fijo para el brazo: parte del kit 1.3 mts.
	Si los cables tienen una longitud distinta con respecto a la indicada por el fabricante, hay que determinar la sección de los cables con arreglo a la absorción efectiva de los dispositivos conectados y según lo establecido por la normativa PY. NP 2 028 13.
	Instalación.

Preparar un encofrado de dimensiones mínimas 36x50x50cm para la base de la barrera.

Poner una rejilla de hierro dentro del encofrado para armar el cemento. Acoplar las cuatro grapas de anclaje a la placa de fijación.

#### ITEM 18 Control de Acceso IP Multi Tecnología.

##### DISPOSITIVOS DE CONTROL DE ACCESO

Características de los equipos de control de acceso IP Multi Tecnología:

Los dispositivos deben tener características de tecnología biométrica añadidas a los terminales.

El Gabinete debe estar protegido contra el acceso indebido, el vandalismo y estar provisto de tornillos de fijación resistentes. También debe contar con un sensor de apertura del armario, que debe generar un código de alarma

cuando se produzca un intento de apertura indebida de acceso interno al armario del equipo, no autorizado previamente.

El terminal debe tener la opción de instalarse en un armario de plástico u otro material con un simple cambio de caja, sin necesidad de cambiar los módulos internos.

El terminal dispositivo de datos también debe tener una aplicación para los sistemas de control de frecuencia, haciendo que los datos recolectados estén disponibles para las áreas de RRHH, como la hora de entrada, salida, almuerzo, horas extras, etc.

Su electrónica debe poder almacenar el software de su aplicación de forma segura e intacta, es decir, sin riesgo de perder información, descargar nuevas versiones o actualizaciones de su aplicación, y debe ser posible actualizarla a distancia.

Debe tener memoria para almacenar el registro de operaciones y/o transacciones gestionando los datos de forma inteligente, precisamente porque tiene toda la inteligencia integrada en un único armario. Toda la información que se almacenará en el equipo, debe hacerse de forma segura contra la pérdida por corte de energía, almacenando al menos 40.000 registros y las transferencias realizadas con la velocidad y la misma seguridad.

En la composición de la memoria del equipo, debe ser posible almacenar los registros de la bitácora de operaciones (40.000 registros) como se ha solicitado anteriormente, así como una copia de seguridad en caso de corte de energía y/o comunicación fuera de línea. Cuando se restablezca la comunicación, es decir, de fuera de línea a en línea, los registros deben ser enviados automáticamente a la base de datos sin ninguna intervención humana.

La recogida de información puede realizarse en línea o fuera de línea, según la mejor arquitectura definida para cada situación.

##### Características Generales o equivalentes

El dispositivo de datos debe disponer de un circuito de reloj preciso, con una alta fiabilidad en cuanto al registro de tiempos o épocas, con la función de eliminar los errores, los inconvenientes y la necesidad de ajustes manuales causados por problemas con la hora mostrada por el usuario y la hora realmente marcada en el software.

El sistema debe adaptarse a situaciones críticas de trabajo, es decir, lugares con temperaturas fluctuantes, humedad extrema, ambientes sujetos a condensación, es decir, donde se requieren soluciones robustas que puedan servir a la SNPP en un ambiente normal con condiciones normales de temperatura y presión o incluso en situaciones inesperadas o lugares con condiciones ambientales extremas.

El equipo debe poder configurarse para su instalación local o remota, con actualizaciones de firmware y aplicaciones.

El dispositivo debe poder instalarse en techos u otros lugares protegidos, dejando sólo visible el módulo de la interfaz de usuario, es decir, el módulo lector de tarjetas y el módulo biométrico, en su caso.

Debe poder interactuar con todos los tipos de soportes de tarjetas disponibles en el mercado para este tipo de aplicaciones, es decir, tarjetas de código de barras, tarjetas magnéticas, tarjetas inteligentes con o sin contacto, tarjetas de proximidad de 125 KHz, lectores biométricos y teclados, entre otros.

El equipo debe tener una interfaz RS 232 y una interfaz TCP-IP nativa, es decir, un puerto Ethernet directamente en la placa del equipo.

El equipo debe ser reversible, es decir, debe ser posible cambiar la placa de interfaz y el software para tener comunicación RS 485 o TCP-IP, para los casos en que la red TCP-IP no esté disponible.

El sistema de alimentación del dispositivo debe tener como objetivo proteger al usuario de los riesgos causados por los cortocircuitos, las

sobrecargas en la fuente o similares y también facilitando las características de instalación de las fuentes de alimentación (red y no ruptura). Por lo tanto, la fuente de alimentación debe ser externa a la unidad de dispositivo es separada de la unidad de control y procesamiento, precisamente para cumplir con los últimos requisitos y conceptos de seguridad a nivel mundial. La fuente de alimentación debe contar con medios de señalización visual que permitan identificar la fuente de alimentación activa, tanto en modo de CA como de CC. La fuente de alimentación debe contener una unidad sin ruptura con una autonomía mínima de 04 (cuatro) horas en funcionamiento continuo.

La fuente de alimentación debe estar en el rango completo de 90 ~ 240 VAC, entrada auxiliar de 12 VDC, entrada de batería de 12 VDC, y cuando haya un corte de energía el equipo funcionará con alimentación externa a través del módulo de fuente.

Datos técnicos

Gabinete: Acero inoxidable 304.

Visualización: LCD 2 x 16 con retroiluminación de alta intensidad con ajuste de contraste.

Teclado: Alta resistencia 12 teclas para la entrada de datos, selección de funciones, contraseñas, opción de configuración local para el administrador.

Pictograma: El equipo dispondrá de señalización visual mediante pictogramas orientativos que indiquen al usuario que su fichaje ha sido aceptado o no y los pictogramas tendrán al menos dos colores diferentes para indicar la actuación positiva y negativa, es decir, para la validación o rechazo de los fichajes o en su caso los eventos de acceso. De esta especificación, el empresario espera una solución de pictograma y no sólo una señalización mediante leds bicolor o incluso dos leds.

Estará equipado con dos lectores de tarjetas inteligentes mifare de 1 KB ISO 14443 tipo "A" y un lector biométrico. El lector biométrico será óptico y leerá en modo 1:1 y 1: N, según se seleccione por software y el tiempo de lectura en 1:1 será como máximo de 1s y en 1: N de 3s.

Comunicación: TCP-IP IPv6.

El equipo debe tener una memoria RAM y Flash de 512 Kb.

Debe estar equipado con un sensor biométrico con una resolución mínima de 500 ppp y un índice de falsa aceptación del 0,00001% y un índice de falso rechazo del 0,001%, permitiendo 9000 usuarios (sólo el modelo con biometría).

También debe ser capaz de almacenar datos durante un periodo superior a 120 horas.

Alimentación: Fuente de rango completo 90-240 Vac, 50-60 Hz - (POE). Consumo: Aproximadamente 10 VA.

Auxiliar: 12 Vdc 1 A.

Debe tener zumbador interno con ajuste.



Baterías: No hay kit de baterías de ruptura que permita el funcionamiento y la comunicación sin alimentación de la red principal Kit integrado en el equipo. No está permitido utilizarlo por separado.

Memoria protegida por super cápsula. Funcionamiento.

Puede funcionar on-line, off-line, Stand-alone o Cliente x Servidor.

Debe tener al menos 6 interfaces de E/S para comunicar y activar dispositivos y otros módulos mediante contacto seco, así como para recibir

información de los sensores mediante contacto seco y gestionar cada una de estas informaciones mediante el envío del software de gestión de accesos y seguridad.

Debe disponer de recursos de puesta en marcha a distancia con decisiones programadas en el propio controlador y/o recibir instrucciones de puesta en marcha desde el software de gestión de accesos para la eventual liberación/bloqueo de una puerta, portón del torniquete, etc. y recursos para la automatización como el encendido de una bombilla, aire acondicionado, activación de sensores, etc.

Características  
específicas o  
equivalentes

Características operativas

La placa lógica o placa electrónica principal del equipo, además de sus funciones de seguridad y acceso a los datos, debe albergar el procesador, las memorias, el circuito de reloj en tiempo real y todos los componentes del dispositivo, excepto la fuente de alimentación.

Cuando el empleado activa el lector de tarjetas, el dispositivo de datos debe verificar si es la tarjeta válida para ese sistema y proceder a la autorización, es decir, registra o no la hora de entrada/salida/comida del empleado, etc. mostrando en el pictograma de leds bicolor (verde/rojo) la señalización correspondiente como sigue:

Será imprescindible que el dispositivo tenga la funcionalidad de leer y escribir tarjetas inteligentes, operando en modo "on line" y "off line" de forma transparente para el usuario, siendo entonces necesario que las condiciones y reglas de cada empleado queden registradas en la memoria de la tarjeta.

Por lo tanto, en la acción de lectura del dispositivo también debe escribir en las tarjetas inteligentes sin contacto.

