



**PROCURADURÍA GENERAL
DE LA REPÚBLICA**

Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

ESPECIFICACIONES TÉCNICAS

Licitación Pública Nacional para la adquisición e instalación de sistema y equipos de seguridad y vigilancia para Recintos Penitenciarios del Plan de Humanización: (i) CCR La Nueva Victoria, (ii) CCR San Juan de la Maguana y (iii) Preventiva San Luis.

Referencia: PROCURADURÍA-CCC-LPN-2019-0008

SANTO DOMINGO, R. D.
Octubre 2019



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

ALTAVOZ

Altavoz de proyección bidireccional.

Power Taps @70V	2.5W, 5W, 10W
Power Taps @100V	5W, 10W, 20W
Impedance	Blue: Com Green: 2 K Ω Yellow: 1K Ω Red: 500 Ω
SPL(1W/1M)	92dB
Max. SPL (Rated W/1M)	105dB
Dimensions	172 x 252mm
Frequency Response (-10dB)	110-15KHz
Speaker Driver	6"x2
Finish	Baffle: Aluminum, White Grille: Steel, White
Speaker Driver	6"x2
IP Rate	IP 66
Weight	3.3Kg
Mounting	With mounting bracket fixed by screw

Altavoz tipo Bocina.

Power Taps @70V	7.5W, 15W
Power Taps @100V	15W, 30W
Impedance	Black: Com Green: 670 Ω White: 330 Ω
SPL(1W/1M)	103dB \pm 3dB
Max. SPL (Rated W/1M)	118dB
Frequency Response (-10dB)	300-13KHz
Dimensions	282 x 210 x 290mm
Finish	Baffle: ABS, White



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

IP Rate	IP66
Weight	2.1Kg
Mounting	With mounting bracket fixed by screw

Altavoz tipo columna.

Power Taps @70V	10W, 20W
Power Taps @100V	20W, 40W
Impedance	Black: Com Green:500Ω White:250Ω
SPL(1W/1M)	94dB±3dB
Max. SPL (Rated W/1M)	110dB±3dB
Frequency Response (-10dB)	130-18KHz
Dimensions	155 x 105 x 610mm
Finish	Body: Aluminum, White Grille: Aluminum, White Cover: ABS, White
Speaker Driver	4" x 4
IP Rate	IP 56
Weight	4Kg
Mounting	With mounting bracket fixed by screw

Intercomunicador (Micrófono de red IP, con pantalla táctil de 7 ").

Communication Protocol	TCP/IP,UDP,IGMP(multicast)
Audio Format	MP3/MP2
Sampling Rate	8K- 48Khz
Screen Resolution	800 x 480 pixel



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

Screen Type	65 k color DGUS screen
Keyboard Types	Virtual QWERTY keyboard
Transmission Speed	100Mbps
Audio Mode	16 digit stereo CD sound quality
Screen Size	7 inch
Keyboard Entry Method	Touch
Rate Power and Impedance of Build-in Speaker	4 Ω , 2W
THD	< 1%
Short-circuit input	Dry contact input
Short-circuit Output	Max 3A/120V Dry contact
Frequency Response	80Hz – 16Khz + 1dB/-3dB
S/N Ratio	>68dB
Rated Power and Impedance of PHONE OUT	32 Ω , 20mW
Level of LINE OUT	1000mV Industry-standard voltage wire terminals
Output Impedance of LINE OUT	470 Ω
Input Sensitivity of LINE IN	350mV Industry- standard voltage wire terminals
Input Sensitivity of MIC	10mV
Working Temp	5°C- 40°C
Humidity	20% - 80% Relative humidity, without condensation
Power Consumption	<6W
Power Supply	DC24V
Dimensions	200 x 160 x 60 mm
Weight	1.2Kg



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Amplificador de audio.

Potencia nominal 120W / 500W a impedancia constante a 4-16Ω o voltaje constante a 70V / 100V.

Con pantalla LCD de 3.4 "para mostrar el estado de funcionamiento de todos los altavoces.

Procesador DSP incorporado; el tiempo de impulso es inferior a 1 s

Decodificador de audio de red de 1 canal incorporado; soporte TCP / IP, UDP, IGMP; puede transmitir una señal de audio con calidad de CD de 16 bits.

1 entrada AUX y 1 MIC con control de volumen independiente y control de temblores y graves.

Prioridad: EMC> MIC> AUX y música de fondo

Montaje tipo rack.

CABLEADO ESTRUCTURADO

INTRODUCCIÓN.

Los oferentes deberán anexar los certificados correspondientes de cumplimiento con las normas mencionadas en el presente documento.

Suministro, instalación y configuración de todos los componentes del canal de cobre y accesorios, deben ser de una sola marca, a fin de garantizar la integridad y garantías correspondientes de la instalación. No se aceptarán ofertas donde se mezclen componentes o subsistemas de cableado de más de un (1) fabricante. Solo se aceptará en otra marca el sistema de fibra óptica, racks, gabinetes, PDU, bandejas ventiladas y organizadores.

Los oferentes deben presentar las evidencias físicas de que los materiales y elementos a suministrar cumplen con las normas y estándares establecidos. Los materiales tendrán identificadores de su respectiva marca para ser aceptados.

ESTÁNDARES.

El cableado estructurado debe cumplir con los siguientes estándares para infraestructura de telecomunicaciones:



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

ANSI: American National Standards Institute.

TIA: Telecommunications Industry Association.

EIA: Electrical Industries Alliance.

ISO: International Standards Organization.

IEC: International Electrotechnical Commission.

ANSI/TIA-568-D.1- Estándares de telecomunicaciones para premisas en edificios.

ANSI/TIA-568-D.2- Estándares de telecomunicaciones de par trenzado balanceado y sus componentes.

ANSI/TIA/EIA-569-D - Estándar para espacios y pasos de acceso en edificios. Se deben de seguir las prácticas de diseño y construcción dentro y entre edificios, hechas en soporte de medios y/o equipos de telecomunicaciones tales como canaletas y guías, facilidades de entrada al edificio, armarios, closet de comunicaciones y cuarto de equipos.

TIA-568-C.4 - Estándares para componentes coaxiales de banda ancha.

TIA-570 - Estándar para telecomunicaciones en infraestructuras.

ANSI/TIA-606-B - Estándar para administración de infraestructura de telecomunicaciones.

ANSI-J-STD-607-C - Requerimientos de aterrizaje, conexión, empalmes a tierra física para telecomunicaciones.

ANSI/TIA-758-B - Estándar para infraestructura planta externa propiedad del usuario.

ANSI/TIA-942-A - Estándar de infraestructura de telecomunicaciones para centros de datos.

ANSI/TIA-1005A - Estándar de infraestructura de telecomunicaciones para premisas industriales.

TIPOS DE CABLES, COMPONENTES, ZONAS DE TRABAJO Y RUTAS.

Todos los componentes del cableado estructurado de cobre deberán ser de un mismo fabricante tales como: cables de cobre, cables de empalme, conectores (jacks) RJ45, paneles de empalme, tapas de pared y cajas superficiales. La solución de cobre debe ser UTP completa. La solución de cableado debe contar con todas las certificaciones de la industria, dentro de las más conocidas: UL, ETL, ISO 9001, ANSI/TIA.

La responsabilidad por el buen funcionamiento y buena calidad de los elementos utilizados en la instalación de la red de cableado estructurados recaerá sobre el único fabricante de los productos utilizados.

El sistema de cableado estructurado se implementará en los siguientes subsistemas:

CABLEADO HORIZONTAL.

Se debe cumplir con lo estipulado en el estándar ANSI/TIA/EIA-569-D.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Las vías de cableado deben diseñarse e instalarse para cumplir con los reglamentos eléctricos y de construcciones aplicables, nacionales o locales para edificios.

El número de cables tendidos en una vía de cableado no deben sobrepasar las especificaciones del fabricante ni afectar la forma geométrica de los cables.

El radio máximo de curvatura del cable no debe sobrepasar las especificaciones del fabricante.

Se usarán sujetadores velcro para amarrar los cables en los cuartos de equipos y telecomunicaciones que requieran modificaciones o reconfiguraciones.

Los amarres deben utilizarse en intervalos adecuados para asegurar el cable y evitar deformaciones en los puntos de terminación, estos amarres no deben tensionarse en exceso hasta el punto de deformar o penetrar en la envoltura del cable.

CABLE DE COBRE CATEGORIA 6 UTP EN LAS AREAS DE TRABAJO.

Este cable debe cumplir o superar las especificaciones de la norma TIA/EIA 568-C.2, para especificaciones de desempeño de transmisión de cables de 4 pares y 100 Ohmios así como los requisitos de cable categoría 6 (clase E) de la norma ISO/IEC 11801 2da edición.

Dentro del cable, los pares deben estar separados entre sí por una barrera física tipo cruceta. Los conductores deben ser de cobre sólido calibre 23 AWG.

Los conductores deben de ser de cobre puro sin aleaciones de aluminio, acero u otros metales con aislante de polietileno HDPE.

El cable de soportar la transmisión de energía para dispositivos Power over Ethernet (PoE) cumpliendo con la especificación IEEE 802.3af PoE (12.95 Watts) y 802.3at PoE+ (25.5 Watts). La chaqueta del cable UTP debe ser del tipo CM o CMR, No Plenum y debe contar con certificado UL o ETL.

No se aceptarán cables LSZH, ni cables blindados.

Diámetro del cable: 5.7mm (0.225 pulg) nominal

Temperatura de operación: -20°C - 60°C (-4°F to 140°F)

Grado de flamabilidad: UL 1685 para CM o UL 1666 para CMR

CABLES DE EMPALME (PATCH CORD) CATEGORÍA 6 UTP.

El Patch Cord debe estar conformado solamente por cable de cobre multifilar Unshield Twisted Pair de 4 pares trenzados de Calibre 24 a 28 AWG, y con plugs modulares Rj45 de alto desempeño en cada extremo.

Los Patch Cords deberán ser ensamblados y probados 100% en fábrica.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Debe cumplir con las pruebas de performance de la ANSI/TIA-568-C.2 Categoría-6, certificados por Laboratorios independientes: UL o ETL.

Debido a que es UTP no deberán contar con ningún blindaje o malla eléctrica alrededor el plug.

Deberá cumplir con los requerimientos de IEEE 802.3af e IEEE 802.3at para aplicaciones PoE y PoE+ y el propuesto IEEE 802.3bt tipo 3 y tipo 4.

La longitud del Patch Cord deberá ser entregable en distancias 1 pie en adelante según se requiera en la aplicación.

Los Plug RJ45 de cada Patch Cord deben tener un sistema anti-enredo o capuchas como parte del Plug RJ45 para evitar atascos durante movimientos o reordenamiento y no deberán tener algún accesorio que amplíe sus dimensiones laterales.

Deberán permitir hasta 2500 ciclos de conexión.

Deberán estar identificados con la categoría y un número de control de calidad para futura rastreabilidad.

Deberá estar catalogado UL 1863.

El fabricante debe contar con al menos 10 colores distintos a fin de facilitar la administración.

Cubierta exterior del cable: Diámetro nominal 0.150 pulg (3.8mm) para calibre 28AWG.

Conductor: Calibre 28 AWG de cobre puro sin aleaciones de aluminio

Grado de flamabilidad: Retardante al fuego tipo CM/LSZH dual-rated (UL 1863)

Temperatura de Operación: -10°C to 75°C para calibre 28AWG.

FACEPLATES (TAPAS DE PARED).

Deberán instalarse face plates dobles por área de trabajo, la salida no utilizada deberá ir con tapa ciega.

Debe incluir sus tornillos de sujeción y etiquetas de identificación para cada puerto del Face Plate, con cobertor transparente.

Deberán estar fabricadas de material ABS.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Debe permitir la inserción de: jacks de categoría 6 o jacks de categoría 6A UTP, acopladores de fibra óptica o aplicaciones de audio y video, a fin de garantizar upgrades futuros.

Deberá estar disponible en al menos 5 colores distintos.

TERMINALES (JACKS) RJ45 CATEGORÍA 6.

Deben ser de categoría 6 de acuerdo con la ANSI/TIA-568-C.2

Deben ser de 8 posiciones tipo IDC, para conectorización sin herramienta de impacto.

Debe permitir la conectorización tipo T568A o T568B contando con una etiqueta que indique el método para ello.

Deberán contar con una certificación component compliance emitida por algún laboratorio neutral de pruebas tipo UL o ETL.

El jack podrá ser re terminado hasta 20 veces.

Deben asegurar la no desconexión del cable UTP sólido al ser expuesto a jalones, contando para ello con una tapa o seguro sobre las conexiones del cable UTP y las conexiones IDC.

Los pines de contacto deberán tener un baño de 50 micropulgadas de oro para garantizar el desempeño.

Deberá poder instalarse en las placas de pared y en los paneles de parcheo modulares.

Deberá contener un aliviador de tensión en la tapa de terminación para controlar el radio de curvatura.

Debe permitir la inserción de iconos plásticos.

El desempeño deberá estar 100% probado de fábrica.

Debe permitir la inserción de patch cord de 2 y 4 pares sin degradarse.

Debe permitir la terminación de cables UTP entre 22 – 26 AWG.

Deberá estar catalogado UL 1863.

Deberá cumplir con la directiva RoHS.

Debe permitir hasta 2500 ciclos de conexión La temperatura de operación debe estar el rango de -10°C to 75°C.

Debe cumplir con las normas IEC 60603-7, IEC 60512-99-001 y ANSI/TIA-1096-A.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Deberá cumplir con los requerimientos de IEEE 802.3af e IEEE 802.3at para aplicaciones PoE y PoE+ y el propuesto IEEE 802.3bt tipo 3 y tipo 4. Deberá soportar Power over HDBaseT hasta 100 watts.

El fabricante debe contar con al menos 10 colores distintos a fin de facilitar la administración.

PLUGS CERTIFICABLES DE TERMINACION EN CAMPO (FIELD PLUGS).

Los plugs deberán ser de 8 posiciones tipo IDC, de 2 piezas, para conectorización sin herramienta de impacto. Debe cumplir con IEEE 802.3af / 802.3at, 802.3bt tipo 3 y tipo 4 (Capaz de manejar aplicaciones HDBaseT hasta 100 watts).

Temperaturas de operación: -40°C to +75°C (-40°F to +167°F).

Deberán permitir la terminación de cables sólidos o multifilares de 22 a 26 AWG.

Deberán permitir hasta 2500 ciclos de conexión.

Debe cumplir con UL 1863, UL 2043, IEC 60603-7, IEC 60529 (IP 20).

Debe ser compatible con las categorías Cat5e/Cat6/Cat6A.

El plug deberá tener la opción de reinstalación (rearmado) por lo menos en 20 ocasiones sin deteriorar su comportamiento físico.

Para conexiones de cámaras, puntos de acceso (AP), aplicaciones de PoE Lighting y dispositivos IoT, se debe utilizar plug de terminación en campo, capaz de permitir la conexión directa del enlace horizontal, y a la vez, capaz de permitir la certificación de dicho enlace con un equipo de prueba de nivel 3.

PANELES DE EMPALME (PATCH PANELS) MODULARES.

Debe permitir la inserción de: 24 jacks de categoría 6 o 24 jacks de categoría 6A UTP o 24 acopladores LC dúplex en 1(RU) o 48 puertos en dos unidades de rack (2U), a fin de garantizar upgrades futuros.

Cada puerto frontal RJ45 debe soportar como mínimo 750 inserciones de Plug RJ45 de 8 posiciones de acuerdo a la IEC 60603-7.

Cada jack del patch panel debe cumplir con las pruebas de performance de la EIA/TIA 568C.2-1 Categoría-6, certificado por laboratorios independientes: UL o ETL.

Deben ser modulares puerto por puerto de tal forma que pueda ser posible cambiar un jack individualmente en caso de fallas y no se requiera tener que adquirir un bloque o módulo de 04 o 06 jacks ni tener que cambiar todo el Patch Panel.

Los conectores RJ45 ofertados para los patch panels deben permitir trabajar con el mapa de cables T568A o el T568B.

Debe tener 19 pulgadas de ancho para ser instalados en los racks o gabinetes.

Deben permitir la conexión total de las salidas de información de todas las aplicaciones (datos, voz, etc), perfectamente identificados en el panel, y con todos los requerimientos para facilitar la administración y manejo de la red, de acuerdo con la norma ANSI/TIA/EIA 606B.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Deben contar con una protección plástica transparente que impida el contacto directo de las manos u otros objetos con las etiquetas garantizando con ello su longevidad de acuerdo con la ANSI/TIA/EIA 606B.

La máscara el patch panel debe ser de material metálico.

Los Patch Panels deben permitir la instalación de los jacks ofertados.

Se deberán colocar módulos individuales / tapas de color negro en todos los puertos no utilizados del Patch Panel.

Deben contar con Certificación ISO 9001.

GABINETES, ORGANIZADORES HORIZONTALES Y PDU.

Deberá contar con 30 unidades de Rack (30U), con las siguientes dimensiones: 600 mm W x 800 mm D, color negro.

Deberá cumplir con las normas ANSI/EIA-310D.

La estructura del rack deberá ser capaz de soportar 1,500 libras.

Deberá incluir tornillos, tuercas, 4 piezas de ruedas y ajustadores, con dos estantes fijos y dos ventiladores para el gabinete.

Material: en acero laminado en frío.

Placa perforada para puerta de entrada.

Los organizadores horizontales deben ser plásticos y de 2 unidades de Rack.

Las PDU horizontal deben tener las siguientes características:

El tamaño debe ser de 1 unidad de rack.

6 salidas tipo NEMA 5-15R

Conector de corriente NEMA 5-15P.

Frecuencia de 50HZ/60HZ.

Voltaje de 100-120 V

GARANTÍA TÉCNICA.

La garantía de instalación que deberá presentar el Oferente/Proponente, debe ser emitida por el fabricante de la solución de cableado estructurado por un tiempo mínimo de 25 años, en la que se especifique la garantía de fabricación de los componentes.

Se debe incluir un informe impreso y electrónico de verificación por cada punto de los parámetros de performance según la ANSI/EIA-568C, requerida para el presente proceso, esto se realizará con un equipo certificador para medir parámetros de performance autorizado por el fabricante del sistema de cableado.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

La garantía deberá contemplar el cambio de componentes, incluyendo el servicio ante el incumplimiento por falla de origen de los componentes, falla de los parámetros de performance solicitados y por falla de las aplicaciones garantizadas. Estos cambios se realizarán a solicitud de la entidad y con la comprobación del oferente o fabricante del producto.