La señalización de los pictogramas debe cumplir, como mínimo, la norma que se indica a continuación.

Verde: Aceptado, tarjeta válida y datos registrados.

Rojo: Rechazada, tarjeta no válida para el sistema, o bloqueada por el administrador por razones predefinidas a través del software.

El administrador del sistema puede, si es necesario y conveniente, acceder a los parámetros de configuración de los dispositivos de datos a través de la tarjeta de administrador, lo que permite cambiar las condiciones de funcionamiento del equipo; sin embargo, estos cambios se pueden realizar a través del software de gestión suministrado con la solución.

Los dispositivos deben comunicarse en protocolo TCP-IP como se ha especificado anteriormente y deben ser compatibles con la base de datos ORACLE/SQL-SERVER. No se aceptarán soluciones que no sean compatibles con la plataforma mencionada, por lo que la SNPP exige en este pliego que sean compatibles con la plataforma de base de datos, en línea.

Comunicación

El dispositivo de datos estará equipado con comunicación TCP-IP, siendo aceptado sólo este tipo de interfaz nativa, pero también será posible, con el intercambio del módulo de interfaz, operar con red serial tipo RS 485 y también GPRS/3G/4G.

Características constructivas o equivalentes	Como la comunicación estándar será del tipo TCP-IP, el dispositivo de esta manera equipado con una interfaz estándar Ethernet nativa, se debe considerar una comunicación half/full-duplex 10 BASE-T (10/100 Mbits/s), con una dirección de red MAC-ADDRESS fija guardada de fábrica en el dispositivo, garantizando una vez más la accesibilidad segura al equipo.
	En modelos con comunicación GPRS debe estar preparada para cualquier operador del mercado. El dispositivo de datos debe tener su propia "cuna" en su placa electrónica interna donde se debe insertar el chip del operador, y no se aceptan soluciones con módems GPRS externos.
	Cuando el proyecto aborda el controlador de la puerta basado únicamente en un lector de tarjetas inteligentes sin contacto, la solución se refiere a este mismo elemento, pero sin las características de cumplir las especificaciones biométricas.
	Los lectores y controladores de los molinetes deben ser compatibles con el sistema de control de acceso y deben contar con la homologación de Anatel o similar.
	El dispositivo debe tener una construcción tecnológica tal que tenga inteligencia distribuida, permitiendo la interconexión de los terminales del dispositivo en una sola red de equipos con comunicación en línea tanto con interfaces tipo TCP-IP como RS 485.  Debe tener un gabinete de acero inoxidable 304, fabricado de acuerdo con la norma ABNT o similar, con clase de seguridad eléctrica y mecánica adecuada a la aplicación.
<b>ITEM 19                      Sensor Sísmico IOT</b>	
Características Generales o equivalentes	Los dispositivos de rastreo de activo con sensores múltiples.
	Deberán ser dispositivos pequeños de alta precisión, versátiles y confiables equipados con sensores múltiples que admiten hasta 50 configuraciones, firmware personalizable.
	Duración de la batería: 10 años *. Número de mensajes: 30.000.
Características específicas o equivalentes	Grado de impermeabilidad: IP68. Batería 1500 mAh.
	Machine learning y mapeo de patrones.
	Detección de Wifi para seguimiento de ubicación precisa de Wifi. Multizona conmutable.
	LED señalizador.
	Rango de medición de temperatura -40 a 60 ° C / ± 0,5 ° C. Barómetro.
	Giroscopio. Podómetro. Tiempo preciso. Acelerómetro. Magnetómetro. Luz ambiental. Anti- sabotaje. KEEP_ALIVE.
	Temperatura de funcionamiento -40 ° C a 60 ° C. Zonas de radio compatibles 1,2,3,4,5,6.
Características constructivas o equivalentes	Programación en línea, haga clic y seleccione. Lote a través de enlace descendente.
	Automatización y flujo de trabajo con integración.
	Firmware personalizable.
	Accesorios para tornillos perforados y bridas de cable de alta resistencia opcionales.
	Botón físico. Volumen 29 cm2.
	*La cantidad de mensajes y la longevidad de la batería en años están relacionados, considerar mínimo el envío de 2 eventos diarios.

ITEM 20	Sensor de Presencia IOT.
Características Generales o equivalentes	<p>Dispositivos de sensor de alarma por presencia. Modos de operación.</p> <p>Detecta multi zonas en espacios internos, detección de intrusión en lugares restringidos.</p> <p>Basado en eventos: Detectar movimiento humano basado en tiempo, número de recuento de humanos.</p> <p>Tipo de sensor: Infra Rojo Pasivo.</p> <p>Temperatura de funcionamiento -20 ° C a 70 ° C. Ángulo de visión: 120°.</p>
	<p>Distancia detección: hasta 10 m.</p> <p>Led indicador: aviso de envío de mensaje. Baterías: 3 años**.</p> <p>KEEP_ALIVE.</p> <p>Agregación de datos: Reduzca el consumo de energía con menos enlaces ascendentes.</p> <p>Carcasa: Plástico ABS. Antena: interna.</p>
	<p>Tamaño aproximado: 32g / 88 (L) x 30 x 20 (H) mm.</p> <p>**La cantidad de mensajes y la longevidad de la batería en años están relacionados, considerar mínimo el envío de 10.000 mensajes.</p>
ITEM 21	Plataforma de Gestión de Alarmas Integrada al VMS y conectividad IOT hasta 20 dispositivos por 24 meses.
Características Generales o equivalentes	<p>Sistema de alarmas de alta seguridad y rastreo de activos en tiempo real conectados al sistema de monitoreo remoto integrado al VMS.</p> <p>La tecnología</p> <p>La tecnología de comunicación deberá ser en una red de área amplia de baja potencia inmune al jamming (bloquear e interferir en diferentes tipos de señales de comunicación).</p> <p>Seguridad de la RED de comunicación:</p> <p>El ecosistema de red deberá integrar la seguridad de forma predeterminada:</p> <p>Autenticación + integridad + anti- reproducción en mensajes propagados en la red.</p> <p>Criptografía basada en AES sin transmisión de clave OTA.</p> <p>Cifrado de carga útil como opción para garantizar la confidencialidad de los datos.</p> <p>Aislamiento de cada parte de la red. Inmune al jammer.</p> <p>El oferente deberá presentar en su oferta la tecnología de red que utilizará, cobertura y seguridad.</p> <p>Dispositivos conectados a la RED</p> <p>Dispositivos de rastreo de activos en tiempo real contarán con información adicional de posición de los puntos de acceso Wi-Fi®.</p> <p>Dispositivos sensores de movimiento por presencia.</p>

	<p>Todos los dispositivos deberán contar con batería de larga duración, detectar eventos específicos de acuerdo con las especificaciones técnicas de cada elemento ofertado.</p> <p>El funcionamiento:</p>
Características específicas o equivalentes	<p>El sistema deberá mantener seguro los activos asignados proporcionando un dato de geolocalización en tiempo real, detección de golpes bruscos, intentos de manipulación, explosivos, temperatura, salida del área de influencia, dispositivo presente/ausente.</p> <p>Deberá enviar al VMS todos los eventos y alarmas preconfigurados, con la información de posicionamiento, mapas, imagen de las cámaras asignadas al dispositivo u evento para la toma de decisiones.</p> <p>Eventos mínimos a ser enviados al centro de Monitoreo. El nombre del dispositivo con su Geolocalización.</p> <p>Eventos generados. Tipo de sensor.</p> <p>Nivel de batería. KEEP_ALIVE.</p> <p>Histórico de datos de mensajes y eventos de los dispositivos. Horario de última actividad.</p> <p>Indicación del recorrido (en caso del activo haya sido movido del lugar o al ambiente externo).</p>
Características constructivas o equivalentes	<p>Todo el sistema tendrá que funcionar en modalidad M2M (maquina a máquina o sea del dispositivo al VMS centralizado) enviando la información de cada dispositivo hasta la central de monitoreo.</p>
<b>ITEM 22</b>	<b>Servicio de Integración de Sistema de Control Inteligente</b>
	<p>Magnitud del Sistema Integral de Control Inteligente estará compuesto por hardware, software, infraestructura de red de datos y ciberseguridad IOT y sistema de misión crítica (Failover).</p> <p>Casa Central, centro operativo y monitoreo.</p> <p>Todo el sistema de video vigilancia, sus integraciones y controles centralizados de gestión de seguridad con las siguientes características y equipos:</p> <p>Todos los equipos deben contar con tecnología IP nativa, una red datos exclusiva y administrable, estar integrados nativos, vía API o Plataforma LOW-CODE y con comunicación y comandos directa por software y todas las instrucciones y flujos de trabajos deben ser recibidos y enviados directos de la plataforma de gestión de vigilancia unificada, no serán aceptados equipos adaptados o placas de contacto seco para esta finalidad cada equipo suministrado ya deberá contar con sus contactos de I/O para la gestión de sensores comandos y bloqueos necesarios en las respectivas integraciones.</p> <p>Funcionamiento</p> <p>Control de acceso por molinetes inteligentes de alto flujo de pase libre, deberá actuar siempre abierto para la rápida autenticación de los usuarios.</p> <p>Deberá contar con lector para autenticación , lo requerido para el registro de datos de los usuarios, se grabará en base de datos, por validación y asociación con el rostro del usuario. Esta función está asociada al método KYC (Know Your Customer) cuyo proceso fundamental define y permite las relaciones empresas/usuarios y que deberán estar integrados con el Sistema de Gestión Empresarial (ERP) (Sistemas, aplicaciones y productos para el procesamiento de datos.) del SNPP por API.</p> <p>Una vez que el método KYC sea validado, el control de acceso y seguimiento de los usuarios será por reconocimiento e identificación facial en todas las cámaras disponibles conectadas en el sistema.</p> <p>Conectividad:</p>
Características Generales o equivalentes	

La infraestructura de red de datos deberá ser utilizada en su totalidad y actualizada para soportar los nuevos equipos, ancho de banda, seguridad IoT y el sistema de Failover (Conmutación por falla) configurado como misión crítica.

Failover (Conmutación por falla) configurado de misión crítica -Replicación Remota en Tiempo Real.

Considerando los factores externos de conectividad IoT, la modalidad y la ciberseguridad, el oferente deberá prever en la oferta, para la seguridad de los equipos en la solución Failover, y seguridad de la red

Estas configuraciones y medidas de seguridad son las mínimas exigidas e indispensables para:

Evitar que el personal no autorizado se infiltre en la red del sistema de seguridad; la asignación de puertos y el direccionamiento ofrece la posibilidad de limitar el rango de direcciones para cada área funcional.

La administración de la red se vuelve una tarea más sencilla al poder controlar (habilitar o denegar) los servicios de red:

Se reducen los dominios de broadcast, es decir, se limita el número de dispositivos conectados de acuerdo con el direccionamiento dinámico establecido.

Se evita la pérdida de información ya que la responsabilidad recae en los usuarios asignados a cada red virtual.

Se pueden compartir recursos de forma responsable asignados por área como pueden ser: Impresoras, servidores, equipos IoT etc.

Deberá justificar con su oferta cómo será la conexión, los equipos a ser utilizados, sistema de ciberseguridad, elementos físicos de red, fibra óptica (Intranet), enlaces y monitoreo, (arquitectura, diagrama, equipos, firewalls, proveedor del servicio, etc.) todo representado en el esquema de topología física de la RED que deberá acompañar a la oferta en formato tipo vision.

Observación:

Tener en cuenta al preparar la Oferta:

La configuración de Failover deberán estar disponibles mínimo por el periodo de 24 meses.

Considerar todos los costos necesarios al preparar la oferta. Infraestructura

El sistema de misión crítica Failover deberá contar con un servidor físico con la capacidad, licencias y recursos asignado en un DATACENTER que mínimo cumpla los estándares TIER3 y la norma ISO 27000 de seguridad de la información (con la respectiva declaración que el DC cumple con las normas).

Toda la implantación deberá contar con soporte local de rápida respuesta y asesoramiento al servicio de su actividad: atención 24 x 7 días a la semana durante el termino de 24 meses, sin costo adicional, todo lo cual deberá estar contemplado en la oferta. Además, justificará en su oferta la manera en que estará disponible el servicio de respuesta rápida.

Deberá tener en cuenta todos los costos necesarios al preparar la oferta en función de la solución propuesta.

Pasados los 24 meses del servicio de misión crítica incluido en la oferta, el sistema failover deberá seguir funcionando por un periodo de 2 meses más acompañado de todas las configuraciones del sistema de misión crítica ciberseguridad y conectividad IoT, durante este periodo el SNPP decidirá la renovación o no, del sistema de misión crítica.

Deberá contar con un técnico certificado en IT service managent (ITSM) Gestión de Servicios de Tecnología de Información.

2. Garantía integral en modalidad ILIMITADA de 2 años, otros datos requeridos y garantizados Todos los componentes del sistema deberán contar con garantía ilimitada de 2 años.

Características  
Específicas o  
Equivalente

El proveedor deberá garantizar una garantía total ilimitada por un periodo mínimo de 24 meses de la solución ofertada, deberá contar con repuestos componentes del sistema disponible para reposición en un plazo no mayor a 48 horas desde el reclamo formal por mail o plataforma de reclamos.

La Garantía, está comprendida para todos los equipos que presenten defectos por cualquier desperfecto que ocurra en la instalación/montaje, independiente de la causa de manera ilimitada.

El proveedor deberá efectuar el cambio y pruebas del equipo en un plazo de 72 hs. posterior al reclamo correspondiente del SNPP.

En caso que se compruebe vandalismo o robo de equipos, el proveedor deberá efectuar el referido informe al Administrador del Contrato, a los efectos de establecer los costos de reposición de los equipos y su montaje correspondiente.

### 3. Sistema de vídeo vigilancia IP existente

El sistema de video vigilancia existente en la, así como sus cámaras IP deberán ser migradas a la nueva plataforma de video vigilancia en su totalidad con las prestaciones, seguridad y funciones disponibles en cada dispositivo con su respectivo mantenimiento.

Prever en su totalidad el mantenimiento correctivo del sistema de videovigilancia del SNPP- Sede Central-Asunción con sus componentes.

El Servicio de mantenimiento contemplará: si necesario actualizar el software de gestión de video, y reemplazar las cámaras que actualmente presentan fallas y no se encuentran operativas (25, ya están en la lista de cámaras), así también, es necesario reemplazar 3 (tres) switches de comunicación Poe para la conectividad de las mismas, prever los cambios en caso

que también se detecten fallas en el cableado actual y, por tanto, necesiten ser modificados.

la Solución de videovigilancia existente a ser actualizada es un sistema Intelligent Security Systems (ISS), esta debe estar operativa y funcionando hasta la migración definitiva.

### 4. Plataforma Abierta de video vigilancia basada en servidor dedicados escalable.

La nueva arquitectura de software de gestión de video integral deberá soportar todas las cámaras, dispositivos, componentes del proyecto y ser escalable para el crecimiento futuro.

La capacidad de grabación deberá ser de 60 días en la plataforma centralizada, considerando un mínimo de 100 cámaras activas y configuradas con estos parámetros:

- Sistema de discos -mínimo RAID 5.
- Detección de movimiento: Server-Side.
- Número de clientes remotos: 10.
- Clientes en transmisión: 16.
- Cámaras: 400 activas.
- Ancho de banda: 567 Mbps.
- Resolución: 2600x1950 (5 MP).
- Compresión de video: H.264-MediumQual.
- Flujo de bits: Tasa de bits variable (VBR).
- Tasa de bits (kb/s): 3097.

- Cuadros por segundo: 12 promedio.
- Periodo de grabación: 60 días.
- Escena: Moderate-30.
- % Diario de grabación: 40.
- Ancho de banda (Mbps): 567 Mbps.
- Storage: dimensionar.

Presentar cálculo técnico que justifique el hardware dimensionado, cantidad y modelo de discos duros presentados, deberá tener en cuenta el almacenamiento unificado y centralizado, rendimiento necesario, velocidad, tiempo de búsqueda de archivos, (no serán aceptados discos duros que no sean específicos para video vigilancia en función de la cantidad de cámaras y volumen de grabación) conforme a requisitos de exigencia y prestaciones de la plataforma ofertada en los ítems 10 y 11 (Licencias Tipo 1: Servidor Remoto,

Licencias Tipo 4: Servidor Centralizado). Los discos deben ser incluidos en el hardware y certificados por el fabricante y la plataforma VMS.