ESPECIFICACIONES FIBRA ÓPTICA

Cada fibra óptica deberá estar formada por núcleo de sílice dosificado con germania, rodeado por un revestimiento concéntrico de vidrio de sílice. La fibra será fabricada mediante el proceso de deposición de vapor externa (OVD Outside Vapor Deposition).

La fibra se recubre con una capa de acrilato de protección dual y el recubrimiento debe estar en contacto físico con la superficie de revestimiento. La fibra monomodo deberá cumplir con los estándares ITU-T G.652.D”.

Descripción	Unidad	Requisito
Estándares Internacionales	NA	ITU-T G.652.D
Tipo de fibra		Fibra Monomodo
Longitud de onda de Operación	nm	1310 y 1550
Protección (Coating)		<i>Acrilato</i>
Atenuación Máxima a 1310nm	dB/km	≤0.32
Atenuación Máxima a 1550nm	dB/km	≤0.18
Dispersión Cromática (1550nm)	ps/nm.km	≤18
Pendiente de dispersión cero	ps/nm.km	≤0.092
Longitud de onda de dispersión nula	nm	1304≤≤≤≤≤1324
Diseño/ Método de Fabricación		<i>OVD (Método de Deposición externa de Vapor)</i>
Diámetro del núcleo típico	μm	8.2



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

Diámetro de campo modal a 1310nm	μm	9.2 ±0.4
Diámetro de campo modal a 1550nm	μm	10.4±0.5
No-circularidad de Recubrimiento (cladding)	%	0.7
Concentricidad del núcleo – recubrimiento cladding	μm	± 0,5
PMD Link según IEC 60794-3 2001	ps/μkm	± 0,04
Máximo por fibra individual	ps/μkm	± 0,1
Incremento de atenuación por doblado de 100 vueltas sobre un mandril de 25mm de diámetro a 1310nm,1550nm y 1625nm	dB/km	± 0,01
Incremento de atenuación por doblado de 10 vueltas sobre un mandril de 15mm de diámetro a 1550nm	dB/km	± 0,05
Incremento de atenuación por variación de temperatura (entre –60° C y +85° C) en ambas longitudes de onda (1310 nm y 1550 nm)	dB/km	± 0,05
Índice de Refracción (Neff)	1310nm	1.4676
Índice de Refracción (Neff)	1550nm	1.4682

ESPECIFICACIONES DEL CABLE – PLANTA INTERNA - EXTERNA (INDOOR/OUTDOOR).

Consideraciones Generales

El cable deberá cumplir con todos los requerimientos mencionados en esta especificación, así como con los requerimientos del código eléctrico NEC, sección 770, diseñado para aplicaciones verticales de acuerdo a las pruebas de flamabilidad UL 1666 OFNR.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Los cables terminados deben cumplir con los requisitos de rendimiento aplicables de la Norma de la Asociación de Ingenieros de Cables Aislados, Inc. (ICEA) para Cable de Fibra Óptica para Exteriores (ICEA S-104-696).

Construcción del Cable

- Las fibras ópticas se colocarán dentro de un tubo holgado. El diámetro externo del tubo holgado será de 2,5 mm. Las fibras no deben adherirse al interior del tubo holgado.
- Cada tubo deberá contener hasta 12 fibras.
- Cada fibra se podrá distinguir mediante una codificación de colores de acuerdo con TIA / EIA-598, "Codificación de color del cable de fibra óptica".

1. Azul	7. Rojo
2. Naranja	8. Negro
3. Verde	9. Amarillo
4. Marrón	10. Violeta
5. Gris	11. Rosa
6. Blanco	12. Aqua

- Las fibras se colorearán con tintas curables por ultravioleta (UV), en tubos de amortiguación que contienen múltiples fibras, los colores deben ser estables en todo el almacenamiento especificado y rangos de temperatura de funcionamiento y no están sujetos a decoloración o manchado el uno al otro. Los colores no harán que las fibras se peguen entre sí.
- Las fibras ópticas no requerirán limpiarse antes de colocarlas en una bandeja de empalme o fan-out kit.
- Los tubos holgados deberán ser resistentes al enroscamiento.
- Cada tubo de protección deberá contener un elemento de bloqueo de agua. El elemento bloqueante de agua no será nutritivo para los hongos, eléctricamente no conductor y homogéneo. También debe estar libre de suciedad. Este elemento impedirá la necesidad de otro elemento de bloqueo del agua. Los tubos holgados deben estar libres de gel.
- Los cables se revestirán con cloruro de polivinilo (PVC) ignífugo. El material de revestimiento se aplicará directamente sobre los elementos de resistencia a la



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

tracción y cinta de bloqueo de agua. El PVC debe contener un compuesto estabilizador UV para proporcionar protección contra la luz ultravioleta y no promoverá el crecimiento de hongos.

- Las fundas de los cables se deberán poder colorear de cualquiera de los 12 colores identificados en EIA / TIA-598, "Codificación de color del cable de fibra óptica". Las chaquetas de colores deben contener estabilizadores UV.
- Chaqueta ignífuga resistente a los rayos UV. Robusto, duradero y fácil de pelar.
- La chaqueta debe ser continua, libre de poros, fracturas, ampollas u otras imperfecciones. La chaqueta debe tener un espesor uniforme y lisa; chaquetas de material extruido a alta presión No son aceptables. La cubierta debe proporcionar al cable un revestimiento resistente, flexible y protector, capaz de soportar las tensiones esperadas en la instalación y servicio normales.
- Las chaquetas de los cables se marcarán con el nombre del fabricante o el número de archivo, mes y año de fabricación, marcas secuenciales del medidor o del pie, un símbolo del teléfono de telecomunicaciones como lo requiere la Sección 350G del Código Nacional de seguridad eléctrica (NESC), número de fibras y tipo de fibra, clasificación de llama y listado de marcado. La longitud real del cable debe estar dentro del 0 y el 1% de las marcas de longitud. El color de impresión de las letras de la chaqueta debe blanco.
- La tensión máxima de tracción será de 1350 N (300 lbf) durante la instalación (a corto plazo); y 400 N (90 lbf) a largo plazo para el cable ya instalado.

Misceláneos

La atenuación de todas las fibras del cable deberán someterse a pruebas de atenuación en un 100%. La atenuación de cada fibra deberá ser proveída con cada carrete de cable.

El fabricante del cable y vidrio deberá ser el mismo para garantizar la calidad y la trazabilidad en todas las etapas del proceso de fabricación.

El fabricante del cable debe estar registrado con ISO-9001 y TL-9000.

Sus laboratorios para pruebas mecánicas deberán estar certificados por la IAS Accreditation Criteria for Testing Laboratories (AC89) y demostrar cumplimiento a la norma ANS/ISO/IEC Standard 17025:2005, "General Criteria for the Competence of Testing and Calibration Laboratories".



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Presentar Carta del Fabricante Certificando una garantía mínima de 20 años para la Fibra.

CÁMARAS DE VIDEO VIGILANCIA

CÁMARA 1:

Cámara tipo Domo de 5MP, 1080p, f= 2.7 ~ 13.5 mm.

- 30 fps @ 2560x1920, 60 fps @ 1920x1080.
- Requerimientos de alimentación.
 - PoE
 - 12VDC.
- Tecnología de compresión H.265.
- Optimización del ancho de banda.
- Iluminadores IR incorporados, efectivos hasta 50 metros.
- SNV (Visibilidad nocturna suprema) para condiciones de poca luz.
- WDR (120dB) para una visibilidad incomparable en entornos extremadamente brillantes y oscuros.
- Detección inteligente de movimiento para reducir falsas alarmas.
- Admite el estándar ONVIF para simplificar la integración y mejorar la interoperabilidad.
- La cámara deberá proporcionar la función ePTZ de zoom digital de 48x (4x en el plug-in Internet Explorer, 12x incorporado).
- La cámara debe de proveer los siguientes 4 tipos de tamper.
 - Alarma por detección de tamper normal (bloqueo de cámara).
 - Alarma de tamper cuando la imagen se encuentra demasiado oscura.
 - Alarma de tamper cuando la imagen se encuentra demasiado brillante.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Alarma de tamper cuando la imagen se encuentra demasiado borrosa.
- Incluye:
 - Software de seguridad para protección contra ataques cibernéticos.
 - Detección y prevención de intrusiones.
 - Protección en los diferentes niveles del modelo OSI.
 - Protección automática del dispositivo, bloqueando direcciones IP y evitando nuevos ataques. Si detecta algún acceso anormal dentro de la cámara (por ejemplo, una conexión sospechosa de la cámara a una dirección IP maliciosa), el sistema pondrá en cuarentena el comportamiento del ataque para evitar daños mayores.
- La cámara debe tener un sensor de golpe incorporado para detectar si la cámara fue golpeada físicamente.
- Resistente a la intemperie, IP67 y a prueba de vandalismo IK10.
- Garantía 36 meses.

CÁMARA 2:

Cámara tipo Bullet de 5MP, 1080p, f= 2.7 ~ 13.5 mm.

- 30 fps @ 2560x1920, 60 fps @ 1920x1080.
- Requerimientos de alimentación
 - PoE
 - 12VDC.
- Tecnología de compresión H.265.
- Optimización del ancho de banda.
- SNV (Visibilidad nocturna suprema) para condiciones de poca luz.
- WDR (120dB) para una visibilidad incomparable en entornos extremadamente brillantes y oscuros.
- Iluminadores IR incorporados, efectivos hasta 50 metros.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Detección inteligente de movimiento para reducir falsas alarmas.
- La cámara debe de proveer los siguientes 4 tipos de tamper.
 - Alarma por detección de tamper normal (bloqueo de cámara).
 - Alarma de tamper cuando la imagen se encuentra demasiado oscura.
 - Alarma de tamper cuando la imagen se encuentra demasiado brillante.
 - Alarma de tamper cuando la imagen se encuentra demasiado borrosa.
- Incluye:
 - Software de seguridad para protección contra ataque cibernéticos.
 - Detección y prevención de intrusiones.
 - Protección en los diferentes niveles del modelo OSI.
 - Protección automática del dispositivo, bloqueando direcciones IP y evitando nuevos ataques. Si detecta algún acceso anormal dentro de la cámara (por ejemplo, una conexión sospechosa de la cámara a una dirección IP maliciosa), el sistema pondrá en cuarentena el comportamiento del ataque para evitar daños mayores.
- Admite el estándar ONVIF para simplificar la integración y mejorar la interoperabilidad.
- La cámara deberá proporcionar la función ePTZ de zoom digital de 48x (4x en el plug-in Internet Explorer, 12x incorporado).
- Resistente a la intemperie, IP67 y a prueba de vandalismo IK10.
- Garantía 36 meses.

CÁMARA 3:

Cámara tipo PTZ de 2MP.

- Compresión H.265, H.264 y MJPEG en tiempo real (códec triple).
- 60 fps a 1080p Full HD.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Lente zoom 30x.
- Optimización del ancho de banda.
- IR de 250 M con IR inteligente (IR de ángulo variable).
- WDR (120dB) para una visibilidad incomparable en entornos de alto contraste.
- 0 ° C ~ 55 ° Amplio rango de temperatura para condiciones climáticas extremas.
- Requerimientos de alimentación
 - PoE
 - 24VDC.
 - 24VAC
- EIS (Estabilización electrónica de imagen) para controlar la estabilidad de la imagen.
- Admite el estándar ONVIF para simplificar la integración y mejorar la interoperabilidad.
- Incluye:
 - Software de seguridad para protección contra ataque cibernético.
 - Detección y prevención de intrusiones.
 - Resistente a la intemperie, IP67 y a prueba de vandalismo IK10.
 - Protección automática del dispositivo, bloqueando direcciones IP evitando nuevos ataques. Si detecta algún acceso anormal dentro de la cámara (por ejemplo, una conexión sospechosa de la cámara a una dirección IP maliciosa), el sistema pondrá en cuarentena el comportamiento del ataque para evitar daños mayores
 - Protección en los diferentes niveles del modelo OSI.
 - Garantía 36 meses.

CÁMARA 4:

Cámara infrarroja.

- Detector infrarrojo VOx sin enfriar.
- f=8.8~19mm.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Detección inteligente de movimiento para reducir falsas alarmas.
- 384x256 Resolución.
- NETD <50 mk @ F1.0.
- Tecnología de compresión H.265.
- Requerimientos de alimentación
 - PoE
 - 12VDC.
 - 24VAC
- Incluye:
 - Software de seguridad para protección contra ataque cibernético.
 - Detección y prevención de intrusiones.
 - Protección en los diferentes niveles del modelo OSI.
 - Protección automática del dispositivo, bloqueando direcciones IP y evitando nuevos ataques. Si detecta algún acceso anormal dentro de la cámara (por ejemplo, una conexión sospechosa de la cámara a una dirección IP maliciosa), el sistema pondrá en cuarentena el comportamiento del ataque para evitar daños mayores.
- Audio bidireccional.
- Admite el estándar ONVIF para simplificar la integración y mejorar la interoperabilidad.
- Resistente a la intemperie IP67, a prueba de vandalismo IK10.
- Garantía 36 meses.

CÁMARA 5:

Cámara analítica LPR 2MP.

- 60 fps @ 1920x1080.
- 4 ~ 9 mm, enfoque remoto, lente P-iris.
- Optimización del ancho de banda.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- SNV (visibilidad nocturna suprema) para condiciones de poca luz.
- WDR (140dB) para proporcionar una visibilidad extrema en entornos extremadamente brillantes u oscuros.
- Iluminadores IR incorporados, efectivos hasta 50 metros.
- La cámara debe tener HLC (Highlight Compensation), la cual detecta una fuente de luz muy alta, como luces de vehículos o linternas en la oscuridad, y procede a disminuirla en la imagen capturada para facilitar el monitoreo.
 - Requerimientos de alimentación
 - PoE
 - 12VDC.
 - 24VAC
- Tecnología inteligente IR para evitar la sobreexposición.
- Detección inteligente de movimiento para reducir falsas alarmas.
- Admite el estándar ONVIF para simplificar la integración y mejorar la interoperabilidad.
- La cámara deberá proporcionar la función ePTZ de zoom digital de 48x (4x en el plugin Internet Explorer, 12x incorporado).
- La cámara debe de proveer los siguientes 4 tipos de tamper.
 - Alarma por detección de tamper normal (bloqueo de cámara).
 - Alarma de tamper cuando la imagen se encuentra demasiado oscura.
 - Alarma de tamper cuando la imagen se encuentra demasiado brillante.
 - Alarma de tamper cuando la imagen se encuentra demasiado borrosa.
- Incluye:
 - Software de seguridad para protección contra ataque cibernético.
 - Detección y prevención de intrusiones.
 - Protección en los diferentes niveles del modelo OSI.
 - Protección automática del dispositivo, bloqueando direcciones IP y evitando nuevos ataques. Si detecta algún acceso anormal dentro de la cámara (por ejemplo, una conexión sospechosa de la cámara a una dirección IP maliciosa), el sistema pondrá en cuarentena el



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

comportamiento del ataque para evitar daños mayores.

- Resistente a la intemperie IP67, a prueba de vandalismo IK10.
- Garantía 36 meses.

CÁMARA 6:

Cámara analítica facial 2MP.

- 60 fps @ 1920x1080.
- 12 ~ 40 mm, enfoque remoto, lente P-iris.
- Optimización del ancho de banda.
- SNV (visibilidad nocturna suprema) para condiciones de poca luz.
- WDR (140dB) para proporcionar una visibilidad extrema en entornos extremadamente brillantes u oscuros.
- La cámara debe tener HLC (Highlight Compensation), la cual detecta una fuente de luz muy alta, como luces de vehículos o linternas en la oscuridad, y procede a disminuirla en la imagen capturada para facilitar el monitoreo.
- Iluminadores IR incorporados, efectivos hasta 100 metros.
 - Requerimientos de alimentación
 - PoE
 - 12VDC.
 - 24VAC
- Tecnología inteligente IR para evitar la sobreexposición.
- Detección inteligente de movimiento para reducir falsas alarmas.
- Admite el estándar ONVIF para simplificar la integración y mejorar la interoperabilidad.
- La cámara deberá proporcionar la función ePTZ de zoom digital de 48x (4x en el plugin Internet Explorer, 12x incorporado).
- La cámara debe de proveer los siguientes 4 tipos de tamper.
 - Alarma por detección de tamper normal (bloqueo de cámara).
 - Alarma de tamper cuando la imagen se encuentra demasiado oscura.
 - Alarma de tamper cuando la imagen se encuentra demasiado brillante.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Alarma de tamper cuando la imagen se encuentra demasiado borrosa.
- Incluye:
 - Software de seguridad para protección contra ataque cibernéticos.
 - Detección y prevención de intrusiones.
 - Protección en los diferentes niveles del modelo OSI.
 - Protección automática del dispositivo, bloqueando direcciones IP y evitando nuevos ataques. Si detecta algún acceso anormal dentro de la cámara (por ejemplo, una conexión sospechosa de la cámara a una dirección IP maliciosa), el sistema pondrá en cuarentena el comportamiento del ataque para evitar daños mayores.
- Resistente a la intemperie IP67, a prueba de vandalismo IK10.
- Garantía 36 meses.

SISTEMA DE CONTROL DE ACCESO.

SOFTWARE DE GESTIÓN DE CONTROL DE ACCESO

Los requisitos mínimos de PC para la instalación del Software de Gestión de Control de Acceso son:

SERVIDOR:

- Procesador Intel Core i5 (Mínimo).
- Memoria RAM de (8) GB (Mínimo).
- Espacio mínimo libre en Disco Duro (10 GB Instalación y 500 GB para funcionamiento).

CLIENTE:

- Procesador Intel Core i5 (Mínimo)
- Memoria RAM de (6) GB (Mínimo).
- Espacio mínimo libre en Disco Duro (10 GB para funcionamiento)



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

El software de Gestión de control de acceso deberá poseer las siguientes características:

- Ser compatible con sistemas operativos Windows en sus versiones 32 y 64 Bits para versiones Pro y Server.
- Poseer como opción un sistema de enrutamiento TCP/IP secundario de Back Up por si la red principal de comunicación sufre alguna afectación.
- Tener arquitectura cliente – servidor y por lo menos 10 estaciones de trabajo incluidas.
- Poseer diferentes niveles de seguridad de acuerdo con los usuarios del sistema.
- Contar con una conexión remota por servicio Cliente Web desde un explorador de internet o aplicativo móvil que permita la gestión y programación en caso de emergencia desde un teléfono móvil inteligente previamente configurado para tal fin de ser necesario.
- Contar con mapas interactivos donde se puedan utilizar formatos DGW de AutoCAD o en su defecto imágenes convencionales JPG o similares con el fin que desde estos mapas se pueda interactuar de manera remota con los diferentes puntos de acceso de manera gráfica.
- Permitir la generación de reportes automatizados por evento o por agendamiento.
- Utilizar como motor de base de datos MS SQL Server y debe permitir el enrolamiento de por lo menos 1500 Lectores.
- Poseer integración con VMS y Sistemas de CCTV tales como cámaras y grabadores de red de terceros. Esta integración debe existir a la fecha con la marca de VMS que el oferente presente en el presente proyecto hacia la entidad para ser adquirida en el presente proceso. Esto debe ser soportado por carta del fabricante (No distribuidor o canal directo del fabricante) dirigida al proceso y firmada por el representante de la región o superior del fabricante del control de acceso a ofertar.
- Tener desarrollado a la fecha el poder controlar puertas o puntos de acceso con y sin lector de manera remota de ser requerido en el futuro.
- Capacidad de crecimiento ilimitado utilizando licenciamientos adicionales de ser necesarios en el futuro.
- Operar de forma centralizada y remota, es decir, podrá configurar los controladores centralizadamente y podrá recibir los diferentes eventos desde los controladores remotamente.
- Permitir la utilización de puertas virtuales en salidas de emergencia de ser requerido en el futuro.
- Ser del mismo fabricante que el resto de los elementos que componen la arquitectura de diseño del sistema, incluyendo de manera concreta y puntual controladores y lectores del sistema.
- Contar con la opción de Antipassback Local y Global.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Contar con formatos de tarjetas preconstituidos dentro de la plataforma y para ser utilizados bastará la escogencia de la casilla correspondiente para tal fin, no deberá existir la necesidad de crear estos formatos desde cero en el software, deberá contar, entre otros, con formatos de 35, 37, 48 y 50 Bits preconstituidos de esta manera.
- Contar con la opción de visualización de las fotografías de los usuarios del sistema en tiempo real por medio de pop up automático de ser necesario al momento del paso de la tarjeta por el sistema de lectura.

El software de gestión de control de acceso deberá estar en la capacidad de realizar las siguientes funciones:

1. Comunicación a terceros por medio de una dirección IP y puerto específico indicando eventos del sistema de manera paralela al diligenciamiento a la base de datos que utilice el sistema.
2. Carga masiva de base de datos otorgada por la Institución hacia el software de gestión de control de acceso.
3. Integración a la fecha (No desarrollos posteriores) con lectores Biométricos Monomarca que utilicen la misma plataforma de gestión dentro del mismo software para crecimiento posterior en esta tecnología.
4. Diligenciamiento de una base de datos de terceros de manera paralela al diligenciamiento a la base de datos que utilice el sistema.
5. Poseer en un licenciamiento a la fecha (No desarrollos posteriores) una forma de comunicación de protocolo abierto por IP - OPC (Open Protocol Communication) para integración con terceros de ser necesaria.

El Oferente/Proponente deberá entregar carta, no mayor de 30 días antes de la presentación de la oferta, firmada por el fabricante de control de acceso ofertado, donde el fabricante avale al oferente para Comercializar, Instalar, Mantener y soportar la línea de negocios ofertada del fabricante en cuestión. (No distribuidor o canal directo del fabricante) dirigida al proceso y firmada por el representante de la región o superior del fabricante de control de acceso a ofertar.

CONTROLADOR MAESTRO DE ACCESO TIPO PARED.

CARACTERÍSTICAS

El Controlador Maestro de Acceso deberá:



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Ser tipo montaje pared que no requiera gabinete para ser instalado, cubierta de aluminio o similar, no PCB (Protoboard Circuit Board), con entradas o conexiones mínimas para 2 lectoras por medio de conexión Wiegand.
- Poseer arquitectura modular, puerto de red Ethernet 10/100.
- Crecer hasta por lo menos 8 lectoras por red local de controladores utilizando las controladoras esclavas descritas en el presente documento.
- Enrolar hasta 50.000 tarjetas y poseer memoria para históricos en desconexión de al menos 30.000 en caso de pérdida de conexión con el Software de gestión de control de acceso.
- Contar con al menos 3 puertos de comunicación tipo RS485.
- Proporcionar datos reales en los eventos enviados hacia la base de datos una vez sea restablecida la comunicación con el software de gestión de control de acceso.
- Permitir la utilización de reglas del sistema en las que al pasar un número determinado de veces la tarjeta por uno de sus lectores, una zona determinada del sistema quede con acceso limitado o nivel de mayor o alta seguridad hasta tanto no se desactive esta función de la misma manera.
- Manejar un mínimo de 5 formatos concurrentes por controlador, salidas tipo relay programables y deberá contar con fuente reguladora de voltaje que de ser requerido tome de manera automática la energía de una fuente de corriente directa, alterna a la alimentación convencional de corriente alterna.
- Permitir la utilización de formatos de tarjeta de 48 Bits o superior.
- Ser de la misma marca y fabricante que el sistema de gestión de control de acceso ofertado.
- Contar con protección térmica embebida en Alimentación de Entrada, Salida y en la Alimentación hacia las Lectoras.
- Luego de ser configurado de manera inicial, deberá poder operar de forma Stand Alone sin intervención alguna del software de gestión de control de acceso u otro sistema alternativo, siempre de manera local, para evitar fallas en su funcionamiento si el servidor por cualquier motivo pierde conexión con el controlador.
- De manera local, de ser necesario, operar la misma cantidad mínima de lectoras por módulo controlador en configuración puerta exclusiva local.
- Poseer por lo menos 4 diferentes leds en total para la visualización de estado y funcionamiento. Y por lo menos 2 leds de diferente color para visualización de operación de transmisión y recepción (conectividad con el software de gestión de control de acceso).
- Utilizar para su comunicación Wiegand y Serial el cable tipo AWG 20 - 22, blindado. Esto debe estar indicado en la hoja de datos del equipo proveniente directamente del fabricante.
- En caso de perder alimentación vía suministro eléctrico de una fuente regulada externa interconectada a él, de manera simultánea, deberá tomar para sí de manera automática



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

un respaldo de energía de batería externa utilizando una conexión de batería directa y embebida a él mismo y sin intermediación alguna de una fuente de alimentación externa que cuente con una batería de respaldo para sí misma.

- Deberá permitir la utilización de formatos de tarjeta de 48 Bits o superior.
- Poder comunicar por medio de sus puertos RS-485 a una distancia máxima de 1200 metros y por medio de sus puertos Weigand a una distancia máxima de 150 metros. Esto debe estar indicado en la hoja de datos del equipo proveniente directamente del fabricante.
- Contar con por lo menos una salida auxiliar de contacto seco y una salida TTL adicional, diferente a la utilizada para liberar el sistema del torniquete / Electroimán o puerta de Minusválidos, para ser utilizada en cualquier integración que se requiera a futuro con otro sistema existente en la entidad.

CONTROLADOR MAESTRO DE ACCESO TIPO RACK.

CARACTERÍSTICAS.

El Controlador Maestro de Acceso deberá:

- Ser tipo montaje rack, cubierta de aluminio o similar para unidades de rack estándar con entradas o conexiones mínimas para 2 lectoras por medio de conexión Wiegand.
- Poseer arquitectura modular, puerto de red Ethernet 10/100.
- Contar con al menos 1 puerto de comunicación tipo RS48.
- Crecer hasta por lo menos 8 lectoras por red local de controladores utilizando las controladoras esclavas descritas en el presente documento.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Enrolar hasta 50.000 tarjetas y poseer memoria para históricos en desconexión de al menos 30.000 en caso de pérdida de conexión con el Software de gestión de control de acceso.
- Proporcionar datos reales en los eventos enviados hacia la base de datos una vez sea restablecida la comunicación con el software de gestión de control de acceso.
- Permitir la utilización de reglas del sistema en las que al pasar un número determinado de veces la tarjeta por uno de sus lectores, una zona determinada del sistema quede con acceso limitado o nivel de mayor o alta seguridad hasta tanto no se desactive esta función de la misma manera.
- Manejar un mínimo de 5 formatos concurrentes por controlador, salidas tipo relay programables y deberá contar con fuente reguladora de voltaje que de ser requerido tome de manera automática la energía de una fuente de corriente directa, alterna a la alimentación convencional de corriente alterna.
- Permitir la utilización de formatos de tarjeta de 48 Bits o superior.
- Ser de la misma marca y fabricante que el sistema de gestión de control de acceso ofertado.
- Contar con protección térmica embebida en Alimentación de Entrada, Salida y en la Alimentación hacia las Lectoras.
- Luego de ser configurado de manera inicial deberá poder operar de forma Stand Alone sin intervención alguna del software de gestión de control de acceso u otro sistema alterno, siempre de manera local para evitar fallas en su funcionamiento si el servidor por cualquier motivo pierde conexión con el Controlador.
- Poseer por lo menos poseer 4 diferentes leds en total para la visualización de estado y funcionamiento. Y por lo menos dos leds de diferente color para visualización de operación de transmisión y recepción (conectividad con el software de gestión de control de acceso).
- De manera local, de ser necesario, operar la misma cantidad mínima de lectoras por módulo controlador en configuración puerta exclusiva local.
- Utilizar para su comunicación Wiegand y Serial el cable tipo AWG 20 - 22, blindado. Esto debe estar indicado en la hoja de datos del equipo proveniente directamente del fabricante.
- En caso de perder alimentación vía suministro eléctrico de una fuente regulada externa interconectada a él, de manera simultánea, deberá tomar para sí de manera automática un respaldo de energía de batería externa utilizando una conexión de batería directa y



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

embebida a él mismo y sin intermediación alguna de una fuente de alimentación externa que cuente con una batería de respaldo para sí misma.

- Comunicar por medio de sus puertos RS-485 a una distancia máxima de 1200 metros y por medio de sus puertos Weigand a una distancia máxima de 150 metros. Esto debe estar indicado en la hoja de datos del equipo proveniente directamente del fabricante.
Contar con por lo menos una salida auxiliar de contacto seco y una salida TTL adicional, diferente a la utilizada para liberar el sistema del torniquete / electroimán o puerta de Minusválidos, para ser utilizada en cualquier integración que se requiera a futuro con otro sistema existente en la entidad.

CONTROLADOR ESCLAVO DE ACCESO.

CARACTERISTICAS.

El Controlador Esclavo de Acceso deberá:

- Contar con al menos 1 puerto de comunicación tipo RS485.
- Enrolar hasta 50.000 tarjetas y poseer memoria para históricos en desconexión de al menos 30.000 en caso de pérdida de conexión con el Software de gestión de control de acceso, dependientes del controlador maestro de acceso en todo momento.
- Poseer por lo menos 3 diferentes leds en total para la visualización de estado y funcionamiento. Y por lo menos 2 leds de diferente color para visualización de operación de transmisión y recepción (conectividad con el software de gestión de control de acceso).
- Permitir la utilización de formatos de tarjeta de 48 Bits o superior.
- Utilizar para su comunicación Wiegand el cable tipo AWG 20 - 22, trenzado y blindado, así como para su comunicación Serial el cable tipo AWG 18, trenzado y blindado. Esto debe estar indicado en la hoja de datos del equipo proveniente directamente del fabricante.
- Comunicar por medio de sus puertos RS-485 a una distancia máxima de 1200 metros y por medio de sus puertos Weigand a una distancia máxima de 150 metros. Esto debe estar indicado en la hoja de datos del equipo proveniente directamente del fabricante.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

LECTOR DEL SISTEMA.

CARACTERÍSTICAS.

El lector deberá:

- Estar diseñado para uso con tarjetas tipo sin contacto, material resistente, montaje vertical u horizontal en interiores y en exteriores.
- Contar con certificación Internal Protection mínima IP67 y un bajo consumo de energía.
- Incluir garantía de por vida.
- Operar a una frecuencia de 13.56 Mhz.
- Incluir puerto de comunicación OSDP Versión 1 o Versión 2, compatible 100% con los controladores de acceso ofertados.
- Contar con led indicador de actividad, rango de temperatura de operación de mínima de 0 a 65 grados centígrados.
- Operar con un voltaje de alimentación de 9 a 15 VDC, y contar con certificaciones CE y FCC.
- Operar dependiendo de un controlador maestro de acceso, pero sin intervención alguna del Servidor u otro sistema alternativo, siempre de manera local entre estos.

TARJETAS DEL SISTEMA.

CARACTERÍSTICAS.

Las tarjetas deberán:

- Operar con frecuencia de 13.56 Mhz - sin contacto, formato de bits controlado directamente por el fabricante igual o superior a 48 Bits.
- Cumplir con el estándar CR-80.
- Cumplir con el formato ISO / IEC 14443.
- Ser tipo Imprimibles y contar con mínimo 2KB interno.

La numeración de las tarjetas debe ser controlada directamente por el fabricante de la solución de control de acceso, esto deberá estar soportado por carta emitida donde el fabricante lo certifique. (No distribuidor o canal directo del fabricante) dirigida al proceso y firmada por el representante de la región o superior del fabricante de control de acceso a ofertar.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

CERRADURA ELECTRICA MOTORIZADA TIPO GANCHO (PICO DE LORO) 35/25MM.

Cerradura Eléctrica motorizada Cilindro de Alta Seguridad de Gancho o pico de loro, que incluya funciones de monitoreo y resistencia a sabotaje. Cerradura de perfil escandinavo, cerrojo con 5 placas internas tipo gancho, modo día/noche, monitoreo de puerta abierta y puerta cerrada en la misma cerradura, estatus de la puerta en la misma cerradura, uso de cilindro.

- Cilindros de Alta Seguridad deben incluir 2 llaves por cilindro y 3 llaves maestras.

CERRADURA ELECTRICA MOTORIZADA 60/24mm.

Cerradura Eléctrica motorizada Cilindro de Alta Seguridad, que incluya funciones de monitoreo y resistencia a sabotaje. Cerrojo motorizado, pestillo de doble acción, bloqueo automático al cierre de la puerta, modo día/noche, cerrojo de 20mm, sensores de monitoreo dentro de la cerradura en: estatus de la puerta, manipulación de manillas, cerrojo adentro, cerrojo fuera, uso de cilindro, sensor de sabotaje. Voltaje de 12/24 Volts, unidad de control resistencia para puertas cortafuego, consumo máximo de 1300mAmp.

- Cilindros de Alta Seguridad deben incluir 2 llaves por cilindro y 3 llaves maestras.

MODULO CIERRAPUERTA.

Módulo de cierra puerta para puertas de hasta 120kg, Grado de resistencia 2-6EN, Presión de aceite y resorte, Sistema de Rack y piñón, Certificación UL, Función de -35°C - +45°C, Dos válvulas de regulación de presión, Ajuste de retraso de cierre DA. Función de Velocidad de apertura BC. Debe cumplir con la norma EN1154 o UL228.



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

EQUIPOS DETECCIÓN

ARCO DETECTOR METALES

Nivel de sensibilidad: 100

Cada nivel de sensibilidad de zona: 255 (ajustable)

Consumo de energía: 12 W

Frecuencia de trabajo: 1-100 bandas

El más alto estándar: tamaño de metal ≥ 6 g

Dimensión externa: 86.6 × 37.4x22in

Ancho interior: 30in

Voltaje de trabajo: AC110V ~ 240V 50 / 60Hz

Temperatura ambiente de trabajo: -40 °C ~ + 85 °C

CARACTERÍSTICAS AVANZADAS

- Pantalla táctil: pantalla táctil LCD HDMI de 7 pulgadas, fácil de operar y comprender.
- 33 zonas independientes disponibles para elegir, detección más precisa de mercancías peligrosas.
- Sensibilidad ajustable de cada zona de detección, sonidos de alarma múltiple para elegir.
- La frecuencia de funcionamiento se puede ajustar de forma manual o automática
- Tecnología de conexión móvil: control remoto de la aplicación móvil (opcional).
- Tecnología de detección: incluso tecnología de detección, sin punto ciego
Tecnología de Internet: sistema de actualización remota y sistema de control remoto.
- Función de consulta: el sistema tiene una función de consulta de información en tiempo real.
- En espera inteligente: el sistema tiene alertas de operación en espera inteligente.
- Velocidad de detección: más de 60 personas pasan y detectan en 1 minuto.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Partición inteligente: puede cambiar las zonas de detección según las demandas de los clientes.
- Tiene 4 tipos de modo infrarrojo: IR ON / IR OFF / Grupo frontal IR ON / Grupo trasero IR ON.
- Integramos 90 ocasiones de aplicación en el programa, podemos cambiar todas las zonas, sensibilidad cuando eliges diferentes ocasiones.
- No daña el cuerpo humano con el pacificador del corazón, las mujeres embarazadas, el disquete magnético y las cintas de grabación.
- Estadísticas: registra los números de pase y alarma.

CONFORMIDAD

- Cumplimiento CE
- Sistema de Gestión de Calidad ISO9001
- Sistema de Gestión Medioambiental ISO14001
- Sistema de Gestión de Salud Ocupacional OHSAS18001
- Dimensiones y peso de envío: 91x29x12 in - Peso 154 lbs

DETECTOR EXPLOSIVO / DROGAS – ESPECIFICACIONES MINIMAS

CARACTERÍSTICAS

- Tecnología de alta sensibilidad que puede detectar tan poco como 100 nanogramos de polvo negro, incluyendo fuegos artificiales y explosivos caseros.
- Tecnología de ionización suave de la lámpara ultravioleta al vacío (VUV), para un uso no radiactivo seguro.
- Pantalla táctil a color TFT de 10 pulgadas.
- Tiempo de identificación de menos de seis segundos.
- Impresora para imprimir los resultados de la prueba.
- El diseño avanzado del tubo de migración garantiza una alta resolución.
- Sistema de limpieza automática.
- Sistema de purificación de gas renovable.
- Base de datos abierta que los usuarios pueden personalizar para agregar / editar nuevos tipos de explosivos.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Re- varilla de nivel utilizable.
- Admite control y transferencia de red.
- Almacenamiento ilimitado, puerto USB para salida de datos.

PARÁMETROS BÁSICOS.

Explosivos Identificable: Nitrificación de nitroglicerina, polvo negro de nitrato de amonio.

Drogas Identificables: cocaína, heroína del ácido clorhídrico, tetrahydrocarbanabinol, metilanilina (metanfetamina), clorhidrato de ketamina, éxtasis, petidina.