#### 5. Distribución de Cámaras SNPP sede San Lorenzo

Ubicación	Subtotal Cámaras	Detalle Cámaras	Tipo Instalación	Planta
<b>Pabellón 1</b>	<b>2</b>			
Esquina Izquierda del Galpón radiando hacia la calle Destacamento Cazal	1		Perimetral	Interiores
A 20 metros del Galpón del lado derecho radiando hacia calle Destacamento Cazal	1		Perimetral	Exteriores
Pasillo entre salones 1201 y 1109 radiando hacia el	1		Interior	planta alta

corredor  
dirección salón  
1207

Salida de baño  
de hombres al  
lado del salón  
1106

1

interior

planta  
baja

**Pabellon 2**

**4**

Esquina lado  
derecho  
radiando hacia  
Viena

1

Perimetral

exteriores

Esquina lado  
izquierdo  
radiando hacia  
calle

1

Perimetral

exteriores

destacamento  
Cazal

Esquina lado  
izquierdo  
radiando hacia  
Galpón del

1

Perimetral

exteriores

**Pabellón 3**

Esquina lado  
derecho  
radiando entre  
Galpón

1

Perimetral

exteriores

pabellón 1 y  
calle Viena

**Pabellón 2**

**4**

pasillo  
radiando hacia  
salón 2204

1

Interior

Planta alta

Pasillo a nivel  
del salón 2204  
radiando hacia  
el salón

1

Interior

Planta alta

2203

pasillo nivel  
entre 2203 y  
2202 radiando  
hacia salón

1

Interior

Planta alta

2201

interna en  
salón 2102

1

Interior

Planta  
baja



<b>Pabellón 3</b>	<b>3</b>		
A definir con el contratista	3	Perimetral	Exterior
<b>Pabellón 3</b>	<b>6</b>		
Salón 3201 centro radiando hacia calle Viena	1	Interior	Planta alta
Pasillo esquina salón 3202 a nivel de escaleras radiando hacia destacamento casal	1	Interior	Planta alta
Salón 3101 radiando hacia calle Viena	1	Interior	Planta baja
Taller de Heladeras radiando entre Pabellón 2 y	1	Interior	Planta Baja
Pabellón 5			
Perimetral Lado Izquierdo a nivel Taller de Soldadura	1	Perimetral	Planta baja
Radiando hacia Viena			
A definir con el contratista	1	Perimetral	Exterior
<b>Pabellón 4</b>	<b>4</b>		
Desde el Archivo hacia las Escaleras dirección		Interior	Planta alta
Limpieza	1		
Puerta de Salón 4202 radiando hacia escaleras	1	Interior	Planta alta
Pasillo esquina del 4105 hacia dirección del corredor	1	Interior	Planta baja

entre 4103 y  
4102

Esquina del  
Salón  
Laboratorio  
Mantenimiento

1

Interior

Planta  
baja

Industrial

**Pabellón 5**

**3**

Salón de  
Auditorio  
radiando hacia  
Destacamento

1

Interiores

Planta  
alta

Cazal

Salón 5201  
Radiando hacia  
calle  
destacamento  
Cazal

1

Interiores

Planta  
alta

Salón 5202  
radiando hacia  
la calle  
destacamento  
Cazal

1

Interiores

Planta  
alta

**Pabellón 5**

**1**

A definir con el  
contratista

1

Perimetral

Exterior

**Pabellón  
Admin**

**1**

A definir con el  
contratista

1

Perimetral

Interiores

**Pabellón  
Admin**

**3**

Informaciones  
Radiando hacia  
secretaria de

1

Interiores

Planta  
baja

Academia  
Técnica

Esquina de  
Seguridad y  
Vigilancia  
radiando hacia

1

Interiores

Planta alta

Deposito

Dirección  
radiando hacia 1  
Dpto.  
Académico

Interiores

Planta alta

## 6 Tiempo de Plazo del Proyecto

El proyecto tendrá 30 días corridos desde su planificación, ejecución e implementación.

## 7 Materiales

Los suministros deberán incluir, sin estar limitados, a las siguientes partidas:

Todos los equipos, dispositivos y elementos necesarios, de manera que permitan el funcionamiento del Sistema integrado de Video Vigilancia IP.

El contratista prever todos los equipos y accesorios para el completo funcionamiento del sistema Como ser:

Los Racks, Ups 1KVA, patcheras, fichas RJ45 CAT6 Switch Core, Switch PoE o no cuando necesarios en cada punto o nudo con su respectivo número de puertos, cableado de datos UTP CAT. 6 que cumpla la norma EIA/TIA 568-C., así como el de alimentación, cajas de paso, canalizaciones y ductos adecuadas a cada punto a ser instalado, protecciones contra descargas para por cada elemento del sistema y los mismos deberán estar conectada a tierra, la interconexión de los Switches será a través de fibra óptica

proveerá dos ejemplares de un Manual de Operación y Mantenimiento del Sistema de Video Vigilancia.

## 8 Mano de Obra:

El oferente deberá de prever en su oferta la mano de obra para la puesta en marcha de todo el sistema.

Deben considerar para el diseño, implementación y puesta en marcha de la plataforma de Video Seguridad Integrada. Deberá prever todos los trabajos necesarios, de manera que permitan el funcionamiento del Sistema de Video Vigilancia IP.

## 9 INSPECCIONES Y PRUEBAS

La Contratante por su administrador de contrato será la máxima autoridad para verificar que la instalación se efectué de acuerdo a estas especificaciones.

Ninguna comunicación verbal tendrá validez para justificar cambios en el proyecto.

## 10 Entrenamiento

El entrenamiento de uso, gestión y administración de la nueva solución de gestión de video deberá ser de un mínimo de 100 horas para el personal designado por el Administrador del Contrato. Las horas de entrenamiento serán computadas una vez que el sistema este instalado e integrado en su totalidad.

## 11 Manuales y Licencias

El Contratista deberá entregar manuales completos y adecuados de la operación. Estos manuales deberán ser en español y deben contener una descripción de funcionamiento y operación individual e integral, y no limitarse a la entrega de catálogos y especificaciones del fabricante, los cuales también deben ser entregados, pudiendo ser los documentos originales del proveedor. El proveedor deberá entregar las licencias originales de todos los softwares instalados.

## 12 Sala de Control, Muebles y Accesorios

Sera suministrada por la Sede del SNPP San Lorenzo, en su totalidad. El cual quedara en custodia el servidore de Video remoto y todos sus accesorios.

### 13 Generalidades

El alcance del proyecto para los sistemas antes mencionados considera el suministro, montaje, pruebas, puesta en servicio.

Es de responsabilidad del oferente reconocer los puntos de instalación e identificar los materiales y accesorios necesarios para la correcta instalación y funcionamiento de estos equipos.

Los trabajos deben contemplar el desarrollo complementario de la Ingeniería necesaria para el montaje, incluido planos, cortes, elevaciones, detalles, suministro de materiales y equipos, mano de obra calificada y especializada, y todo lo que resulte necesario para la provisión, montaje y puesta en servicio del Sistema de Video Seguridad Integrado.

Durante todo el curso de los trabajos el Contratista deberá mantener una persona en el lugar de la obra, quien estará en condiciones de suministrar la información relativa a los trabajos y recibir las indicaciones del Contratante.

La omisión o no inclusión de algún ítem necesario y esencial para el buen funcionamiento de la solución no exime al Contratista de la responsabilidad de presentar una solución de conjunto que permita el funcionamiento integral de la misma, con desempeño satisfactorio y un máximo nivel de confianza.

Quedará a cargo del oferente todos los trabajos para el montaje y puesta en funcionamiento del sistema, por lo que para la cotización deberá tener en cuenta los siguientes ítems:

- \* Los equipos y componentes con las características básicas obligatorias, conforme a lo especificado y las cantidades definidas
- \* Accesorios para la instalación de todo el sistema (conductores, ductos, soportes, etc.).
- \* Instalación, configuración y puesta en servicio de todo el Sistema de Video Seguridad Integrado.
- \* Tendido de cableado e interconexión entre los Switches
- \* Licencia legal del software proveído.
- \* Soporte técnico tanto de hardware como de software

## Identificación de la unidad solicitante y justificaciones

JUSTIFICACION DE LA NECESIDAD QUE SE PRETENDE SATISFACER MEDIANTE LA CONTRATACION A SER REALIZADA.	Dicho pedido obedece a la necesidad de realizar una ampliación de cámaras disminuyendo así los puntos ciegos existentes, capacidad de almacenamiento y el reemplazo de cámaras que se encuentran quemadas.
DETERMINAR SI SE TRATA DE UN LLAMADO PERIODICO O SUCESIVO, O SI EL MISMO RESPONDE A UNA NECESIDAD TEMPORAL.	TEMPORAL

**JUSTIFICAR LAS  
ESPECIFICACIONES  
TECNICAS  
ESTABLECIDAS.**

Las especificaciones tecnicas han sido elaboradas en base a las necesidades que se requiere con respecto a la adquisicion de camaras de circuito cerrado, se solicitan que los bienes a ser adquiridos cumplan con caracteristicas minimas para el optimo funcionamiento de los mismos. todo ello en busca de adquirir la mejor calidad de los bienes al menor costo posible.