- Tiempo de inicio: menos de 15 minutos.
- Tiempo de análisis: Menos de 6 segundos.
- Tasas de falsas Alarmas: Menos de 1%.
- Tasa de detección: Más de 99%.

OTRAS CARACTERÍSTICAS.

- La base de datos se puede actualizar según sea necesario.
- Método de muestreo: Las muestras se limpian con papel de prueba, muestra de absorción.
- Detección de drogas y explosivos: **SI**.
- Impresión de texto de almacenamiento de datos o imagen.
- Sonido y luz de alarma Pantalla.
- Pantalla táctil a color TFT de 10".

ELÉCTRICO

- Voltaje de funcionamiento 110Vac / 220Vac ($\pm 10\%$) (especificar en el momento del pedido).
- Consumo de energía 300W.

AMBIENTAL

- Temperatura de funcionamiento 14 ° F a 122 ° F [-10 ° C a 50 ° C].
- Temperatura de almacenamiento 14 ° F a 122 ° F [-10 ° C a 50 ° C].
- Humedad de funcionamiento hasta 95% (sin condensación).



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Humedad de almacenamiento hasta 95% (sin condensación).
- Presión de trabajo 60kPa a 106kPa.
- Certificación: CE

DETECTOR DE METALES DE MANO TIPO PALETA.

CARACTERÍSTICAS.

- Resistente a golpes, alta capacidad de detección, incluyendo armas de fuego, cuchillos, alfileres, teléfonos, munición, y otros componentes metálicos.
- Apagado automático.
- Operación en temperaturas y condiciones extremas, mínimo -10 a 65 grados centígrados.
- Luz Indicador de cambio batería.
- Bajo consumo de energía. Mínimo 100 horas de uso.
- Controlador de nivel de sensibilidad.

ESCANER CUERPO –CAVIDADES.

CARACTERÍSTICAS.

- Tiempo de escaneo de los paquetes menor a 7 seg.
- El tipo de plataforma debe ser del tipo de cinta transportadora y el generador debe ser fijo.
- Sistema operativo del scanner Linux.
- Dosímetro integrado para medir la cantidad de rayos X que genera el equipo.
- Cuerpo Completo.
- Capacidad detección cavidades exterior e interior de objetos como explosivos, drogas, armas, teléfonos y objetos no permitidos.
- Botón de Emergencia
- Capacidad de alertar al usuario si se ha excedido el número de escaneos o niveles de radiación.
- Capacidad de pan/zoom, ajuste contraste, exportación de imágenes, ajuste contraste.
- Capacidad de operación en rangos de temperaturas desde 0 a 50 grados centígrados.
- Cumplimiento FDA



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

RAYOS X TÚNEL

CARACTERÍSTICAS MINIMAS

- 600 mm (W) × 500 mm (H) tamaño de túnel.
- Mejora de imagen HD.
- Mejora de penetración de imagen.
- Rechazo de orgánicos.

PARÁMETROS BÁSICOS MINIMOS

- Velocidad del transportador 0.65ft / s [0.2m / s].
- Carga máxima del transportador 441lbs [200kg].
- Velocidad de paso 1500 pieza / hora.
- Penetración a través de placa de acero típica 30mm) / típica 32mm.
- Alambre de metal resolución típica 40AWG / Φ 0.0787mm.
- Dosis por inspección típica 2 μ Gy.
- Fuga de rayos X típica 1 μ Gy / ha 2 "[5cm] desde la máquina Seguridad.
- Medicina, alimentos a la exposición a rayos X no tienen efectos adversos.
- Película ISO1600.
- Sistema operativo Linux / Windows.

GENERADOR DE RAYOS X

- Corriente del tubo (ajustable) 0.4 a 1.2mA.
- Voltaje del tubo (ajustable) 160kV.
- Dirección del haz inferior, ángulo, 80 grados.
- Cantidad del generador uno (generador único).
- Refrigeración / ciclo de trabajo refrigeración por aceite / 100%.

PROCESAMIENTO DE IMÁGENES

- Detector de matriz de fotodiodos con sensor de rayos (doble energía).
- Almacenamiento mínimo de imagen 50,000 imágenes.
- Pantalla de imagen una LCD color de alta resolución.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Resolución máxima de imagen 1920 × 1080 píxeles.
- Procesamiento de imagen 24 bits para procesamiento en tiempo real; mejora de bordes, estiramiento, retorno, recuperación.
- Opciones de imagen alta penetración, baja penetración, lupa, brillo / oscurecimiento;
- Lupa de 1 a 64 veces (observación continua en pantalla completa).
- Pantalla multicolor para energía orgánica naranja para orgánico, azul para inorgánico, verde para mezcla.
- Tecla de visualización de alta energía / baja energía.
- Detección asistida de mercancías peligrosas (armas, drogas, explosivos).

ELÉCTRICO

- Voltaje de funcionamiento 110Vac / 220Vac ($\pm 10\%$) (especifique en el momento del pedido).
- Consumo de energía 500W (máx.) / 300W (nominal).
- UPS 20 minutos en espera.

AMBIENTAL

- Temperatura de funcionamiento 32 ° F a 114 ° F [0 ° C a 45 ° C].
- Temperatura de almacenamiento -4 ° F a 140 ° F [-20 ° C a 60 ° C].
- Humedad de funcionamiento 20% a 95% (sin condensación).
- Humedad de almacenamiento 20% a 95% (sin condensación).

CARACTERÍSTICAS FÍSICAS DEL RAYO X

- Longitud 86.5 "[2195 mm] – incluidas las cintas transportadoras IN / OUT 46.75" [1190 mm] - excluidas las cintas transportadoras IN / OUT.
- Ancho 35.5 "[902 mm].
- Altura 53.75" [1362.5 mm].
- Altura de la cinta transportadora 27.5 "[700 mm].
- Peso 992 lb [450 kg] / 1047 lb [475 kg].



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

GENERAL

- Pantalla de visualización LED verde - dispositivo en LED rojo - Rayos X en uso / calibración LED ámbar.
- Controla el botón y el mouse del botón de emergencia.
- Alarma Ruido del sistema 58 dB.
- Comunicación ethernet.
- Certificación FDA, CE

FIREWALL

Requerimiento Técnico Mínimo (de obligatorio cumplimiento) **Plataforma de Filtrado de Contenido Regulatorio.**

GENERALIDADES.

Llevar a cabo la implementación tecnológica del sistema de seguridad informática del tipo Firewall de Nueva Generación a ser instalado en el centro de datos.

RENDIMIENTO

El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:

- 20 Gbps Firewall Throughput.
- 2,2 Gbps IPS.
- 2 M Concurrent sessions (TCP).
- 7,2 Gbps IPsec VPN throughputs.
- 820 mbps Inspection SSL.
- 1,8 Gbps NGFW.

Los equipos deben contar con un ciclo de vida no menor a 5 años, contando con equipos de última generación dentro de la oferta del fabricante.

CARACTERÍSTICAS GENERALES

- El dispositivo debe ser un equipo de arquitectura integrada de propósito específico



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

para ofrecer un alto rendimiento y baja latencia.

- Solución en alta disponibilidad, dos equipos de la misma referencia funcionando en modo clúster.
- El equipo debe tener un rendimiento alto de firewall para tráfico IPv4 e IPv6.
- El equipo deberá contar con las siguientes interfaces de conexión, totalmente provisionadas:
 - 2x GE RJ45 WAN Ports
 - 14x GE RJ45 Ports/ 4x GE SFP Slots / 1 console Ports USB Ports / 2x GE RJ45 Management/ HA Ports
- El fabricante de la solución debe estar validado a nivel de rendimiento y seguridad por los siguientes laboratorios de pruebas de terceros, líderes en la industria de protección: NSS Labs, VB100, AV Comparatives e ICSA.
- El dispositivo debe tener una base de datos que contenga una lista de direcciones Botnet C&C (command and control) que sean actualizadas dinámicamente y almacenadas en el NGFW.
- El equipo debe estar respaldado por un laboratorio de investigación y desarrollo que ofrezca inteligencia en tiempo real entregando actualizaciones de seguridad completas, investigadores de amenazas de seguridad.
- El dispositivo debe proporcionar información granular para aplicaciones basadas en nube, tales como: YouTube, Dropbox, Baidu, Microsoft Office 365, Amazon, entre otras.
- Los equipos ofertados deben ser suministrados con soporte técnico y retorno de hardware por parte del fabricante por un periodo de 1 año (Oferta 1) y 3 años en un esquema 7 x 24 incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono.
- El Oferente/Proponente debe aportar información sobre la ubicación de su solución propuesta en el Gartner 2018 Magic Quadrant, donde se calificará como deseable, si esta se encuentra en calificación de líder. Es deseable que la solución se encuentre dentro de las principales listas de soluciones, como por Ejemplo NSSLABS, FORESTER, Gartner.
- NAT dinámico: Overloading y overlapping NAT
- NAT estático
- PAT
- NAT64, NAT46, NAT 66



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

FUNCIONES BÁSICAS DE FIREWALL

- La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios. Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.
- La solución soportará políticas basadas en dispositivo. Esto significa que podrán definirse políticas de seguridad de acuerdo al dispositivo (móvil, laptop) que tenga el usuario. Esta característica no requerirá ningún tipo de licenciamiento adicional.
- Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
- Debe ser posible hacer políticas basados en usuarios, grupos de usuarios y dispositivos sobre una misma política, de esta forma se es lo más granular posible en la definición de políticas.
- El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces.
- El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.
- Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis

CONECTIVIDAD Y ENRUTAMIENTO

- Soporte de enrutamiento basado en políticas para envío de tráfico de diferentes tipos basado en protocolo de tráfico entrante, dirección o interfaz fuente, dirección destino o número de puerto.
- Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs. La solución debe soportar el aprovisionamiento de los rangos estándar y extendidos.
- Soporte a ruteo dinámico OSPF, OSPFv3, BGP, IS-IS, Static routing.
- Soporte a ruteo de multicast PIM SM y PIM DM.
- La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6.
- La solución podrá habilitar políticas de ruteo en IPv6 Dual-Stack.
- La solución debe soportar integraciones con tecnología Cisco ACI, VXLAN, en el cual se pueda obtener escenarios de automatización.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

VPN IPSEC

- Soporte para IKEv2 e IKE Configuration Method.
- Soporte a certificados RSA X.509 para construcción de VPNs cliente a sitio (client-to-site).
- Soporte de VPNs IPsec sitio a sitio y cliente – sitio.
- Soporte de VPNs con algoritmos de cifrado: AES256, AES192, AES128, DES, 3DES.
- Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
- Se deben soportar VPNs basadas en rutas y VPNs basadas en políticas.

VPN SSL

- Soporte a SSL 2.0 y 3.0, TLS 1.0,1.1 y 1.2.
- Capacidad de realizar SSL VPNs sin necesidad de licenciamiento por usuarios. De lo contrario, la solución debe ser provista con el licenciamiento para 20000.
- Soporte para modo de operación basado en web o modo túnel.
- Soporte a certificados RSA X.509 para construcción de VPNs SSL.
- Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
- Soporte de autenticación de dos factores con token, la solución debe estar en la capacidad de suplir o integrarse con tokens físicos o basados en software.
- Validación de equipos de plataformas Windows mediante la comprobación de sistema operativo, firewall de Windows, antivirus para obtener acceso mediante VPN SSL.
- Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.
- Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.
- Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning).
- La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS.
- Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL.
- Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.

- Los portales personalizados deberán soportar al menos la definición de:
 - Widgets a mostrar.
 - Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC.
 - Soporte para Escritorio Virtual.
- Política de verificación de la estación de trabajo.

AUTENTICACIÓN

- Capacidad de integrarse con Servidores de Autenticación: RADIUS, LDAP, TACACS+, POP3, SSO y RSA ACE.
- Autenticación basada en contraseña y en doble factor de autenticación (certificado, correo, SMS y tokens).
- Soporte de tokens basados en software para dispositivos IOS o Android y hardware integrados a la solución de NGFW.
- Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”.

MANEJO DE TRÁFICO Y CALIDAD DE SERVICIO

- El equipo debe permitir la configuración de reglas de prioridad de tráfico por dirección fuente, grupo de usuarios, dirección destino, numero de protocolo y aplicaciones basadas en nube.
- El equipo debe soportar traffic shaper basado en fuente (dirección IP, usuarios locales y grupos), destino (dirección IP, FQDN, URL o categoría), servicio (General, acceso web, acceso a archivos, servicios de correo y red, autenticación, acceso remoto, tunneling, VoIP, mensajería y otras aplicaciones, web proxy), aplicación, categoría de aplicaciones, categoría de URLs.
- Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.
- Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall.
- Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

tráfico en distintos sentidos de una misma sesión.

- Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo.
- Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo.

ANTIMALWARE

- Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer antivirus en tiempo real en al menos los siguientes protocolos: HTTP, SMTP, IMAP, POP3, FTP, NNTP, HTTPS, IMAPS, POP3S, SMTPS y FTPS.
- Debe mitigar las siguientes amenazas: Virus, gusanos, troyanos, ransomware, scareware, spyware, adware, botnets, entre otros.
- El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma.
- El Antivirus deberá integrarse de forma nativa con una solución de sandboxing en la nube del fabricante de tal manera que envíen muestras de archivos para su análisis. Incluido en el licenciamiento ofrecido.
- El Antivirus deberá poder configurarse de forma que los archivos que pasan sean totalmente capturados y analizados, permitiendo hacer análisis sobre archivos que tengan varios niveles de compresión (Mínimo 3 niveles).
- El antivirus deberá escanear tráfico de compartición de archivos: CIFS, SMB y SAMBA.
- El antivirus debe permitir las siguientes opciones de inspección: amenazas en ejecutables Windows que se encuentran embebidas en un adjunto de correo electrónico y protección para malware de dispositivos móviles.
- Antivirus en tiempo real, integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
- El antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.
- El antivirus deberá escanear tráfico de compartición de archivos: CIFS, SMB y SAMBA.
- La solución deberá integrarse de forma nativa con una solución de Sandboxing en la nube del fabricante sin la necesidad de licencias adicionales.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- La solución debe incluir mecanismos para detectar y detener conexiones a redes Botnet y servidores C&C.

FILTRADO WEB

- La solución debe permitir filtrado de contenido web, filtrado de URLs y servicio de filtrado web basado en firmas desarrolladas por laboratorio de investigación y desarrollo propio del fabricante.
- Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 70 categorías y por lo menos 47 millones de sitios web en la base de datos.
- Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
- Debe poder categorizar contenido Web requerido mediante IPv6.
- La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación.
- La solución de Filtrado de Contenido debe soportar la característica de “Safe Search” o “Búsqueda Segura” para prevenir imágenes y sitios web con contenido explícito en los resultados de búsqueda. Esto debe ser soportado para los siguientes sitios: Google, Yahoo, Bing y Yandex.
- Será posible exceptuar la inspección de HTTPS por categoría.
- El filtrado de contenido web debe permitir la definición de palabras, frases, patrones, wildcards y expresiones regulares Perl para prevenir acceso a páginas con material cuestionable.
- El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en categoría, grupo de categoría o clasificación.
- La solución debe poder aplicar distintos perfiles de navegación de acuerdo al usuario que se esté autenticando. Estos perfiles deben poder ser aplicados a usuarios o grupos de usuarios.
- El filtrado debe ser sobre tráfico HTTP y HTTPS.

PROTECCIÓN CONTRA INTRUSOS (IPS)

- El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

inspeccionar desde un switch con un puerto configurado en span o mirror.

- Deberá ser posible seleccionar el sistema operativo, protocolo, severidad y objetivo para la configuración de perfiles IPS.
- Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6 a través de sensores.
- Capacidad de detección de más de 4000 ataques.
- El IPS debe tener la posibilidad de tomar las siguientes acciones: permitir, monitorear, bloquear, resetear la sesión, guardar copia de los paquetes que coincidan con las firmas, hacer cuarentena con base en dirección IP del atacante y tiempo basado en días, horas o minutos.
- El sistema de protección de intrusos debe utilizar decodificadores de protocolo para identificar patrones de tráfico anormal que no reúnan los requerimientos de protocolo y estándares.
- Capacidad de actualización automática de firmas IPS mediante tecnología de tipo “Push” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas).
- El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.
- El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad “appliance, sin necesidad de instalar un servidor o appliance externo. La interfaz de administración del sistema de detección y prevención de intrusos deberá estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.
- Actualización automática de firmas para el detector de intrusos.
- El sistema de detección y prevención de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / Rate base).
- Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

configurar firmas nuevas para cualquier protocolo.

- El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.
- Métodos de notificación:
 - Alarmas mostradas en la consola de administración del appliance
 - Alertas vía correo electrónico.
 - Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.
 - La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma “indefinida”, hasta que un administrador tome una acción al respecto.
 - Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

CONTROL DE APLICACIONES

- La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
- La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
- Debe basarse en categorías que permitan seleccionar grupos de firmas basados en un tipo de categoría.
- El listado de aplicaciones debe actualizarse periódicamente.
- La solución debe tener un listado de al menos 2300 aplicaciones ya definidas por el fabricante.
- Preferentemente deben soportar mayor granularidad en las acciones.
- Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, hacer traffic shapping, registrar en log, ver firmas y bloquear acceso a una aplicación por un periodo de tiempo específico basado en días, horas y minutos.
- Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.



Departamento de Compras y Contrataciones

“Año de la Innovación y la Competitividad”

- Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
- Debe ser posible inspeccionar aplicaciones tipo Cloud como YouTube, Dropbox, Baidu, Amazon entre otras entregando información como login de usuarios, transferencia de archivos y videos visualizados.

INSPECCIÓN DE CONTENIDO SSL/SSH

- La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3.
- La inspección deberá realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o sólo inspeccionando el certificado sin necesidad de hacer full inspection.
- Debe ser posible definir si la inspección se realiza desde múltiples clientes conectando a servidores (es decir usuarios que navegan a servicios externos con SSL) o protegiendo un servidor interno de un cliente.
- Debe ser posible definir perfiles de inspección SSL donde sea posible definir los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad.
- El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS.
- Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.
- Debe ser posible inspeccionar tráfico SSH y funcionalidades como Exec, Port-Forward o X11.

VISIBILIDAD

- El equipo debe permitir la visualización de la topología física y lógica, con el fin de obtener mayor información de los dispositivos y conexiones.
- La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional.
- Menú tipo dropdown para navegar por la información.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- El equipo debe entregar las siguientes consolas para reunir los siguientes objetivos:
 - Políticas: Permite monitoreo de actividad de políticas, con el fin de discernir cuales políticas no se usan y pueden ser borradas.
Interfaces: Permite realizar monitoreo actual e histórico de ancho de banda por interfaz.
Países: Filtrado de trafico de acuerdo a países fuente y destino.
 - Traffic shaping: Permite monitoreo de traffic shappers configurados.
 - Mapa de amenazas: Permite monitorear riesgos provenientes de varias ubicaciones internacionales llegando a una ubicación específica.
 - Autenticaciones fallidas: Permite determinar si el NGFW presenta un ataque de fuerza bruta, así como: acceso no autorizado a interfaz por telnet, SSH, HTTP y HTTPS, fallas para hacer una consulta por SNMP, intentos fallidos para establecer conexión de una VPN IPsec Dial-up, conexiones de VPNs IPsec Sitio a Sitio y conexiones de VPNs SSL.
- Mostrar las aplicaciones y su categorización según riesgo.
- Mostrar los orígenes del tráfico o usuarios que lo generan.
- Visibilidad de destinos del tráfico.
- Visibilidad de las amenazas o incidentes que han ocurriendo en la red.
- Visibilidad de los sitios web más consultados por los usuarios.
- Visibilidad de aplicaciones Cloud usadas por el usuario.
- Se deben ver aplicaciones, sitios, amenazas por cada usuario.
- Se debe ver el tiempo de navegación por cada sitio o categoría de sitios.
- En la información de fuentes, aplicaciones, navegación debe ser posible con un doble-clic filtrar la información para ser más específica la búsqueda.
- De las aplicaciones Cloud que permitan compartir archivos como Dropbox debe ser posible ver que archivos fueron subidos y descargados por los usuarios.
- De aplicaciones de contenido como YouTube debe ser posible ver que videos fueron vistos por los usuarios.

CARACTERÍSTICAS DE ADMINISTRACIÓN

- Interfase basada en línea de comando (CLI) para administración de la solución.
- Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura



Departamento de Compras y Contrataciones

“Año de la Innovación y la Competitividad”

nativa de la solución para administrar la solución localmente. Por seguridad la interfase debe soportar SSL sobre HTTP (HTTPS).

- El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales.
- Puerto de consola dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.
- Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH).
- El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales.
- Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.
- El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
- El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, http o HTTPS.
- Soporte de SNMP versión 2.
- Soporte de SNMP versión 3
- Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.
- Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos
- Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.
- Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.
- Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.
- Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard).



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa.
- Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.

VIRTUALIZACIÓN

- El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains”
- Cada instancia virtual debe poder tener un administrador independiente.
- La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS.
- Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red
- La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.
- Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.
- Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.
- Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el tráfico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente.
- Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.
- Se debe poder ver el consumo de CPU y memoria de cada instancia virtual.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

RADIO COMUNICACIÓN **(SISTEMA TRONCALIZADO DIGITAL MULTISITIO AVANZADO)**

CARACTERÍSTICAS GENERALES

- El sistema de radio comunicaciones y los equipos de radio deberán operar en la banda de UHF.
 - Para optimizar el uso de los recursos al aire, el sistema de radio comunicaciones y los equipos de radio deberán soportar transmisiones digitales en modo de acceso múltiple por división de tiempo (TDMA), con 2 ranuras de comunicación en cada canal Radioeléctrico.
 - La arquitectura del sistema ofertado deberá incorporar las siguientes características:
 - Sistema troncalizado de área extendida Multi-Sitio, es decir; contar con la capacidad de múltiples sitios de transmisión ubicados en locaciones geográficamente distintas e interconectadas entre sí. Las comunicaciones de radio generadas en un sitio podrán ser escuchadas y/o respondidas en 1 ó más sitios distintos, según corresponda.
 - El sistema debe admitir al menos 15 sitios de RF sin la necesidad de colocar Hardware adicional.
 - Cada sitio de repetición deberá tener la capacidad de soportar 15 repetidores de RF en distintas frecuencias de operación, según la cantidad de tráfico que se requiera manejar, hasta 6 repetidoras de exclusivas para GPS Mejorado.
 - La arquitectura debe permitir definir canales para uso exclusivo de datos (no llamadas de voz) en cada sitio de repetición, hasta 6 repetidoras exclusivas para GPS Mejorado.
- Todas las informaciones, tales como: voz, datos, señalización, etc.; deberán transportarse mediante el protocolo IP. No se aceptarán medios analógicos o digitales por conmutación de circuitos (E1-T1).
- El diseño del sistema debe permitir la conexión de cualquier sitio en la red a través de vínculos IP para lograr la conectividad requerida entre ellos. La infraestructura de red debe permitirle al operador del sistema la flexibilidad de poder configurar la red en un modo lineal, malla o estrella.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- El sistema de radio comunicaciones deberá contar con una administración central, la cual permita administrar, configurar y monitorear la red; a través de los vínculos que conforman la red de interconexión de la plataforma.
- El sistema de radio comunicaciones y los equipos de radio deben tener incorporada tecnología digital de corrección de errores, para así incrementar la claridad del audio en todo el rango.
- El montaje de los equipos repetidores debe ser modular en bastidores estándar de 19". Deben considerarse normas de instalación reconocidas a nivel mundial para asegurar la calidad de la plataforma, la seguridad de las personas que los manipulan y el máximo rendimiento y duración de los propios equipos.

CARACTERÍSTICAS DE LA RED DE RADIOCOMUNICACIONES

- **Capacidades y Funcionalidades requeridas a nivel de sistema**
 - Control de acceso de suscriptor.
 - Asignación de sitio crítico.
 - Redundancia del canal de control.
 - Interrupción de transmisión.
 - Administración de registro masivo.
 - Administración inalámbrica de baterías.
 - Agregar sitios y canales adicionales sin reprogramar las radios.
 - Entrada tardía.
 - Modo Trunking a nivel de Rpt (Pérdida de red local).
 - Encripción de tráfico de voz y datos.
 - DMO.
 - Protección password a nivel de aplicación.
 - El sistema debe tener capacidad para soportar hasta 2000 usuarios de radio registrados.
 - Los equipos deberán soportar variaciones y retardos producidos por los vínculos IP.
 - El tiempo promedio de configuración de la llamada para una llamada de grupo donde todas las radios participantes están en un solo sitio DEBE ser inferior a 500 ms., donde el tiempo de establecimiento de la llamada se define como el tiempo



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

entre el PTT de inicio y la primera ranura de audio a transmitir por la radio de inicio.

- El tiempo promedio de configuración de la llamada para una llamada grupal en la que las radios participantes están distribuidas en múltiples sitios DEBE ser inferior a 600 ms.
- El sistema debe ofrecer la capacidad de programación de radios por aire sin que esto afecte la comunicación de voz, al entrar una llamada. La adición de nuevos sitios, frecuencias, licencias, etc. debe poder llevarse a cabo sin necesidad de traer los radios físicamente a un sitio específico a ser reprogramados.
- El retardo promedio del sistema para una llamada de grupo DEBE ser inferior a 1000 ms. donde la demora del sistema de extremo a extremo se define como el tiempo entre el momento de la emisión de la voz por la radio transmisora y el momento en que se recibe la voz a través del altavoz de la radio receptora.
- El sistema debe ofrecer la capacidad de actualizar el firmware de los suscriptores por WIFI.
- El sistema debe ser compatible con plataforma pulsar para hablar (PTT) destinada a mejorar y optimizar las comunicaciones del grupo de trabajo. Con el fin de conectar diferentes redes tales como radios, celulares, Wi-Fi y telefonía; entre otras, para posibilitar la comunicación entre ellas. Ya sea con un smartphone, radio, teléfono fijo o cualquier otro dispositivo de comunicación.
- El sistema deberá soportar la capacidad de asignar tráfico de voz o datos a canales disponibles en el sistema para maximizar la eficiencia. El sistema troncalizado deberá detectar automáticamente una solicitud de PTT (Push to talk) y automáticamente seleccionar y asignar un canal de comunicación de voz para el grupo de conversación (talkgroup) seleccionado. Diversas entidades y grupos de comunicación deben poder comunicarse sin importar la selección del canal, del sitio o la ubicación geográfica.
- El diseño del sistema deberá contemplar el desplazamiento de los equipos de radio (roaming) entre sitios de repetición. El sistema dispondrá de conmutación automática entre los sitios que componen la red, sin acción alguna por parte del usuario para ofrecer movilidad sin interrupción, dentro del área de cobertura.
- El sistema deberá ser capaz de soportar comunicaciones de datos que incluyen servicios de localización por GPS, localización in-door, mensajería de texto y una interfaz de datos para otro tipo de aplicaciones específicas incluyendo telemetría, gestión de desempeño del sistema, VoIP, despacho, AVL, gestión de órdenes de



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

trabajo y conectividad de email. Asimismo, deberá contar con arquitectura que permita definir canales exclusivos para este tipo de transmisiones.

- En caso de falla en el vínculo IP, el sistema seguirá manteniendo su funcionamiento troncalizado local (comunicando a los usuarios dentro de la misma cobertura del sitio de repetición que se aísla) y continuará proporcionando comunicaciones de área extendida donde haya un vínculo IP de área extendida disponible entre los sitios de repetición.
- Las funcionalidades mínimas requeridas a nivel de sistema se enumeran a continuación:
 1. Llamada de grupo: Uno a muchos.
 2. Llamada Privada: Uno a uno.
 3. Llamada de Sitio: Uno a todos los usuarios del sitio.
 4. Llamada a todos: Uno a todos los usuarios del sistema.
 5. Llamadas Telefónicas.
 6. Mensajería corta.
 7. Gestión de Llamadas y Alertas de emergencia.
 8. Transmisión de datos IP y/o telemetría.
 9. Interrupción de llamadas configurable.
 10. Habilitación/Deshabilitación remota de un equipo de radio.
 11. Matar/Revivir remota de un equipo de radio perdido.
 12. Monitoreo y chequeo remoto de un equipo de radio.
- **Capacidades y Funcionalidades requeridas a nivel de Equipos de radio**
- Todos los equipos de radio deben incluir la capacidad de generar llamadas de emergencia con la activación de un único botón dedicado para este propósito. El modo de emergencia deberá proveer notificación de estado visual y audible para los radios especificados. La propuesta deberá incluir una descripción detallada de las características del modo de emergencia y las opciones de programación.
- Los radios portátiles deben poseer la capacidad de conexión WiFi a redes comerciales para inter-operar con los grupos de conversación de radio cuando no exista cobertura de RF en UHF.
- Los radios portátiles deben poseer la capacidad de operar con redes WiFi 802.11b/g/n.
- Todos los equipos deberán tener Memoria 256MB Flash y 128MB RAM.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Todos los equipos deberán contar con Bluetooth 4.0 (audio, data), para interconexión de tabletas u otros dispositivos que permitan el desarrollo de software para envío y recepción de datos cortos.
- El usuario del sistema tendrá la opción de solicitar la licencia para obtener información detallada de la interfaz de radio. Esta información permitirá al usuario de radio, de ser posible, desarrollar aplicaciones personalizadas.
- Los equipos de radio podrán ser programados mediante una aplicación dedicada para este efecto, permitiendo proteger la configuración mediante una contraseña. Los usuarios de radio no tendrán acceso a parámetros vitales para la operación de los equipos de radio, desde el propio equipo; evitando así fallas por manipulación accidental o premeditada.
- Todos los equipos de radio deben tener la opción de operar en modo de comunicación directo (radio a radio), además de a través del repetidor, cambiando de un modo a otro mediante menús.
- Todos los equipos de radio deben tener la opción de operar en modo analógico, además del modo digital, cambiando de un modo a otro mediante menús o perillas, y deberán contar con capacidad de señalización.
- Todos los equipos deberán tener la capacidad de:
 - A. Poseer encriptación 40 bits
 - B. Localización en interiores
 - C. Interrupción de transmisiónSin agregar hardware adicional
- Los suscriptores de radio deberán contar con la posibilidad de asumir distintas funciones de seguridad con la sola incorporación de Firmware en la radio:
 1. Alerta de Hombre caído: El dispositivo debe contar con un acelerómetro que permita enviar alertas al centro de Monitoreo o a los grupos de alarma en el sistema de radio, cuando el mismo cambie de inclinación de acuerdo a un parámetro definido por el usuario.
 2. Alerta de No Movimiento: El dispositivo debe ser capaz de enviar una alerta al sistema de radio o al sistema de monitoreo al transcurrir una cantidad de tiempo fijada por el usuario sin experimentar movimiento o vibraciones por encima de un umbral predefinido.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

3. Alerta de detección de choques/colisiones: EL dispositivo debe contar con la capacidad de reconocer secuencias de aceleración/desaceleración y tiempo en detenido de forma de enviar alertas cuando el mismo se coloca en una unidad y la misma experimenta una colisión o choque tanto en automóviles como vehículos motorizados.
 4. Geocercas: El dispositivo de radio debe contar con la posibilidad de alertar cuando la misma ha entrado o salido de una zona geográfica definida por el usuario. La alerta podrá ser enviada al sistema de radio o al centro de monitoreo.
 5. Almacenamiento de datos de posición: El dispositivo de radio debe contar con la capacidad de almacenar datos de ubicación en su memoria, por tiempo transcurrido, distancia recorrida o cambios en la dirección. Los datos de ubicación almacenados deben poder ser enviados en conglomerados de paquetes comprimidos cuando el centro de Monitoreo lo solicite o cada cierto intervalo recorrido realizado por el usuario.
 6. Administración de alarmas: El dispositivo de radio deberá contar con la posibilidad de incorporar la administración de alarmas embebida, activándose esta misma a requerimiento con sólo una actualización de firmware. La administración de alarmas deberá permitir al dispositivo de radio ejecutar acciones ante eventos detectados por el mismo.
- Los eventos que deben ser detectados por el radio son los siguientes:
 - Exceso de velocidad.
 - Cruce de región.
 - Alerta de Hombre caído (en portátiles).
 - Detección de Colisiones.
 - Alerta de No Movimiento.
 - Alerta de Trabajador solitario.
 - Cambios en los pines de telemetría.
 - Ante estos eventos la radio debe tener la posibilidad de ejecutar acciones de forma autónoma ante los eventos previamente mencionados sin depender de un centro de monitoreo:



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Enviar una alarma al sistema de radio

Enviar mensajes de texto.

Enviar una alarma al centro de monitoreo (en caso de que exista uno habilitado).

Reproducir un tono en la radio.

Mostrar un texto definido por el usuario en la pantalla.

○ **Equipos de Radio Portátil**

Los radios portátiles deben soportar las siguientes características y funciones:

1. Todos los radios portátiles deben incluir tecnología de baterías / cargadores inteligentes para el mantenimiento automático y reacondicionamiento.
2. Soportar el uso de accesorios para control automático de ganancia y supresión de ruido.
3. Incluir receptores GPS integrados. No se permitirán receptores externos adicionales o accesorios para recibir o enviar información de GPS. Funcionalidad GPS debe ser soportada tanto en modo directo, como a través del repetidor.
4. Los radios portátiles que tengan display y teclado completo, deben incluir capacidades de mensajería de texto integradas. No se requerirán equipos externos adicionales o accesorios para recibir o enviar información de mensajes de texto. Los suscriptores con teclado completo deben tener la capacidad de crear mensajes de texto de usuario a usuario. El equipo debe soportar al menos 280 caracteres. La mensajería de texto debe ser soportada en modo directo o a través del repetidor.
5. Tener un botón de emergencia con un color distintivo, respecto del resto de los botones/teclas.
6. Los radios portátiles, que se indiquen, deben tener una pantalla alfanumérica y soportar al menos 1000 canales.
7. Proveer ajuste automático de audio, en dependencia directa del nivel de ruido en el entorno en el que se encuentre.
8. Tener capacidad de ganancia automática donde este aumenta o disminuye la ganancia del micrófono.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

9. Proveer audio fuerte y claro, usando un protocolo de minimización de distorsión aun a altos niveles.
10. Proveer funcionalidad de bluetooth para audio y para datos, y el proveedor debe brindar un portafolio variado de auriculares alámbricos e inalámbricos para uso en dicha modalidad.
11. Los radios deben también tener la modalidad de “modem”, donde son usados para el envío y recepción de datos.
12. Tener la capacidad de anunciar a través de un mensaje audible, programable: la modalidad, canal, zona, o grupo, etc. en el que se encuentra, así evitándole al usuario el tener que mirar físicamente la pantalla al este hacer un cambio en cualquiera de sus botones. Estos archivos de audio deben ser predeterminados y personalizables.
13. Ofrecer la capacidad de transmitir y recibir telemetría. Estos deben soportar lecturas de cambios de voltajes, etc.
14. El Oferente/Proponente debe ofrecer modelos de radios que incluyan modalidad encubierta; es decir, el radio cuando es usado en esta modalidad, debe deshabilitar todos los indicadores, pantalla, luces, tonos o cualquier audio. Este debe tener la opción de escuchar las transmisiones de audio usando Bluetooth inalámbrico o accesorios de vigilancia.
15. Todos los radios portátiles deben poseer botones programables para facilitar el acceso a diferentes funciones como contactos, grupos, capacidades, etc., de manera rápida y eficiente.
16. El Oferente/Proponente debe proveer para los modelos de radios con pantalla, que estas sean a color, de no menos de cinco líneas de texto, fácil de leer y con modalidad de inversión de colores / contraste para uso en la noche.
17. Interpretar señalización digital – PTT ID, llamada privada, llamada a todos, alerta de llamada, emergencia, chequeo de radio, desactivar / activar radio y monitoreo remoto.
18. El proveedor debe incluir en su portafolio, portátiles que soporten señalización analógica - MDC1200: PTT ID, Emergencia y llamada de Alerta.
19. Los radios portátiles deben tener un selector de canales de cómo mínimo 16 posiciones. Estos deben ofrecer diferentes configuraciones de programación.
20. Soportar la funcionalidad de escaneo de grupo.
21. Tener una opción intrínsecamente segura.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

22. Cumplir con el grado de sumersión IP68.
23. Poseer privacidad con claves de 40 bits de longitud en las comunicaciones.
24. La capacidad de las baterías debe permitir una duración de más de 27 horas de trabajo continuo a ciclos de 5 / 5 / 90 (% de Tx/Rx/Stdby) en modo digital.
25. Los radios portátiles deben cumplir con los estándares militares 810C, 810D, 810E 810F and 810G.
26. Cumplir con los estándares TIA/EIA-603, Sección 5.