## Plan de entrega de los bienes

La entrega de los bienes se realizará de acuerdo al Plan de Entrega y Cronograma de Cumplimiento, indicado en el presente apartado. Así mismo, de los documentos de embarque y otros que deberá suministrar el Proveedor indicados a continuación:

Ítem	Descripción del bien	Cantidad	Unidad de medida	Lugar de entrega de los bienes	Fecha(s) final(es) de entrega de los bienes
1	Sistema de circuito cerrado de video vigilancia	1	UNIDAD	Según Especificaciones Técnicas	30 DIAS CALENDARIO

## Planos y diseños

Para la presente contratación se pone a disposición los siguientes planos o diseños:

No Aplica

## Embalajes y documentos

El embalaje, la identificación y la documentación dentro y fuera de los paquetes serán como se indican a continuación:

No Aplica

## Inspecciones y pruebas

Las inspecciones y pruebas serán como se indica a continuación:

**CONFORME A LO INDICADO EN LAS ESPECIFICACIONES TÉCNICAS EL ADMINISTRADOR DE CONTRATO REALIZARÁ TODAS LA VERIFICACIONES PERTINENTES**

1. El proveedor realizará todas las pruebas y/o inspecciones de los Bienes, por su cuenta y sin costo alguno para la contratante.
2. Las inspecciones y pruebas podrán realizarse en las instalaciones del Proveedor o de sus subcontratistas, en el lugar de entrega y/o en el lugar de destino final de entrega de los bienes, o en otro lugar en este apartado.  
Cuando dichas inspecciones o pruebas sean realizadas en recintos del Proveedor o de sus subcontratistas se le proporcionarán a los inspectores todas las facilidades y asistencia razonables, incluso el acceso a los planos y datos sobre producción, sin cargo alguno para la contratante.
3. La contratante o su representante designado tendrá derecho a presenciar las pruebas y/o inspecciones mencionadas en la cláusula anterior, siempre y cuando éste asuma todos los costos y gastos que ocasione su participación, incluyendo gastos de viaje, alojamiento y alimentación.
4. Cuando el proveedor esté listo para realizar dichas pruebas e inspecciones, notificará oportunamente a la contratante indicándole el lugar y la hora. El proveedor obtendrá de una tercera parte, si corresponde, o del fabricante cualquier permiso o consentimiento necesario para permitir al contratante o a su representante designado presenciar las pruebas o inspecciones.
5. La contratante podrá requerirle al proveedor que realice algunas pruebas y/o inspecciones que no están requeridas en el contrato, pero que considere necesarias para verificar que las características y funcionamiento de los bienes cumplan con los códigos de las especificaciones técnicas y normas establecidas en el contrato. Los costos adicionales razonables que incurra el proveedor por dichas pruebas e inspecciones serán sumados al precio del contrato, en cuyo caso la contratante deberá justificar a través de un dictamen fundado en el interés público comprometido. Asimismo, si dichas pruebas y/o inspecciones impidieran el avance de la fabricación y/o el desempeño de otras obligaciones del proveedor bajo el contrato, deberán realizarse los ajustes correspondientes a las Fechas de Entrega y de Cumplimiento y de las otras obligaciones afectadas.
6. El proveedor presentará a la contratante un informe de los resultados de dichas pruebas y/o inspecciones.
7. La contratante podrá rechazar algunos de los bienes o componentes de ellos que no pasen las pruebas o inspecciones o que no se ajusten a las especificaciones. El proveedor tendrá que rectificar o reemplazar dichos bienes o componentes rechazados o hacer las modificaciones necesarias para cumplir con las especificaciones sin ningún costo para la contratante. Asimismo, tendrá que repetir las pruebas o inspecciones, sin ningún costo para la contratante, una vez que notifique a la contratante.
8. El proveedor acepta que ni la realización de pruebas o inspecciones de los bienes o de parte de ellos, ni la presencia de la contratante o de su representante, ni la emisión de informes, lo eximirán de las garantías u otras obligaciones en virtud del contrato.

## Indicadores de Cumplimiento

El documento requerido para acreditar el cumplimiento contractual, será:

Planificación de indicadores de cumplimiento:

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA <i>(se indica la fecha que debe presentar según el PBC)</i>
<i>Nota de Remisión / Acta de recepción 1</i>	<i>Nota de Remisión / Acta de recepción</i>	<i>Diciembre 2021</i>

De manera a establecer indicadores de cumplimiento, a través del sistema de seguimiento de contratos, la convocante deberá determinar

el tipo de documento que acredite el efectivo cumplimiento de la ejecución del contrato, así como planificar la cantidad de indicadores que deberán ser presentados durante la ejecución. Por lo tanto, la convocante en este apartado y de acuerdo al tipo de contratación de que se trate, deberá indicar el documento a ser comunicado a través del módulo de Seguimiento de Contratos y la cantidad de los mismos.

---

## **Criterios de Adjudicación**

La Convocante adjudicará el contrato al oferente cuya oferta haya sido evaluada como la más baja y cumpla sustancialmente con los requisitos de las bases y condiciones, siempre y cuando la convocante determine que el oferente está calificado para ejecutar el contrato satisfactoriamente.

1. La adjudicación en los procesos de contratación en los cuales se aplique la modalidad de contrato abierto, se efectuará por las cantidades o montos máximos solicitados en el llamado, sin que ello implique obligación de la convocante de requerir la provisión de esa cantidad o monto durante de la vigencia del contrato, obligándose sí respecto de las cantidades o montos mínimos establecidos.
2. En caso de que la convocante no haya adquirido la cantidad o monto mínimo establecido, deberá consultar al proveedor si desea ampliarlo para el siguiente ejercicio fiscal, hasta cumplir el mínimo.
3. Al momento de adjudicar el contrato, la convocante se reserva el derecho a disminuir la cantidad de bienes requeridos, por razones de disponibilidad presupuestaria u otras razones debidamente justificadas. Estas variaciones no podrán alterar los precios unitarios u otros términos y condiciones de la oferta y de los documentos de la licitación.

En aquellos llamados en los cuales se aplique la modalidad de contrato abierto, cuando la convocante deba disminuir cantidades o montos a ser adjudicados, no podrá modificar el monto o las cantidades mínimas establecidas en las bases de la contratación.

---

## **Notificaciones**

La comunicación de la adjudicación a los oferentes será como sigue:

1. Dentro de los cinco (5) días corridos de haberse resuelto la adjudicación, la convocante comunicará a través del Sistema de Información de Contrataciones Públicas, copia del informe de evaluación y del acto administrativo de adjudicación, los cuales serán puestos a disposición pública en el referido sistema. Adicionalmente el sistema generará una notificación a los oferentes por los medios remotos de comunicación electrónica pertinentes, la cual será reglamentada por la DNCP.
2. En sustitución de la notificación a través del Sistema de Información de Contrataciones Públicas, las convocantes podrán dar a conocer la adjudicación por cédula de notificación a cada uno de los oferentes, acompañados de la copia íntegra del acto administrativo y del informe de evaluación. La no entrega del informe en ocasión de la notificación, suspende el plazo para formular protestas hasta tanto la convocante haga entrega de dicha copia al oferente solicitante.
3. En caso de la convocante opte por la notificación física a los oferentes participantes, deberá realizarse únicamente con el acuse de recibo y en el mismo con expresa mención de haber recibido el informe de evaluación y la resolución de adjudicación.
4. Las cancelaciones o declaraciones desiertas deberán ser notificadas a todos los oferentes, según el procedimiento indicado precedentemente.
5. Las notificaciones realizadas en virtud al contrato, deberán ser por escrito y dirigirse a la dirección indicada en el contrato.

---

## **Audiencia Informativa**

Una vez notificado el resultado del proceso, el oferente tendrá la facultad de solicitar una audiencia a fin de que la convocante explique los fundamentos que motivan su decisión.

La solicitud de audiencia informativa no suspenderá ni interrumpirá el plazo para la interposición de protestas.

La misma deberá ser solicitada dentro de los dos (2) días hábiles siguientes en que el oferente haya tomado conocimiento de los términos del Informe de Evaluación de Ofertas.

La convocante deberá dar respuesta a dicha solicitud dentro de los dos (2) días hábiles de haberla recibido y realizar la audiencia en un plazo que no exceda de dos (2) días hábiles siguientes a la fecha de respuesta al oferente.

## **Documentación requerida para la firma del contrato**

Luego de la notificación de adjudicación, el proveedor deberá presentar en el plazo establecido en las reglamentaciones vigentes, los documentos indicados en el presente apartado.

1. Personas Físicas / Jurídicas
<ul style="list-style-type: none"><li>• Certificado de no encontrarse en quiebra o en convocatoria de acreedores expedido por la Dirección General de Registros Públicos;</li></ul>
<ul style="list-style-type: none"><li>• Certificado de no hallarse en interdicción judicial expedido por la Dirección General de Registros Públicos;</li></ul>
<ul style="list-style-type: none"><li>• Constancia de no adeudar aporte obrero patronal expedida por el Instituto de Previsión Social;</li></ul>
<ul style="list-style-type: none"><li>• Certificado laboral vigente expedido por la Dirección de Obrero Patronal dependiente del Viceministerio de Trabajo, siempre que el sujeto esté obligado a contar con el mismo, de conformidad a la reglamentación pertinente - CPS;</li></ul>
<ul style="list-style-type: none"><li>• 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;</li></ul>
<ul style="list-style-type: none"><li>• Certificado de cumplimiento tributario vigente a la firma del contrato.</li></ul>
2. Documentos. Consorcios
<ul style="list-style-type: none"><li>• Cada integrante del consorcio que sea una persona física o jurídica deberá presentar los documentos requeridos para oferentes individuales especificados en los apartados precedentes.</li></ul>
<ul style="list-style-type: none"><li>• Original o fotocopia del consorcio constituido.</li></ul>



- Documentos que acrediten las facultades del firmante del contrato para comprometer solidariamente al consorcio.

- 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.

# CONDICIONES CONTRACTUALES

Esta sección constituye las condiciones contractuales a ser adoptadas por las partes para la ejecución del contrato.

## Interpretación

### Interpretación

1. Si el contexto así lo requiere, el singular significa el plural y viceversa; y "día" significa día calendario, salvo que se haya indicado expresamente que se trata de días hábiles.

2. Condiciones prohibidas, inválidas o inejecutables

Si cualquier provisión o condición del Contrato es prohibida o resultase inválida o inejecutable, dicha prohibición, invalidez o falta de ejecución no afectará la validez o el cumplimiento de las otras provisiones o condiciones del Contrato.

3. Limitación de Dispensas:

a) Toda dispensa a los derechos o facultades de una de las partes en virtud del Contrato, deberá ser documentada por escrito, indicar la fecha, estar firmada por un representante autorizado de la parte que otorga dicha dispensa y deberá especificar la obligación que está dispensando y el alcance de la dispensa.

b) Sujeto a lo indicado en el inciso precedente, ningún retraso, prórroga, demora o aprobación por cualquiera de las partes al hacer cumplir algún término y condición del contrato o el otorgar prórrogas por una de las partes a la otra, perjudicará, afectará o limitará los derechos de esa parte en virtud del Contrato. Asimismo, ninguna prórroga concedida por cualquiera de las partes por un incumplimiento del Contrato, servirá de dispensa para incumplimientos posteriores o continuos del Contrato.

## Subcontratación

El porcentaje permitido para la subcontratación será de:

No Aplica

La subcontratación del contrato deberá ser realizada conforme a las disposiciones contenidas en la Ley, el Decreto Reglamentario y la reglamentación que emita para el efecto la DNCP.

## Derechos Intelectuales

1. Los derechos de propiedad intelectual de todos los planos, documentos y otros materiales conteniendo datos e información proporcionada a la contratante por el proveedor, seguirán siendo salvo prueba en contrario de propiedad del proveedor. Si esta información fue suministrada a la contratante directamente o a través del proveedor por terceros, incluyendo proveedores de materiales, los derechos de propiedad intelectual de dichos materiales seguirá siendo de propiedad de dichos terceros

2. Sujeto al cumplimiento por parte de la contratante del párrafo siguiente, el proveedor indemnizará y liberará de toda responsabilidad a la contratante, sus empleados y funcionarios en caso de pleitos, acciones o procedimientos administrativos, reclamaciones, demandas,

pérdidas, daños, costos y gastos de cualquier naturaleza, incluyendo gastos y honorarios por representación legal, que la contratante tenga que incurrir como resultado de la transgresión o supuesta transgresión de derechos de propiedad intelectual como patentes, dibujos y modelos industriales registrados, marcas registradas, derechos de autor u otro derecho de propiedad intelectual registrado o ya existente en la fecha del contrato debido a:

- a) La instalación de los bienes por el proveedor o el uso de los bienes en la República del Paraguay; y
- b) La venta de los productos producidos por los bienes en cualquier país.

Dicha indemnización no procederá si los bienes o una parte de ellos fuesen utilizados para fines no previstos en el Contrato o para fines que no pudieran inferirse razonablemente del Contrato. La indemnización tampoco cubrirá cualquier transgresión que resultara del uso de los bienes o parte de ellos, o de cualquier producto producido como resultado de asociación o combinación con otro equipo, planta o materiales no suministrados por el proveedor en virtud del Contrato.

3. Si se entablara un proceso legal o una demanda contra la Contratante como resultado de alguna de las situaciones indicadas en la cláusula anterior, la Contratante notificará prontamente al proveedor y éste por su propia cuenta y en nombre de la Contratante responderá a dicho proceso o demanda, y realizará las negociaciones necesarias para llegar a un acuerdo de dicho proceso o demanda.

4. Si el Proveedor no notifica a la Contratante dentro de treinta (30) días a partir del recibo de dicha comunicación de su intención de proceder con tales procesos o reclamos, la Contratante tendrá derecho a emprender dichas acciones en su propio nombre.

5. La Contratante se compromete, a solicitud del proveedor, a prestarle toda la asistencia posible para que el proveedor pueda contestar las citadas acciones legales o reclamaciones. La Contratante será reembolsada por el proveedor por todos los gastos razonables en que hubiera incurrido.

6. La Contratante deberá indemnizar y eximir de culpa al proveedor y a sus empleados, funcionarios y subcontratistas, por cualquier litigio, acción legal o procedimiento administrativo, reclamo, demanda, pérdida, daño, costo y gasto, de cualquier naturaleza, incluyendo honorarios y gastos de abogado, que pudieran afectar al proveedor como resultado de cualquier transgresión o supuesta transgresión de patentes, modelos de aparatos, diseños registrados, marcas registradas, derechos de autor, o cualquier otro derecho de propiedad intelectual registrado o ya existente a la fecha del Contrato, que pudieran suscitarse con motivo de cualquier diseño, datos, planos, especificaciones, u otros documentos o materiales que hubieran sido suministrados o diseñados por la Contratante o a nombre suyo.

---

## Transporte

La responsabilidad por el transporte de los bienes será según se establece en los Incoterms.

Si las mismas no está de acuerdo con los Incoterms, el transporte deberá ser como sigue:

No Aplica

---

## Confidencialidad de la información

1. No deberá darse a conocer información alguna acerca del análisis, aclaración y evaluación de las ofertas ni sobre las recomendaciones relativas a la adjudicación, después de la apertura en público de las ofertas, a los oferentes ni a personas no involucradas en el proceso de evaluación, hasta que haya sido dictada la Resolución de Adjudicación.

2. La contratante y el proveedor deberán mantener confidencialidad y en ningún momento divulgarán a terceros, sin el consentimiento de la otra parte, documentos, datos u otra información que hubiera sido directa o indirectamente proporcionada por la otra parte en conexión con el contrato, antes, durante o después de la ejecución del mismo. No obstante, el proveedor podrá proporcionar a sus subcontratistas los documentos, datos e información recibidos de la contratante para que puedan cumplir con su trabajo en virtud del contrato. En tal caso, el proveedor obtendrá de dichos subcontratistas un compromiso de confidencialidad similar al requerido al proveedor en la presente cláusula.

3. La Contratante no utilizará dichos documentos, datos u otra información recibida del proveedor para ningún uso que no esté relacionado con el contrato. Así mismo el proveedor no utilizará los documentos, datos u otra información recibida de la contratante para ningún otro propósito diferente al de la ejecución del contrato.

4. La obligación de las partes arriba mencionadas, no aplicará a la información que:
- a) La contratante o el proveedor requieran compartir con otras instituciones que participan en el financiamiento del Contrato;
  - b) Actualmente o en el futuro se hace de dominio público sin culpa de ninguna de las partes;
  - c) Puede comprobarse que estaba en posesión de esa parte en el momento que fue divulgada y no fue previamente obtenida directa o indirectamente de la otra parte; o
  - d) Que de otra manera fue legalmente puesta a la disponibilidad de esa parte por un tercero que no tenía obligación de confidencialidad.
5. Las disposiciones precedentes no modificarán de ninguna manera ningún compromiso de confidencialidad otorgado por cualquiera de las partes a quien esto compete antes de la fecha del contrato con respecto a los suministros o cualquier parte de ellos.
6. Las disposiciones de esta cláusula permanecerán válidas después del cumplimiento o terminación del contrato por cualquier razón.

---

## Obligatoriedad de declarar información del personal del contratista en el SICP

1. El proveedor deberá proporcionar los datos de identificación de sus subproveedores, así como de las personas físicas por medio de las cuales propone cumplir con las obligaciones del contrato, dentro de los treinta días posteriores a la obtención del código de contratación, y con anterioridad al primer pago que vaya a percibir en el marco de dicho contrato, con las especificaciones respecto a cada una de ellas. A ese respecto, el Contratista deberá consignar dichos datos en el Formulario de Información del Personal (FIP) y en el Formulario de Informe de Servicios Personales (FIS), a través del SIPE.

2. Cuando ocurra algún cambio en la nómina del personal o de los subcontratistas propuestos, el proveedor o contratista está obligado a actualizar el FIP.
3. Como requerimiento para efectuar los pagos a los proveedores o contratistas, la contratante, a través del procedimiento establecido para el efecto por la entidad previsional, verificará que el proveedor o contratista se encuentre al día en el cumplimiento con sus obligaciones para con el Instituto de Previsión Social (IPS).
4. La Contratante podrá realizar las diligencias que considere necesarias para verificar que la totalidad de las personas que prestan servicios personales en relación de dependencia para la contratista y eventuales subcontratistas se encuentren debidamente individualizados en los listados recibidos.
5. El proveedor o contratista deberá permitir y facilitar los controles de cumplimiento de sus obligaciones de aporte obrero patronal, tanto los que fueran realizados por la contratante como los realizados por el IPS y por funcionarios de la DNCP. La negativa expresa o tácita se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.
6. En caso de detectarse que el proveedor o contratista o alguno de los subcontratistas, no se encontraran al día con el cumplimiento de sus obligaciones para con el IPS, deberán ser emplazados por la contratante para que en diez (10) días hábiles cumplan con sus obligaciones pendientes con la previsional. En el caso de que no lo hiciera, se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.