Los suscriptores portátiles deben cumplir o exceder las siguientes especificaciones:

<u>Transmisor</u>	
Rango de frecuencia	403 – 527 MHz
Estabilidad de Frecuencia	+/- 0.5ppm
Potencia máxima de Salida RF	4 watts
Espaciamiento de Canal	12.5 KHz (Digital) / 25 KHz (Análogo)
Rechazo de Canal Adyacente	60 dB @ 12.5 kHz
Zumbido y ruido	-40 dB (canal de 12.5 kHz),
Emisión espúrea conducida (TIA603D)	-57 dBm
Modulación digital 4FSK	12.5 kHz; Datos: 7K60F1D y 7K60FXD 12.5 kHz; Voz: 7K60F1E y 7K60FXE Combinación de voz y datos (12.5 kHz): 7K60F1W
Protocolo digital	ETSI TS 102 361-1, -2, -3
Emisión conducida/radiada (TIA603D)	-36 dBm < 1GHz, -30 dBm > 1GHz
<u>Receptor</u>	



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Rango de Frecuencia	403 -527 MHz
Espaciamiento de Canal	12.5 KHz (Digital) / 25 KHz (Analógico)
Sensibilidad Digital	0.25 uV (0,19 uV típica)
Selectividad de Canal Adyacente	60dB a 12.5 kHz @ (TIA603A) 45dB a 12.5 kHz @ (TIA603D)
Rechazo a Espurias	70 dB
Distorsión de Audio	3% (típico)
Intermodulación (TIA603D)	70 dB
Emisión espúrea conducida (TIA603D)	-57 dBm

○ **Equipos de Radio Móvil**

Los radios móviles deben soportar las siguientes características y funciones:

1. Los radios móviles deben soportar el uso de accesorios para control automático de ganancia y supresión de ruido.
2. Incluir receptores GPS integrados. No se permitirán receptores externos adicionales o accesorios para recibir o enviar información de GPS.
3. Incluir capacidades de mensajería de texto integradas. No se permitirán receptores externos adicionales para la recepción de mensajes de texto. Los suscriptores deben tener la capacidad de crear mensajes de texto de usuario a usuario, solo con el micrófono con teclado, si es requerido. El equipo debe soportar al menos 280 caracteres. La mensajería de texto debe ser soportada en modo repetidor y/o directo.
4. Los radios móviles, que así se definan, deben tener una pantalla alfanumérica.
5. Soportar 1000 canales.
6. Interpretar señalización digital – PTT ID, llamada privada, llamada a todos, alerta de llamada, emergencia, chequeo de radio, desactivar / activar radio y monitoreo remoto.
7. Soportar la funcionalidad de escaneo de grupo.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

8. Tener 4 botones programables (que soporten tanto pulsación corta como larga).
9. Proveer ajuste automático de audio, en dependencia directa del nivel de ruido en el entorno en el que se encuentre.
10. De igual manera el radio debe proveer audio fuerte y claro, usando un protocolo de minimización de distorsión aun a altos niveles.
11. Proveer funcionalidad de bluetooth para audio y datos.
12. Las radios móviles deberán tener la posibilidad de tener un accesorio de audio bluetooth que incluya linterna con alcance superior a 90 metros, que posibilite al usuario descender del vehículo y poder operarlo a esa distancia,
13. Tener la modalidad de “modem”, donde son usados para el envío y recepción de datos.
14. El proveedor debe incluir en su portafolio, móviles que soporten señalización analógica - MDC1200: PTT ID, Emergencia y llamada de Alerta.
15. El radio debe tener la capacidad de anunciar a través de una voz audible, programable, la modalidad, canal, zona, o grupo, etc. en el que se encuentra, así evitándole al usuario el tener que mirar físicamente la pantalla al este hacer un cambio en cualquiera de sus botones. Estos archivos de audio deben ser predeterminados y personalizables.
16. Tener capacidad de ganancia automática donde este aumenta o disminuye la ganancia del micrófono.
17. Ofrecer la capacidad de transmitir y recibir diferentes tipos de datos de telemetría. Estos deben soportar lecturas de cambios de voltajes, etc.
18. Todos los radios móviles deben poseer botones programables para facilitar el acceso a diferentes funciones como contactos, grupos, capacidades, etc., de manera rápida y eficiente.
19. El Oferente/Proponente debe proveer modelos de radios con pantallas a color, de no menos de cinco líneas de texto, fácil de leer y con modalidad de inversión de colores / contraste para uso en la noche.
20. Los radios móviles deben cumplir con los estándares militares 810C, 810D, 810E and 810F.

Los radios móviles deben cumplir o exceder las siguientes especificaciones.



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

<u>Transmisor</u>	
Rango de Frecuencia	403 - 470 MHz
Estabilidad de Frecuencia	+/- 0.5ppm
Potencia de Salida de RF	1 – 40 watts
Espaciamiento de Canal	12.5 KHz (Digital) / 25 KHz (Analógico)
Rechazo de Canal Adyacente	60 dB @ 12.5 kHz
Zumbido y ruido	-40 dB (canal de 12.5 kHz)
Emisión espúrea conducida (TIA603D)	-57 dBm
Modulación digital 4FSK	12.5 kHz; Datos: 7K60F1D y 7K60FXD 12.5 kHz; Voz: 7K60F1E y 7K60FXE Combinación de 12.5 kHz Voz y datos: 7K60F1W
Protocolo digital	ETSI TS 102 361-1, -2, -3
Emisiones conducidas/radiadas (TIA603D)	-36 dBm < 1GHz, -30 dBm > 1GHz
<u>Receptor</u>	
Rango de Frecuencia	403 - 470 MHz
Espaciamiento de Canal	12.5 KHz (Digital) / 25 KHz (Analógico)
Sensibilidad Digital	5% BER: 0.25 uV (0,19 uV típico)
Selectividad Canal Adyacente	50dB at 12.5 kHz (TIA603D)
Rechazo a espurias	75 dB
Distorsión de Audio	3% (típico)



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Intermodulación (TIA603D)	75 dB
Emisión espúrea conducida (TIA603D)	-57 dBm

- Capacidades y Funcionalidades requeridas para cada sitio de repetición
 - Cada sitio de repetición deberá soportar más de 1000 usuarios de radio registrados al mismo tiempo.
 - Cada sitio de repetición debe soportar hasta 15 repetidores para una capacidad máxima de 29 canales de tráfico voz/datos (TCH).
 - Cada sitio de repetición debe soportar hasta 6 repetidores para una capacidad máxima de 12 canales exclusivos de datos.
 - Cada sitio de repetición deberá estar montada en bastidores estándar de 19” e incluir el sistema de distribución de radiofrecuencia (RDFS: Combinadores, Multiacopladores, coaxiales, etc.) adecuado a cada una de las configuraciones solicitadas.
 - En caso de falla de un transceptor, el sistema deberá continuar su operación en modo troncalizado, independientemente de cuál falla.
 - El sistema propuesto debe contener todos los componentes de red necesarios (por ejemplo, switches y routers) para permitir la comunicación entre los repetidores, los otros sitios de repetición y el sistema de Administración.
 - Se debe proporcionar Diagnósticos remotos de los transceptores, incluyendo: estado de la estación (habilitada-deshabilitada), potencia transmitida y canales disponibles.
 - Se debe proporcionar Control remoto de los transceptores, incluyendo: cambio de canales, cambio de potencia a la que transmite la estación, re-inicialización (reset) de la estación y desactivación (“knockdown”). Los reportes de Alarma deben incluir monitoreo del estado, incluyendo:
 - RX (Falla de Lock del repetidor).
 - TX (Detector de Lock de Transmisor).
 - Temperatura (sobrecalentamiento de la estación).
 - Energía (AC falla de fuente de energía).
 - Ventilador (falla de ventilador).
 - Voltaje del PA.



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

ROE.
Potencia de TX.

Los equipos repetidores de RF deberán cumplir con las siguientes especificaciones:

<u>General</u>	
Voltaje de Entrada	AC: 100-240 VAC / DC: 12/24 VDC
Rango de temperatura	-30°C to +60°C
Conectores de Antena	Tipo N
Capacidad de Canal	64
Estabilidad de Frecuencia	0.5 ppm
Pasos de canal	5 Hz
Ciclo de Operación	100 %
<u>Transmisor</u>	
Rango de Frecuencia	400 – 470 MHz
Potencia de salida de RF	100 watts
Espaciamiento de canal digital	12.5 kHz (6.25e)
Zumbido y ruido FM	-45dB @12.5KHz
Potencia de Canal Adyacente	60 dB
Ciclo de trabajo	100%@100 W
<u>Receptor</u>	
Rango de Frecuencia	403 – 470 MHz
Sensibilidad Digital (5% BER)	0.30 uV (0.22 V típico)
Rechazo de espurias	73dB



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Intermodulación	78 dB
Distorsión de audio	Menor que 1.5 %

SOFTWARE DE MONITOREO DE UNIDADES Y DESPACHO

El sistema de administración y despacho de la red de radios tendrá como finalidad permitir el monitoreo de la ubicación de las unidades, así como la comunicación entre el centro de despacho y grupos del sistema de radiocomunicaciones, o cuando el caso lo amerite, con unidades individuales.

- La solución a proveer para el despacho y monitoreo del sistema de comunicaciones provisto debe soportar las siguientes características y funciones:
 - Recepción y transmisión de llamadas de voz en diferentes redes de radio.
 - Grabación de todas las conversaciones de radio en formato WAV y formato propietario.
 - Arquitectura de la aplicación tipo Cliente- Servidor o Cliente- Agente- Servidor basada sobre IP.
 - Encipción de datos entre el Servidor y los despachadores
 - Unificación de diferentes redes de radio en un mismo grupo de conversación, para transmisión y recepción desde las unidades de radio y desde el software de despacho.
 - Recepción y procesamiento de llamadas de emergencia desde los abonados de Recepción y transmisión de mensajes de texto.
 - Transferencia de mensajes de texto vía e-mail.
 - Transmisión y recepción de llamadas de los abonados de radio con redes telefónicas, se debe tener conexión desde el servidor de aplicaciones a una planta PBX que maneje SIP 2.0. ó a través de conexión a Troncal SIP.
 - Localización (Seguimiento en tiempo real de las unidades de radio, historial de las rutas recorridas, cercas geográficas con activación de eventos de aplicación al entrar o salir de una zona definida, control de velocidad y tiempo en espera de una unidad).
 - Creación de los siguientes tipos de Geocercas: Poligonales de N lados para una región, asociadas a una ruta o trayecto específico y Geocercas móviles asociadas al desplazamiento de un radio.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Selección desde el despachador de los siguientes mapas para visualización de las unidades de radio: MAPNIK, CYCLE, TRANSPORT, LANDSCAPE, MAPQUEST, BING_ROAD, BING_AREA, BING_HYBRID, GOOGLE EARTH y cartografía propietaria adquirible posteriormente.
- Recepción, transmisión y procesamiento de señales de telemetría de abonados de radio.
- Registro de acontecimientos, estadística e informes.
- Creación de informes del sistema en formatos PDF, HTML, MHT, RFT, Excel, CSV, Text, BMP, EMF, WMF, GIF, JPEG, PNG, TIFF.
- Habilitación de Correo Electrónico, previa configuración de un servidor POP3 o SMTP.
- Servicio de SMS a Celulares, previa configuración de un Gateway SMS.
- Capacidad de redundancia Activo - Activo o Activo - Pasivo.
- Funciones de automatización de procesos: actividad de radios, trabajador solitario, geocercas, bloqueo y habilitación de radio, monitor de micrófono remoto, control de velocidad y envío de mensajes de texto programados.
- Compatibilidad con módulo adicional de administración de rutas, que permita validar si un abonado de radio pasó sobre un punto específico en una hora predefinida.
- Compatibilidad con módulo adicional de administración de alarmas, que permita generar una acción como envío de: Alarmas pop up al despachador, Email, SMS, Mensaje de texto a un radio o grupo, llamada de grupo o privada, llamada telefónica, mensaje de telemetría u orden de trabajo, A partir de las siguientes fuentes: estado de radio Encendido/ Apagado, llamada de radio, mensaje de texto, mensaje de telemetría, DTMF, alarma de emergencia o alarma de Geocerca.
- Compatibilidad como módulo adicional para creación y seguimiento de tickets con órdenes de trabajo.
- Compatibilidad con módulo adicional para transmisión y recepción de voz, monitoreo GPS, órdenes de Trabajo y mensajería de texto desde dispositivos Android 4.1 o mayor.
- Compatibilidad con módulo adicional para posicionamiento en Interiores, esta funcionalidad debe apoyarse en la instalación de hardware externo tipo baliza para tener continuo monitoreo de la ubicación de los equipos tanto en exteriores como en interiores aptos para tal fin.
- Compatibilidad con módulo adicional para habilitar en los radios vía software la función de Localización mejorada.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Compatibilidad con módulo adicional IP que incorpore al sistema a nivel de audios interconexión con diferentes sistemas, tales como: P25, TETRA ANALOGO u otras redes de comunicación de radios.

SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA PARA GABINETE DE DISTRIBUCIÓN 1.5 kVA escalable, 120V

GENERAL

La UPS mantendrá automáticamente la alimentación de AC a la carga crítica dentro de las tolerancias especificadas y sin interrupción durante falla o deterioro de la fuente de alimentación normal.

El fabricante deberá diseñar y suministrar todos los materiales y equipos para que sean totalmente compatibles con las condiciones eléctricas, ambientales y espaciales en el sitio. La UPS incluirá todo el equipo para conectar correctamente la fuente de alimentación de AC a la carga prevista y se diseñará para funcionamiento desatendido.

ESTÁNDARES

La UPS deberá estar construida en concordancia con los siguientes estándares aplicables:

- La UPS deberá estar listada por el estándar UL Standard 1778, cuarta edición.
- Cumplir con las Reglas y Reglamentos de la FCC, Clase A. Este cumplimiento es legalmente requerido para prevenir interferencia con equipos adyacentes.
- Será compatible con las prácticas de cableado, los materiales y la codificación de acuerdo con los requisitos del Código Eléctrico Nacional y los códigos y normas locales aplicables. Se deben hacer provisiones en los gabinetes para permitir la instalación de cableado de entrada, salida y control externo usando canalización o conducto para acceso superior e inferior a entradas, salidas, bypass y conexiones.



Departamento de Compras y Contrataciones “Año de la Innovación y la Competitividad”

DESCRIPCIÓN DEL SISTEMA

DISEÑO DE REQUERIMIENTOS

- La UPS debe dimensionarse para proporcionar un mínimo de 1.5 kVA a la salida.
- El voltaje de la carga y el voltaje de la línea de derivación serán de 120VAC.
- La planta de baterías será un sistema de batería de celdas sellado, localizado en gabinete. Las baterías deben soportar el UPS a 100% de carga final (2.7 KW) durante al menos 15 minutos. Deberán ser baterías de válvula-regulada (VRLA) de calcio plomo, sellado y de mantenimiento reducido.
- La UPS deberá tener un convertidor / rectificador con corrección activa de factor de potencia, capaz de mantener el factor de potencia de entrada y la distorsión armónica total de corriente de entrada (THDi) dentro de las especificaciones sin un filtro de entrada adicional.
- La UPS debe ser un diseño libre de transformador (no debe requerir ningún transformador interno en la vía de alimentación principal para el funcionamiento básico del módulo). Los transformadores opcionales en gabinetes o de otro modo externo al módulo básico del UPS deberán permitir el aislamiento.

MODOS DE OPERACIÓN

La UPS funcionará como un sistema **en línea** en los siguientes modos:

Normal: La carga crítica de AC debe alimentarse continuamente con el inversor del UPS. El rectificador / cargador derivará energía de la fuente de AC de la red eléctrica y suministrará corriente continua al convertidor DC-DC, que a su vez suministrará al inversor mientras flota simultáneamente cargando la batería.

Baterías: En caso de fallo de la fuente alterna de la red eléctrica, la carga crítica será alimentada por el inversor, el cual, sin ninguna conmutación, obtendrá su energía de la batería a través del convertidor DC-DC. No se producirá interrupción en la alimentación de la carga crítica al fallar o restaurar la fuente AC de la red eléctrica.

Recarga: Al restaurar la fuente de alimentación de la red eléctrica, el rectificador suministrará energía al inversor de salida y al convertidor DC-DC, que al mismo tiempo



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

recargará las baterías. Ésta será una función automática y no causará interrupción de la carga crítica.

Bypass: Si se desconecta la UPS, el interruptor de transferencia estática transferirá la carga a la fuente de derivación. El proceso de transferencia no causará interrupción en la alimentación de la carga crítica. Se utilizará un bypass de mantenimiento externo para asegurar el aislamiento completo de la unidad para el servicio de los componentes internos al mismo tiempo que proporciona seguridad contra el arco voltaico.

REQUISITOS DE RENDIMIENTO

Los componentes de potencia de estado sólido, dispositivos magnéticos, dispositivos electrónicos y dispositivos de protección contra sobre-corriente deben operar dentro de la temperatura recomendada por el fabricante cuando la UPS está funcionando a una carga crítica del 100% y mantener la carga de la batería bajo temperaturas de operación en el rango de 32°F to 104°F (0°C to 40°C).

ENTRADA

Voltaje: Las especificaciones de voltaje de entrada/salida del UPS
Rectificador Entrada de AC: 120V. Monofásico, dos hilos más de tierra
Bypass Entrada de AC: 120V. Monofásico, dos hilos más de tierra
Salida AC: 120v, monofásico, de dos hilos más tierra.

Rango de voltaje: debe soportar los siguientes voltajes ante de entrar a baterías de acuerdo con la carga.

Load Level	1500-3000 VA 120 VAC Input Voltage
100%	102 VAC
90%	96 VAC
80%	90 VAC
70%	84 VAC
60%	78 VAC
50%	72 VAC
40%	66 VAC



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

30%	60 VAC
-----	--------

Rango frecuencia: 40 - 70Hz

Factor de potencia: mínimo 0.99 a carga completa con tensión de entrada nominal

Sobrecarga: 200% por 2 segundos; 150% por 50 segundos con transferencia a bypass.

Salida AC

Capacidad de carga: 100% de la capacidad de carga a 104 ° F (40 ° C) para cualquier carga desde 0,5 a la unidad.

Regulación voltaje: $\pm 3\%$ RMS cargas balanceadas.

Rango de ajuste de voltaje: 110V, 115V, 120V, 127V.

Forma de onda: Sinusoidal.

Eficiencia del sistema: Definida como kW salida / kW de entrada al factor de potencia de carga deberá ser mayor al 88%.

Tierra

El chasis del UPS tendrá terminal de tierra del equipo.

Condiciones ambientales

La UPS será capaz de soportar las siguientes condiciones ambientales sin dañar o degradar las características operativas:

Temperatura ambiente de funcionamiento

UPS: 32°F a 104°F (0°C a 40°C).