---

## Formas y condiciones de pago

El adjudicado para solicitar el pago de las obligaciones deberá presentar la solicitud acompañada de los siguientes documentos:

1. Documentos Genéricos:

- 1. Nota de remisión;
- 2. La factura de pago, con timbrado vigente, la cual deberán expresar claramente por separado el Impuesto al Valor Agregado (IVA) de conformidad con las disposiciones tributarias aplicables. En ningún caso el valor total facturado podrá exceder el valor adjudicado o las adendas aprobadas;
- 3. REPSE (registro de prestadores de servicios) todos los que son prestadores de servicios;
- 4. Certificado de Cumplimiento Tributario;
- 5. Constancia de Cumplimiento con la Seguridad Social;
- 6. Formulario de Informe de Servicios Personales (FIS).

Otras formas y condiciones de pago al proveedor en virtud del contrato serán las siguientes:

*Para el Ejercicio Fiscal 2021 y, conforme a la asignación de Plan de caja, con fuente de 30 Recursos Propios, del Ministerio de Hacienda. La moneda de pago será en Guaraníes, a través, del pago directo a Proveedores (transferencia en cta. bancaria.)*

*El plazo de pago de las facturas será en un máximo de 60 (sesenta) días, después de la presentación de la factura por el Proveedor. Una vez que la contratante haya aceptado, dicha aceptación deberá darse a más tardar en quince días posteriores a su presentación.*

*Para el pago, el proveedor deberá presentar:*

*- Nota de pedido de pago del proveedor a la Convocante*

*-Factura Crédito*

*-Nota de Remisión con la conformidad de la dependencia receptora.*

*-Nota de Remisión.*

*- Copia del Certificado de Cumplimiento con el Seguro Social o Constancia de no estar inscripto en el Instituto de Previsión Social (IPS) vigente.*

*- Copia la última declaración de IVA y del Certificado de Cumplimiento Tributario vigente y/o copia de boleta de pago del impuesto.*

*-Una vez concreta la transferencia en la cuenta bancaria del proveedor, remitir recibo de pago con la misma fecha de dicha transferencia.*

*- Presentación de Información del Personal (FIP) y en el Formulario de Informe de Servicios Personales (FIS)*

2. La Contratante efectuará los pagos, dentro del plazo establecido en este apartado, sin exceder sesenta (60) días después de la presentación de una factura por el proveedor, y después de que la contratante la haya aceptado. Dicha aceptación o rechazo, deberá darse a más tardar en quince (15) días posteriores a su presentación.

3. De conformidad a las disposiciones del Decreto N° 7781/2006, del 30 de Junio de 2006 y modificatoria, en las contrataciones con Organismos de la Administración Central, el proveedor deberá habilitar su respectiva cuenta corriente o caja de ahorro en un Banco de plaza y comunicar a la Contratante para que ésta gestione ante la Dirección General del Tesoro Público, la habilitación en el Sistema de Tesorería (SITE).

## **Solicitud de suspensión de la ejecución del contrato**

Si la mora en el pago por parte de la contratante fuere superior a sesenta (60) días, el proveedor, consultor o contratista, tendrá derecho a solicitar por escrito la suspensión de la ejecución del contrato por causas imputables a la contratante.

La solicitud deberá ser respondida por la contratante dentro de los 10 (diez) días calendario de haber recibido por escrito el requerimiento. Pasado dicho plazo sin respuesta se considerará denegado el pedido, con lo que se agota la instancia administrativa quedando expedita la vía contencioso administrativa.

## **Solicitud de Pago de Anticipo**

El plazo dentro del cual se solicitará el anticipo será (en días corridos) de:

No Aplica

## Reajuste

El precio del contrato estará sujeto a reajustes. La fórmula y el procedimiento para el reajuste serán los siguientes:

El reajuste de precio deberá ser solicitado por el Proveedor y aprobado por el Contratante por medio de notas oficiales. Los precios ofertados estarán sujetos a reajustes, siempre y cuando la variación del IPC publicado por el BCP haya sufrido una variación igual o mayor al quince por ciento (15%) referente a la fecha de apertura de ofertas, conforme a la siguiente fórmula:  $Pr = P \times IPC1 / IPC0$ , donde: Pr: Precio Reajustado; P: Precio adjudicado; IPC1: Índice de precios al consumidor publicado por el Banco Central del Paraguay, correspondiente a la fecha de la resolución de Adjudicación; IPC0: Índice de precios al consumidor publicado por el Banco Central del Paraguay, correspondiente al mes de la apertura de sobres. No se reconocerán reajustes de precios si el suministro se encuentra atrasado respecto al cronograma de entregas aprobado.

## Porcentaje de multas

El valor del porcentaje de multas que será aplicado por el atraso en la entrega de los bienes, prestación de servicios será de:

0,05 %

La contratante podrá deducir en concepto de multas una suma equivalente al porcentaje del precio de entrega de los bienes atrasados, por cada día de atraso indicado en este apartado. La contratante podrá rescindir administrativamente el contrato cuando el valor de las multas supere el monto de la Garantía de Cumplimiento de Contrato.

La aplicación de multas no libera al proveedor del cumplimiento de sus obligaciones contractuales.

## Tasa de interés por Mora

En caso de que la contratante incurriera en mora en los pagos, se aplicará una tasa de interés por cada día de atraso, del:

0,01

La mora será computada a partir del día siguiente del vencimiento del pago y no incluye el día en el que la contratante realiza el pago.

Si la Contratante no efectuara cualquiera de los pagos al proveedor en las fechas de vencimiento correspondiente o dentro del plazo establecido en la presente cláusula, la Contratante pagará al proveedor interés sobre los montos de los pagos morosos a la tasa establecida en este apartado, por el período de la demora hasta que haya efectuado el pago completo, ya sea antes o después de cualquier juicio.

## Impuestos y derechos

En el caso de bienes de origen extranjero, el Proveedor será totalmente responsable del pago de todos los impuestos, derechos, gravámenes, timbres, comisiones por licencias y otros cargos similares que sean exigibles fuera y dentro de la República del Paraguay, hasta el momento en que los bienes contratados sean entregados al contratante.

En el caso de origen nacional, el Proveedor será totalmente responsable por todos los impuestos, gravámenes, comisiones por licencias y otros cargos similares incurridos hasta el momento en que los bienes contratados sean entregados a la contratante.

El Proveedor será responsable del pago de todos los impuestos y otros tributos o gravámenes con excepción de los siguientes:

*SIN EXCEPCIÓN ALGUNA*

## **Convenios Modificatorios**

La Contratante podrá acordar modificaciones al contrato conforme al artículo N° 63 de la Ley N° 2051/2003.

1. Cuando el sistema de adjudicación adoptado sea de abastecimiento simultáneo las ampliaciones de los contratos se registrarán por las disposiciones contenidas en la Ley N° 2051/2003, sus modificaciones y reglamentaciones, que para el efecto emita la DNCP.
2. Tratándose de contratos abiertos, las modificaciones a ser introducidas se registrarán atendiendo a la reglamentación vigente.
3. La celebración de un Convenio Modificatorio conforme a las reglas establecidas en el artículo N° 63 de la Ley 2051/2003, que constituyan condiciones de agravación del riesgo cuando la Garantía de Cumplimiento de Contrato sea formalizada a través de póliza de caución, obliga al proveedor a informar a la compañía aseguradora sobre las modificaciones a ser realizadas y en su caso, presentar ante la contratante los endosos por ajustes que se realicen a la póliza original en razón al convenio celebrado con la contratante.

## **Limitación de responsabilidad**

Excepto en casos de negligencia grave o actuación de mala fe, el proveedor no tendrá ninguna responsabilidad contractual de agravio o de otra índole frente a la Contratante por pérdidas o daños indirectos o consiguientes, pérdidas de utilización, pérdidas de producción, o pérdidas de ganancias o por costo de intereses, estipulándose que esta exclusión no se aplicará a ninguna de las obligaciones del proveedor de pagar a la Contratante las multas previstas en el Contrato.

## **Responsabilidad del proveedor**

El proveedor deberá suministrar todos los bienes o servicios de acuerdo con las condiciones establecidas en el pliego de bases y condiciones.

## **Fuerza mayor**

El proveedor no estará sujeto a la ejecución de su Garantía de Cumplimiento, liquidación por daños y perjuicios o terminación

por incumplimiento en la medida en que la demora o el incumplimiento de sus obligaciones en virtud del contrato sea el resultado de un evento de Fuerza Mayor.