Baterías: 77°F (25°C), $\pm 5^\circ\text{F}$ ($\pm 3^\circ\text{C}$).

Humedad relativa

0 a 95%, sin condensación.

Nivel de ruido audible



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

< 46 dBA, a 1 metro.

GARANTÍA Y MANTENIMIENTOS

UPS

El fabricante de la UPS garantizará la unidad contra defectos de mano de obra y materiales durante 24 meses después de la puesta en marcha inicial.

Fabricación

Materiales

Todos los materiales del UPS serán nuevos, de fabricación actual, de alto grado y no deberán haber estado en servicio previo excepto como se requiera durante las pruebas de fábrica. Todos los dispositivos electrónicos activos deberán ser de estado sólido. Todos los semiconductores de potencia deben estar sellados. La lógica de control y los fusibles deben estar físicamente aislados de los componentes del tren de potencia para garantizar la seguridad del operador y la protección contra el calor.

Construcción y montaje

La UPS deberá estar en gabinetes con encerramiento NEMA Tipo 1, diseñados para montaje en el suelo.

Enfriamiento

Se deben proveer sensores de temperatura para monitorear la temperatura interna del UPS. Al detectar temperaturas superiores a las recomendaciones del fabricante, los sensores deben hacer sonar las alarmas audibles y se visualizarán las alarmas visuales en el panel de control del UPS. Los filtros de aire deben estar situados en el punto de entrada de aire y ser cambiables. En la parte trasera del sistema no se requerirá limpieza o ventilación.

EQUIPAMIENTO

Sistema UPS

El sistema UPS deberá estar compuesto de un rectificador y un inversor monofásico sin transformador, un interruptor de transferencia estática de bypass, circuitos de sincronización de bypass y dispositivos de protección. El sistema especificado también incluirá un interruptor de desconexión de batería y un sistema de batería.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Protección contra sobretensiones

El UPS deberá tener protección incorporada contra sobretensiones, caídas y sobre corriente de la fuente AC.

Protección de salida

La UPS estará protegida contra cambios repentinos en la carga de salida y cortocircuitos en las terminales de salida. Deberá tener protección incorporada contra daños permanentes a sí mismo y a la carga conectada para todos los tipos de averías predecibles. Se utilizarán dispositivos limitadores de corriente de acción rápida para proteger contra fallas en cascada de dispositivos de estado sólido.

PANTALLA Y CONTROL

a) Panel de control

La UPS deberá estar provista de un panel de control basado en microprocesador para la interfaz del operador para configurar y supervisar. El panel de control debe estar ubicado en la parte frontal de la unidad donde se puede operar sin abrir la puerta frontal con bisagras. Se utilizará una pantalla de cristal líquido con pantalla táctil a color y retro iluminada, con gráficos completos, para introducir los puntos de ajuste, información del sistema, información de mediciones, eventos activos, historial de eventos, instrucciones de inicio.

No se utilizarán pulsadores mecánicos.

b) Valores medibles

Un microprocesador controlará las funciones de visualización y memoria del sistema de monitorización. Todos los parámetros de tensión y corriente deben ser monitorizados usando mediciones de RMS verdaderas para una precisión de $\pm 3\%$ de la tensión, $\pm 5\%$ de corriente alterna.

Se visualizarán los siguientes parámetros:

Tensión de entrada, línea a línea.

Corriente de entrada por fase.

Voltaje de la batería.

Frecuencia de entrada.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Potencia aparente de entrada (kVA).

Corriente de carga / descarga de la batería.

Tensión de salida, línea a línea.

Frecuencia de salida.

Tensión de entrada bypass, línea a línea.

Bypass: frecuencia de entrada.

Corriente de carga.

Potencia real de la carga (kW), total y porcentaje.

Potencia aparente de la carga (kVA), total y porcentaje.

Porcentaje de carga.

Temperatura de la batería.

Estado de carga de la batería

c) Indicador de estado de batería

El indicador de estado de la batería mostrará las condiciones de alarma de DC, El estado de carga de la batería, el voltaje actual de la batería, el tiempo total de descarga.

d) Registro de eventos

Este elemento de menú mostrará la lista de eventos que se han producido recientemente mientras la UPS estaba en funcionamiento. El registro de eventos almacenará hasta 255 eventos.

e) Alarmas

Deberá mostrar mensaje de alarma en caso de anomalía en voltajes, frecuencias, corrientes, paso a bypass, sobre cargas, etc.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Capacidades de monitoreo e integración remota

Deberá estar equipada con tarjeta de comunicación proporcionando capacidades de supervisión y gestión de UPS basadas en la Web y de los siguientes protocolos abiertos de terceros:

Protocolos SNMP

SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA PARA GABINETE DE DISTRIBUCIÓN 3 kVA escalable, 120V

GENERAL

La UPS mantendrá automáticamente la alimentación de AC a la carga crítica dentro de las tolerancias especificadas y sin interrupción durante falla o deterioro de la fuente de alimentación normal.

El fabricante deberá diseñar y suministrar todos los materiales y equipos para que sean totalmente compatibles con las condiciones eléctricas, ambientales y espaciales en el sitio. La UPS incluirá todo el equipo para conectar correctamente la fuente de alimentación de AC a la carga prevista y se diseñará para funcionamiento desatendido.

ESTÁNDARES

La UPS deberá estar construida en concordancia con los siguientes estándares aplicables:

- La UPS deberá estar listada por el estándar UL Standard 1778, cuarta edición.
- Cumplir con las Reglas y Reglamentos de la FCC, Clase A. Este cumplimiento es legalmente requerido para prevenir interferencia con equipos adyacentes.
- Será compatible con las prácticas de cableado, los materiales y la codificación de acuerdo con los requisitos del Código Eléctrico Nacional y los códigos y normas locales aplicables. Se deben hacer provisiones en los gabinetes para permitir la instalación de cableado de entrada, salida y control externo usando canalización o conducto para acceso superior e inferior a entradas, salidas, bypass y conexiones.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

DESCRIPCIÓN DEL SISTEMA

DISEÑO DE REQUERIMIENTOS

- La UPS debe dimensionarse para proporcionar un mínimo de 3 kVA a la salida.
- El voltaje de la carga y el voltaje de la línea de derivación serán de 120VAC.
- La planta de baterías será un sistema de batería de celdas sellado, localizado en gabinete. Las baterías deben soportar el UPS a 100% de carga final (2.7 KW) durante al menos 15 minutos. Deberán ser baterías de válvula-regulada (VRLA) de calcio plomo, sellado y de mantenimiento reducido.
- La UPS debe ser un diseño libre de transformador (no debe requerir ningún transformador interno en la vía de alimentación principal para el funcionamiento básico del módulo). Los transformadores opcionales en gabinetes o de otro modo externo al módulo básico del UPS deberán permitir el aislamiento.
- La UPS deberá tener un convertidor / rectificador con corrección activa de factor de potencia, capaz de mantener el factor de potencia de entrada y la distorsión armónica total de corriente de entrada (THDi) dentro de las especificaciones sin un filtro de entrada adicional.

MODOS DE OPERACIÓN

La UPS funcionará como un sistema en línea en los siguientes modos:

A. Normal: La carga crítica de AC debe alimentarse continuamente con el inversor del UPS. El rectificador / cargador derivará energía de la fuente de AC de la red eléctrica y suministrará corriente continua al convertidor DC-DC, que a su vez suministrará al inversor mientras flota simultáneamente cargando la batería.

B. Baterías: En caso de fallo de la fuente alterna de la red eléctrica, la carga crítica será alimentada por el inversor, el cual, sin ninguna conmutación, obtendrá su energía de la batería a través del convertidor DC-DC. No se producirá interrupción en la alimentación de la carga crítica al fallar o restaurar la fuente AC de la red eléctrica.

C. Recarga: Al restaurar la fuente de alimentación de la red eléctrica, el rectificador suministrará energía al inversor de salida y al convertidor DC-DC, que al mismo tiempo recargará las baterías. Ésta será una función automática y no causará interrupción de la carga crítica.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

D. Bypass: Si se desconecta la UPS, el interruptor de transferencia estática transferirá la carga a la fuente de derivación. El proceso de transferencia no causará interrupción en la alimentación de la carga crítica. Se utilizará un bypass de mantenimiento externo para asegurar el aislamiento completo de la unidad para el servicio de los componentes internos al mismo tiempo que proporciona seguridad contra el arco voltaico.

Requisitos de rendimiento

Los componentes de potencia de estado sólido, dispositivos magnéticos, dispositivos electrónicos y dispositivos de protección contra sobre-corriente deben operar dentro de la temperatura recomendada por el fabricante cuando la UPS está funcionando a una carga crítica del 100% y mantener la carga de la batería bajo temperaturas de operación en el rango de 32°F to 104°F (0°C to 40°C)

Entrada

Voltaje: Las especificaciones de voltaje de entrada/salida del UPS.

Rectificador Entrada de AC: 120V. monofásico, dos hilos más de tierra.

Bypass Entrada de AC: 120V. monofásico, dos hilos más de tierra.

SALIDA AC: 120V, MONOFÁSICO, DE DOS HILOS MÁS TIERRA.

Rango de voltaje: debe soportar los siguientes voltajes ante de entrar a baterías de acuerdo con la carga.

Load Level	1500-3000 VA 120 VAC Input Voltage
100%	102 VAC
90%	96 VAC
80%	90 VAC
70%	84 VAC
60%	78 VAC
50%	72 VAC
40%	66 VAC
30%	60 VAC

Rango frecuencia: 40 - 70Hz.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Factor de potencia: mínimo 0.99 a carga completa con tensión de entrada nominal.

Sobrecarga: 200% por 2 segundos; 150% por 50 segundos con transferencia a bypass.

Salida AC

Capacidad de carga: 100% de la capacidad de carga a 104 ° F (40 ° C) para cualquier carga desde 0,5 a la unidad.

Regulación voltaje: $\pm 3\%$ RMS cargas balanceadas.

Rango de ajuste de voltaje: 110V, 115V, 120V, 127V.

Forma de onda: Sinusoidal.

Eficiencia del sistema: Definida como kW salida / kW de entrada al factor de potencia de carga deberá ser mayor al 88%.

Tierra

El chasis del UPS tendrá terminal de tierra del equipo.

Condiciones ambientales

La UPS será capaz de soportar las siguientes condiciones ambientales sin dañar o degradar las características operativas:

Temperatura ambiente de funcionamiento

UPS: 32°F a 104°F (0°C a 40°C).

Baterías: 77°F (25°C), $\pm 5^\circ\text{F}$ ($\pm 3^\circ\text{C}$).

Humedad relativa

0 a 95%, sin condensación.

Nivel de ruido audible

< 46 dBA, a 1 metro.



Departamento de Compras y Contrataciones

“Año de la Innovación y la Competitividad”

GARANTÍA Y MANTENIMIENTOS

UPS

El fabricante de la UPS garantizará la unidad contra defectos de mano de obra y materiales durante 24 meses después de la puesta en marcha inicial.

FABRICACIÓN

Materiales

Todos los materiales del UPS serán nuevos, de fabricación actual, de alto grado y no deberán haber estado en servicio previo excepto como se requiera durante las pruebas de fábrica. Todos los dispositivos electrónicos activos deberán ser de estado sólido. Todos los semiconductores de potencia deben estar sellados. La lógica de control y los fusibles deben estar físicamente aislados de los componentes del tren de potencia para garantizar la seguridad del operador y la protección contra el calor.

Construcción y montaje

La UPS deberá estar en gabinetes con encerramiento NEMA Tipo 1, diseñados para montaje en el suelo.

Enfriamiento

Se deben proveer sensores de temperatura para monitorear la temperatura interna del UPS. Al detectar temperaturas superiores a las recomendaciones del fabricante, los sensores deben hacer sonar las alarmas audibles y se visualizarán las alarmas visuales en el panel de control del UPS. Los filtros de aire deben estar situados en el punto de entrada de aire y ser cambiables. En la parte trasera del sistema no se requerirá limpieza o ventilación.

EQUIPAMIENTO

Sistema UPS

El sistema UPS deberá estar compuesto de un rectificador y un inversor monofásico sin transformador, un interruptor de transferencia estática de bypass, circuitos de sincronización de bypass y dispositivos de protección. El sistema especificado también incluirá un interruptor de desconexión de batería y un sistema de batería.

Protección contra sobretensiones

El UPS deberá tener protección incorporada contra sobretensiones, caídas y sobre corriente de la fuente AC.



Departamento de Compras y Contrataciones

“Año de la Innovación y la Competitividad”

Protección de salida

La UPS estará protegida contra cambios repentinos en la carga de salida y cortocircuitos en las terminales de salida. Deberá tener protección incorporada contra daños permanentes a sí mismo ya la carga conectada para todos los tipos de averías predecibles. Se utilizarán dispositivos limitadores de corriente de acción rápida para proteger contra fallas en cascada de dispositivos de estado sólido.

PANTALLA Y CONTROL

Panel de control

La UPS deberá estar provista de un panel de control basado en microprocesador para la interfaz del operador para configurar y supervisar. El panel de control debe estar ubicado en la parte frontal de la unidad donde se puede operar sin abrir la puerta frontal con bisagras. Se utilizará una pantalla de cristal líquido con pantalla táctil a color y retroiluminada, con gráficos completos, para introducir los puntos de ajuste, información del sistema, información de mediciones, eventos activos, historial de eventos, instrucciones de inicio.

No se utilizarán pulsadores mecánicos.

Valores medibles

Un microprocesador controlará las funciones de visualización y memoria del sistema de monitorización. Todos los parámetros de tensión y corriente deben ser monitorizados usando mediciones de RMS verdaderas para una precisión de $\pm 3\%$ de la tensión, $\pm 5\%$ de corriente alterna. Se visualizarán los siguientes parámetros:

Tensión de entrada, línea a línea

Corriente de entrada por fase

Frecuencia de entrada

Potencia aparente de entrada (kVA)

Voltaje de la batería

Corriente de carga / descarga de la batería

Tensión de salida, línea a línea

Frecuencia de salida

Tensión de entrada bypass, línea a línea



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Bypass: frecuencia de entrada

Corriente de carga

Potencia real de la carga (kW), total y porcentaje

Potencia aparente de la carga (kVA), total y porcentaje

Porcentaje de carga

Temperatura de la batería

Estado de carga de la batería

Indicador de estado de batería

El indicador de estado de la batería mostrará las condiciones de alarma de DC, El estado de carga de la batería, el voltaje actual de la batería, el tiempo total de descarga.

Registro de eventos

Este elemento de menú mostrará la lista de eventos que se han producido recientemente mientras la UPS estaba en funcionamiento. El registro de eventos almacenará hasta 255 eventos.

Alarmas

Deberá mostrar mensaje de alarma en caso de anomalía en voltajes, frecuencias, corrientes, paso a bypass, sobre cargas, etc.

Capacidades de monitoreo e integración remota

Deberá estar equipada con tarjeta de comunicación proporcionando capacidades de supervisión y gestión de UPS basadas en la Web y de los siguientes protocolos abiertos de terceros:

Protocolos SNMP



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA PARA GABINETE DE DISTRIBUCIÓN 6 kVA escalable, 208V

GENERAL

La UPS mantendrá automáticamente la alimentación de AC a la carga crítica dentro de las tolerancias especificadas y sin interrupción durante falla o deterioro de la fuente de alimentación normal.

El fabricante deberá diseñar y suministrar todos los materiales y equipos para que sean totalmente compatibles con las condiciones eléctricas, ambientales y espaciales en el sitio. La UPS incluirá todo el equipo para conectar correctamente la fuente de alimentación de AC a la carga prevista y se diseñará para funcionamiento desatendido.

ESTÁNDARES

La UPS deberá estar construida en concordancia con los siguientes estándares aplicables:

- La UPS deberá estar listada por el estándar UL Standard 1778, cuarta edición.
- Cumplir con las Reglas y Reglamentos de la FCC, Clase A. Este cumplimiento es legalmente requerido para prevenir interferencia con equipos adyacentes.
- Será compatible con las prácticas de cableado, los materiales y la codificación de acuerdo con los requisitos del Código Eléctrico Nacional y los códigos y normas locales aplicables. Se deben hacer provisiones en los gabinetes para permitir la instalación de cableado de entrada, salida y control externo usando canalización o conducto para acceso superior e inferior a entradas, salidas, bypass y conexiones.

DESCRIPCIÓN DEL SISTEMA

DISEÑO DE REQUERIMIENTOS

- La UPS debe dimensionarse para proporcionar un mínimo de 6 kVA a la salida.
- El voltaje de la carga y el voltaje de la línea de derivación serán de 208VAC, bifásico, dos hilos más tierra. El voltaje de entrada será 208VAC, bifásico, dos hilos más tierra. La fuente de entrada de AC y la fuente de entrada de derivación deberán ser cada una un servicio de punto de conexión sólidamente conectado a tierra.



Departamento de Compras y Contrataciones “Año de la Innovación y la Competitividad”

- La planta de baterías será un sistema de batería de celdas sellado, localizado en gabinete. Las baterías deben soportar el UPS a 100% de carga final (4.2 KW) durante al menos 15 minutos. Deberán ser baterías de válvula-regulada (VRLA) de calcio plomo, sellado y de mantenimiento reducido.
- La UPS deberá tener un convertidor / rectificador con corrección activa de factor de potencia, capaz de mantener el factor de potencia de entrada y la distorsión armónica total de corriente de entrada (THDi) dentro de las especificaciones sin un filtro de entrada adicional.
- La UPS debe ser un diseño libre de transformador (no debe requerir ningún transformador interno en la vía de alimentación principal para el funcionamiento básico del módulo). Los transformadores opcionales en gabinetes o de otro modo externo al módulo básico del UPS deberán permitir el aislamiento.

MODOS DE OPERACIÓN

El UPS funcionará como un sistema **en línea** en los siguientes modos:

Normal: La carga crítica de AC debe alimentarse continuamente con el inversor del UPS. El rectificador / cargador derivará energía de la fuente de AC de la red eléctrica y suministrará corriente continua al convertidor DC-DC, que a su vez suministrará al inversor mientras flota simultáneamente cargando la batería.

Baterías: En caso de fallo de la fuente alterna de la red eléctrica, la carga crítica será alimentada por el inversor, el cual, sin ninguna conmutación, obtendrá su energía de la batería a través del convertidor DC-DC. No se producirá interrupción en la alimentación de la carga crítica al fallar o restaurar la fuente AC de la red eléctrica.