1. Para fines de esta cláusula, "Fuerza Mayor" significa un evento o situación fuera del control del proveedor que es imprevisible, inevitable y no se origina por descuido o negligencia del mismo. Tales eventos pueden incluir sin que éstos sean los únicos actos de la autoridad en su capacidad soberana, guerras o revoluciones, incendios, inundaciones, epidemias, pandemias, restricciones de cuarentena, y embargos de cargamentos.
2. El proveedor deberá demostrar el nexo existente entre el caso notorio y la obligación pendiente de cumplimiento. La fuerza mayor solamente podrá afectar a la parte del contrato cuyo cumplimiento imposible fue probado.
3. No se considerarán casos de Fuerza Mayor los actos o acontecimientos que hagan el cumplimiento de una obligación únicamente más difícil o más onerosa para la parte correspondiente.
4. Si se presentara un evento de Fuerza Mayor, el proveedor notificará por escrito a la contratante sobre dicha condición y causa, en el plazo de siete (7) días calendario a partir del día siguiente en que el proveedor haya tenido conocimiento del evento o debiera haber tenido conocimiento del evento. Transcurrido el mencionado plazo, sin que el proveedor o contratista haya notificado a la convocante la situación que le impide cumplir con las condiciones contractuales, no podrá invocar caso fortuito o fuerza mayor. Excepcionalmente, la convocante bajo su responsabilidad, podrá aceptar la notificación del evento de caso fortuito en un plazo mayor, debiendo acreditar el interés público comprometido.
5. La fuerza mayor debe ser invocada con posterioridad a la suscripción del contrato y con anterioridad al vencimiento del plazo de cumplimiento de las obligaciones contractuales.
6. A menos que la contratante disponga otra cosa por escrito, el proveedor continuará cumpliendo con sus obligaciones en virtud del contrato en la medida que sea razonablemente práctico, y buscará todos los medios alternativos de cumplimiento que no estuviesen afectados por la situación de fuerza mayor existente.

## **Causales de terminación del contrato**

### **1. Terminación por Incumplimiento**

a) La Contratante, sin perjuicio de otros recursos a su disposición en caso de incumplimiento del contrato, podrá terminar el contrato, en cualquiera de las siguientes circunstancias:

- i. Si el proveedor no entrega parte o ninguno de los bienes dentro del período establecido en el contrato, o dentro de alguna prórroga otorgada por la contratante; o
- ii. Si el proveedor no cumple con cualquier otra obligación en virtud del contrato; o
- iii. Si el proveedor, a juicio de la contratante, durante el proceso de licitación o de ejecución del contrato, ha participado en actos de fraude y corrupción;
- iv. Cuando las multas por atraso superen el monto de la Garantía de Cumplimiento de Contrato;
- v. Por suspensión de los trabajos, imputable al proveedor o al contratista, por más de sesenta días calendarios, sin que medie fuerza mayor o caso fortuito;
- vi. En los demás casos previstos en este apartado.

### **2. Terminación por Insolvencia o quiebra**

La Contratante podrá rescindir el contrato mediante comunicación por escrito al proveedor si éste se declarase en quiebra o en estado de insolvencia.

### **3. Terminación por conveniencia**

a) La contratante podrá en cualquier momento terminar total o parcialmente el contrato por razones de interés público debidamente justificada, mediante notificación escrita al proveedor. La notificación indicará la razón de la terminación así como el alcance de la terminación con respecto a las obligaciones del proveedor, y la fecha en que se hace efectiva dicha terminación.

b) Los bienes que ya estén fabricados y estuviesen listos para ser enviados a la contratante dentro de los treinta (30) días siguientes a la fecha de recibo de la notificación de terminación del contrato deberán ser aceptados por la contratante de acuerdo con los términos y precios establecidos en el contrato. En cuanto al resto de los bienes la contratante podrá elegir entre las siguientes opciones:

- i. Que se complete alguna porción y se entregue de acuerdo con las condiciones y precios del contrato; y/o
- ii. Que se cancele la entrega restante y se pague al proveedor una suma convenida por aquellos bienes que hubiesen sido



parcialmente completados y por los materiales y repuestos adquiridos previamente por el proveedor.

## Otras causales de terminación del contrato

Además de las ya indicadas en la cláusula anterior, otras causales de terminación de contrato son:

No Aplica

## Resolución de Conflictos a través del Arbitraje

Las partes se someterán a Arbitraje:

Si

En caso que la Convocante adopte el arbitraje como mecanismo de resolución de conflicto, la cláusula arbitral que regirá a las partes es la siguiente:

"Todas las controversias que deriven del presente contrato o que guarden relación con éste serán resueltas definitivamente por arbitraje, conforme con las disposiciones de la ley N° 2051/03 "De Contrataciones Públicas", de la ley N° 1879/02 "De arbitraje y mediación" y las condiciones del Contrato. El procedimiento arbitral se llevará a cabo ante el Centro de Arbitraje y Mediación del Paraguay (en adelante, "CAMP"). El tribunal estará conformado por tres árbitros designados de la lista del cuerpo arbitral del CAMP, que decidirá conforme a derecho, siendo el laudo definitivo y vinculante para las partes. Se aplicará el reglamento respectivo y demás disposiciones que regule dicho procedimiento al momento de ser requerido, declarando las partes conocer y aceptar los vigentes, incluso en orden a su régimen de gastos y costas, considerándolos parte integrante del presente Contrato. Para la ejecución del laudo arbitral, o para dirimir cuestiones que no sean arbitrables, las partes se someterán a la jurisdicción de los tribunales de la ciudad de Asunción, República del Paraguay".

## Fraude y Corrupción

1. La Convocante exige que los participantes en los procedimientos de contratación, observen los más altos niveles éticos, ya sea durante el proceso de licitación o de ejecución de un contrato. La Convocante actuará frente a cualquier hecho o reclamación que se considere fraudulento o corrupto.

2. Si se comprueba que un funcionario público, o quien actúe en su lugar, y/o el oferente o adjudicatario propuesto en un proceso de contratación, hayan incurrido en prácticas fraudulentas o corruptas, la Convocante deberá:

(i) En la etapa de oferta, se descalificará cualquier oferta del oferente y/o rechazará cualquier propuesta de adjudicación relacionada con el proceso de adquisición o contratación de que se trate; y/o

(ii) Durante la ejecución del contrato, se rescindirá el contrato por causa imputable al proveedor;

(iii) Se remitirán los antecedentes del oferente o proveedor directamente involucrado en las prácticas fraudulentas o corruptivas, a la Dirección Nacional de Contrataciones Públicas, a los efectos de la aplicación de las sanciones previstas.

(iv) Se presentará la denuncia penal ante las instancias correspondientes si el hecho conocido se encontrare tipificado en la legislación penal.

Fraude y corrupción comprenden actos como:

(i) Ofrecer, dar, recibir o solicitar, directa o indirectamente, cualquier cosa de valor para influenciar las acciones de otra parte;

(ii) Cualquier acto u omisión, incluyendo la tergiversación de hechos y circunstancias, que engañen, o intenten engañar, a alguna parte para obtener un beneficio económico o de otra naturaleza o para evadir una obligación;

(iii) Perjudicar o causar daño, o amenazar con perjudicar o causar daño, directa o indirectamente, a cualquier parte o a sus bienes para influenciar las acciones de una parte;

(iv) Colusión o acuerdo entre dos o más partes realizado con la intención de alcanzar un propósito inapropiado, incluyendo influenciar en forma inapropiada las acciones de otra parte.

(v) Cualquier otro acto considerado como tal en la legislación vigente.

3. Los Oferentes deberán declarar que por sí mismos o a través de interpósita persona, se abstendrán de adoptar conductas orientadas a que los funcionarios o empleados de la convocante induzcan o alteren las evaluaciones de las propuestas, el resultado del procedimiento u otros aspectos que les otorguen condiciones más ventajosas con relación a los demás participantes (Declaratoria de Integridad).

# MODELO DE CONTRATO

Este modelo de contrato, constituye la proforma del contrato a ser utilizado una vez adjudicado al proveedor y en los plazos dispuestos para el efecto por la normativa vigente.

EL MODELO DE CONTRATO SE ENCUENTRA EN UN ARCHIVO ANEXO A ESTE DOCUMENTO.

# FORMULARIOS

Los formularios dispuestos en esta sección son los estándar a ser utilizados por los potenciales oferentes para la preparación de sus ofertas.

ESTA SECCIÓN DE FORMULARIOS SE ENCUENTRA EN UN ARCHIVO ANEXO A ESTE DOCUMENTO, DEBIENDO LA CONVOCANTE MANTENERLO EN FORMATO EDITABLE A FIN DE QUE EL OFERENTE LO PUEDA UTILIZAR EN LA PREPARACION DE SU OFERTA.