Recarga: Al restaurar la fuente de alimentación de la red eléctrica, el rectificador suministrará energía al inversor de salida y al convertidor DC-DC, que al mismo tiempo recargará las baterías. Ésta será una función automática y no causará interrupción de la carga crítica.

Bypass: Si se desconecta la UPS, el interruptor de transferencia estática transferirá la carga a la fuente de derivación. El proceso de transferencia no causará interrupción en la alimentación de la carga crítica. Se utilizará un bypass de mantenimiento externo para asegurar el aislamiento completo de la unidad para el servicio de los componentes internos al mismo tiempo que proporciona seguridad contra el arco voltaico.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

REQUISITOS DE RENDIMIENTO

Los componentes de potencia de estado sólido, dispositivos magnéticos, dispositivos electrónicos y dispositivos de protección contra sobre corriente deben operar dentro de la temperatura recomendada por el fabricante cuando la UPS está funcionando a una carga crítica del 100% y mantener la carga de la batería bajo temperaturas de operación en el rango de 32°F to 104°F (0°C to 40°C).

Entrada

Voltaje: Las especificaciones de voltaje de entrada/salida del UPS

Rectificador Entrada de AC: 208V, bifásico, de dos hilos-más-tierra.

Bypass Entrada de AC: 208V, bifásico, de dos hilos más tierra.

Salida AC: 208V, bifásico, de dos hilos más tierra.

Rango de voltaje: debe soportar los siguientes voltajes ante de entrar a baterías de acuerdo con la carga

Porcentaje de carga	voltaje
100% to 91%	188 ± 5.0VAC
90% to 71%	171 ± 5.0VAC
70% to 31%	151 ± 5.0VAC
30% to 0%	112 ± 5.0VAC

Rango frecuencia: 40 - 70Hz.

Factor de potencia: mínimo 0.99 a carga completa con tensión de entrada nominal.

Sobrecarga: 200% por 2 segundos; 150% por 50 segundos con transferencia a bypass.

Salida AC

Capacidad de carga: 100% de la capacidad de carga a 104 ° F (40 ° C) para cualquier carga desde 0,5 a la unidad.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Regulación voltaje: $\pm 3\%$ RMS cargas balanceadas.

Rango de ajuste de voltaje: 208/220/230/240 VAC.

Forma de onda: Sinusoidal.

Eficiencia del sistema: Definida como kW salida / kW de entrada al factor de potencia de carga deberá ser mayor al 88%.

Tierra

El chasis del UPS tendrá terminal de tierra del equipo.

CONDICIONES AMBIENTALES

La UPS será capaz de soportar las siguientes condiciones ambientales sin dañar o degradar las características operativas:

Temperatura ambiente de funcionamiento

UPS: 32°F a 104°F (0°C a 40°C).

Baterías: 77°F (25°C), $\pm 5^\circ\text{F}$ ($\pm 3^\circ\text{C}$).

Humedad relativa

0 a 95%, sin condensación.

Nivel de ruido audible

< 46 dBA, a 1 metro.

GARANTÍA Y MANTENIMIENTOS

UPS

El fabricante de la UPS garantizará la unidad contra defectos de mano de obra y materiales durante 12 meses después de la puesta en marcha inicial, incluirá los mantenimientos pertinentes.



Departamento de Compras y Contrataciones

“Año de la Innovación y la Competitividad”

FABRICACIÓN

Materiales

Todos los materiales del UPS serán nuevos, de fabricación actual, de alto grado y no deberán haber estado en servicio previo excepto como se requiera durante las pruebas de fábrica. Todos los dispositivos electrónicos activos deberán ser de estado sólido. Todos los semiconductores de potencia deben estar sellados. La lógica de control y los fusibles deben estar físicamente aislados de los componentes del tren de potencia para garantizar la seguridad del operador y la protección contra el calor.

Construcción y montaje

La UPS deberá estar en gabinetes con encerramiento NEMA Tipo 1, diseñados para montaje en el suelo.

Enfriamiento

Se deben proveer sensores de temperatura para monitorear la temperatura interna del UPS. Al detectar temperaturas superiores a las recomendaciones del fabricante, los sensores deben hacer sonar las alarmas audibles y se visualizarán las alarmas visuales en el panel de control del UPS. Los filtros de aire deben estar situados en el punto de entrada de aire y ser cambiables. En la parte trasera del sistema no se requerirá limpieza o ventilación.

EQUIPAMIENTO

Sistema UPS

El sistema UPS deberá estar compuesto de un rectificador, y un inversor bifásico sin transformador, un interruptor de transferencia estática de bypass, circuitos de sincronización de bypass y dispositivos de protección. El sistema especificado también incluirá un interruptor de desconexión de batería y un sistema de batería.

Protección contra sobretensiones

El UPS deberá tener protección incorporada contra sobretensiones, caídas y sobre corriente de la fuente AC. La protección deberá cumplir con los requisitos de ANSI C62.41 A3 y B3.

Protección de salida

La UPS estará protegida contra cambios repentinos en la carga de salida y cortocircuitos en las terminales de salida. Deberá tener protección incorporada contra daños permanentes a sí mismo y a la carga conectada para todos los tipos de averías predecibles. Se utilizarán dispositivos limitadores de corriente de acción rápida para proteger contra fallas en cascada de dispositivos de estado sólido.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

PANTALLA Y CONTROL

Panel de control

La UPS deberá estar provista de un panel de control basado en microprocesador para la interfaz del operador para configurar y supervisar. El panel de control debe estar ubicado en la parte frontal de la unidad donde se puede operar sin abrir la puerta frontal con bisagras. Se utilizará una pantalla de cristal líquido con pantalla táctil a color y retroiluminada, con gráficos completos, para introducir los puntos de ajuste, información del sistema, información de mediciones, eventos activos, historial de eventos, instrucciones de inicio.

No se utilizarán pulsadores mecánicos.

Valores medibles

Un microprocesador controlará las funciones de visualización y memoria del sistema de monitorización. Las dos fases de los parámetros bifásicos se visualizarán simultáneamente. Todos los parámetros de tensión y corriente deben ser monitorizados usando mediciones de RMS verdaderas para una precisión de $\pm 3\%$ de la tensión, $\pm 5\%$ de corriente alterna. Se visualizarán los siguientes parámetros:

- Tensión de entrada, línea a línea
- Corriente de entrada por fase
- Frecuencia de entrada
- Potencia aparente de entrada (kVA)
- Voltaje de la batería
- Corriente de carga / descarga de la batería
- Tensión de salida, línea a línea
- Frecuencia de salida
- Tensión de entrada bypass, línea a línea
- Bypass: frecuencia de entrada
- Corriente de carga
- Potencia real de la carga (kW), total y porcentaje
- Potencia aparente de la carga (kVA), total y porcentaje
- Porcentaje de carga
- Temperatura de la batería
- Estado de carga de la batería



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Indicador de estado de batería

El indicador de estado de la batería mostrará las condiciones de alarma de DC, el estado de carga de la batería, el voltaje actual de la batería, el tiempo total de descarga.

Registro de eventos

Este elemento de menú mostrará la lista de eventos que se han producido recientemente mientras la UPS estaba en funcionamiento. El registro de eventos almacenará hasta 255 eventos.

Alarmas

Deberá mostrar mensaje de alarma en caso de anomalía en voltajes, frecuencias, corrientes, paso a bypass, sobre cargas, etc.

Capacidades de monitoreo e integración remota

Deberá estar equipada con tarjeta de comunicación proporcionando capacidades de supervisión y gestión de UPS basadas en la Web y de los siguientes protocolos abiertos de terceros:

Protocolos SNMP

SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA PARA GABINETE DE DISTRIBUCIÓN 10 kVA escalable, 208V

GENERAL

La UPS mantendrá automáticamente la alimentación de AC a la carga crítica dentro de las tolerancias especificadas y sin interrupción durante falla o deterioro de la fuente de alimentación normal.

El fabricante deberá diseñar y suministrar todos los materiales y equipos para que sean totalmente compatibles con las condiciones eléctricas, ambientales y espaciales en el sitio. La UPS incluirá todo el equipo para conectar correctamente la fuente de alimentación de AC a la carga prevista y se diseñará para funcionamiento desatendido.

ESTÁNDARES

La UPS deberá estar construida en concordancia con los siguientes estándares aplicables:

- La UPS deberá estar listada por el estándar UL Standard 1778, cuarta edición.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Cumplir con las Reglas y Reglamentos de la FCC, Clase A. Este cumplimiento es legalmente requerido para prevenir interferencia con equipos adyacentes.
- Será compatible con las prácticas de cableado, los materiales y la codificación de acuerdo con los requisitos del Código Eléctrico Nacional y los códigos y normas locales aplicables. Se deben hacer provisiones en los gabinetes para permitir la instalación de cableado de entrada, salida y control externo usando canalización o conducto para acceso superior e inferior a entradas, salidas, bypass y conexiones.

DESCRIPCIÓN DEL SISTEMA

DISEÑO DE REQUERIMIENTOS

La UPS debe dimensionarse para proporcionar un mínimo de 10 kVA a la salida.

- El voltaje de la carga y el voltaje de la línea de derivación serán de 208VAC, bifásico, dos hilos más tierra. El voltaje de entrada será 208VAC, bifásico, dos hilos más tierra. La fuente de entrada de AC y la fuente de entrada de derivación deberán ser cada una un servicio de punto de conexión sólidamente conectado a tierra.
- La planta de baterías será un sistema de batería de celdas sellado, localizado en gabinete. Las baterías deben soportar el UPS a 100% de carga final (9 KW) durante al menos 15 minutos. Deberán ser baterías de válvula-regulada (VRLA) de calcio plomo, sellado y de mantenimiento reducido.
- La UPS deberá tener un convertidor / rectificador con corrección activa de factor de potencia, capaz de mantener el factor de potencia de entrada y la distorsión armónica total de corriente de entrada (THDi) dentro de las especificaciones sin un filtro de entrada adicional.
- La UPS debe ser un diseño libre de transformador (no debe requerir ningún transformador interno en la vía de alimentación principal para el funcionamiento básico del módulo). Los transformadores opcionales en gabinetes o de otro modo externo al módulo básico del UPS deberán permitir el aislamiento.

MODOS DE OPERACIÓN

El UPS funcionará como un sistema **en línea** en los siguientes modos:

Normal: La carga crítica de AC debe alimentarse continuamente con el inversor del UPS. El rectificador / cargador derivará energía de la fuente de AC de la red eléctrica y



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

suministrará corriente continua al convertidor DC-DC, que a su vez suministrará al inversor mientras flota simultáneamente cargando la batería.

Baterías: En caso de fallo de la fuente alterna de la red eléctrica, la carga crítica será alimentada por el inversor, el cual, sin ninguna conmutación, obtendrá su energía de la batería a través del convertidor DC-DC. No se producirá interrupción en la alimentación de la carga crítica al fallar o restaurar la fuente AC de la red eléctrica.

Recarga: Al restaurar la fuente de alimentación de la red eléctrica, el rectificador suministrará energía al inversor de salida y al convertidor DC-DC, que al mismo tiempo recargará las baterías. Ésta será una función automática y no causará interrupción de la carga crítica.

Bypass: Si se desconecta la UPS, el interruptor de transferencia estática transferirá la carga a la fuente de derivación. El proceso de transferencia no causará interrupción en la alimentación de la carga crítica. Se utilizará un bypass de mantenimiento externo para asegurar el aislamiento completo de la unidad para el servicio de los componentes internos al mismo tiempo que proporciona seguridad contra el arco voltaico.

REQUISITOS DE RENDIMIENTO

Los componentes de potencia de estado sólido, dispositivos magnéticos, dispositivos electrónicos y dispositivos de protección contra sobre corriente deben operar dentro de la temperatura recomendada por el fabricante cuando la UPS está funcionando a una carga crítica del 100% y mantener la carga de la batería bajo temperaturas de operación en el rango de 32°F to 104°F (0°C to 40°C).

Entrada

Voltaje: Las especificaciones de voltaje de entrada/salida del UPS

Rectificador Entrada de AC: 208V, bifásico, de dos hilos-más-tierra.

Bypass Entrada de AC: 208V, bifásico, de dos hilos más tierra.

Salida AC: 208V, bifásico, de dos hilos más tierra.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Rango de voltaje: debe soportar los siguientes voltajes ante de entrar a baterías de acuerdo con la carga

Carga	voltaje
100% to 91%	100 ± 3.1VAC
90% to 71%	91 ± 3.1VAC
70% to 31%	77 ± 3.1VAC
30% to 0%	• ± 3.1VAC

Rango frecuencia: 40 - 70Hz.

Factor de potencia: mínimo 0.99 a carga completa con tensión de entrada nominal.

Sobrecarga: 200% por 2 segundos; 150% por 50 segundos con transferencia a bypass.

Salida AC

Capacidad de carga: 100% de la capacidad de carga a 104 ° F (40 ° C) para cualquier carga desde 0,5 a la unidad.

Regulación voltaje: ±3% RMS cargas balanceadas.

Rango de ajuste de voltaje: 208/220/230/240 VAC.

Forma de onda: Sinusoidal.

Eficiencia del sistema: Definida como kW salida / kW de entrada al factor de potencia de carga deberá ser mayor al 88%.

Tierra

El chasis del UPS tendrá terminal de tierra del equipo.

Condiciones ambientales

La UPS será capaz de soportar las siguientes condiciones ambientales sin dañar o degradar las características operativas:



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Temperatura ambiente de funcionamiento

UPS: 32°F a 104°F (0°C a 40°C).

Baterías: 77°F (25°C), ±5°F (±3°C).

Humedad relativa

0 a 95%, sin condensación.

Nivel de ruido audible

< 46 dBA, a 1 metro.

GARANTÍA Y MANTENIMIENTOS

UPS

El fabricante de la UPS garantizará la unidad contra defectos de mano de obra y materiales durante 12 meses después de la puesta en marcha inicial, incluirá los mantenimientos pertinentes.

FABRICACIÓN

Materiales

Todos los materiales del UPS serán nuevos, de fabricación actual, de alto grado y no deberán haber estado en servicio previo excepto como se requiera durante las pruebas de fábrica. Todos los dispositivos electrónicos activos deberán ser de estado sólido. Todos los semiconductores de potencia deben estar sellados. La lógica de control y los fusibles deben estar físicamente aislados de los componentes del tren de potencia para garantizar la seguridad del operador y la protección contra el calor.

Construcción y montaje

La UPS deberá estar en gabinetes con encerramiento NEMA Tipo 1, diseñados para montaje en el suelo.

Enfriamiento

Se deben proveer sensores de temperatura para monitorear la temperatura interna del UPS. Al detectar temperaturas superiores a las recomendaciones del fabricante, los sensores deben hacer sonar las alarmas audibles y se visualizarán las alarmas visuales en el panel de control del UPS. Los filtros de aire deben estar situados en el punto de entrada de aire y ser cambiables. En la parte trasera del sistema no se requerirá limpieza o ventilación.



Departamento de Compras y Contrataciones

“Año de la Innovación y la Competitividad”

EQUIPAMIENTO

Sistema UPS

El sistema UPS deberá estar compuesto de un rectificador, y un inversor bifásico sin transformador, un interruptor de transferencia estática de bypass, circuitos de sincronización de bypass y dispositivos de protección. El sistema especificado también incluirá un interruptor de desconexión de batería y un sistema de batería.

Protección contra sobretensiones

El UPS deberá tener protección incorporada contra sobretensiones, caídas y sobre corriente de la fuente AC. La protección deberá cumplir con los requisitos de ANSI C62.41 A3 y B3.

Protección de salida

La UPS estará protegida contra cambios repentinos en la carga de salida y cortocircuitos en las terminales de salida. Deberá tener protección incorporada contra daños permanentes a sí mismo ya la carga conectada para todos los tipos de averías predecibles. Se utilizarán dispositivos limitadores de corriente de acción rápida para proteger contra fallas en cascada de dispositivos de estado sólido.

PANTALLA Y CONTROL

PANEL DE CONTROL

La UPS deberá estar provista de un panel de control basado en microprocesador para la interfaz del operador para configurar y supervisar. El panel de control debe estar ubicado en la parte frontal de la unidad donde se puede operar sin abrir la puerta frontal con bisagras. Se utilizará una pantalla de cristal líquido con pantalla táctil a color y retro iluminada, con gráficos completos, para introducir los puntos de ajuste, información del sistema, información de mediciones, eventos activos, historial de eventos, instrucciones de inicio.

No se utilizarán pulsadores mecánicos.

Valores medibles

Un microprocesador controlará las funciones de visualización y memoria del sistema de monitorización. Las dos fases de los parámetros bifásicos se visualizarán simultáneamente. Todos los parámetros de tensión y corriente deben ser monitorizados usando mediciones de RMS verdaderas para una precisión de $\pm 3\%$ de la tensión, $\pm 5\%$ de corriente alterna. Se visualizarán los siguientes parámetros:

Tensión de entrada, línea a línea.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Corriente de entrada por fase.
Frecuencia de entrada.
Potencia aparente de entrada (kVA).
Voltaje de la batería.
Corriente de carga / descarga de la batería.
Tensión de salida, línea a línea.
Frecuencia de salida.
Tensión de entrada bypass, línea a línea.
Bypass: frecuencia de entrada.
Corriente de carga.
Potencia real de la carga (kW), total y porcentaje.
Potencia aparente de la carga (kVA), total y porcentaje.
Porcentaje de carga.
Temperatura de la batería.
Estado de carga de la batería.

Registro de eventos

Este elemento de menú mostrará la lista de eventos que se han producido recientemente mientras la UPS estaba en funcionamiento. El registro de eventos almacenará hasta 255 eventos.

Indicador de estado de batería

El indicador de estado de la batería mostrará las condiciones de alarma de DC, el estado de carga de la batería, el voltaje actual de la batería, el tiempo total de descarga.

Alarmas

Deberá mostrar mensaje de alarma en caso de anormalidad en voltajes, frecuencias, corrientes, paso a bypass, sobre cargas, etc.

Capacidades de monitoreo e integración remota

Deberá estar equipada con tarjeta de comunicación proporcionando capacidades de supervisión y gestión de UPS basadas en la Web y de los siguientes protocolos abiertos de terceros:

Protocolos SNMP.



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

SWITCH

INTRODUCCIÓN

Suministro, instalación y configuración de todos los equipos de red descritos a continuación deben ser de una sola marca, a fin de garantizar la integridad y garantías correspondientes de la instalación. No se aceptarán ofertas donde se mezclen componentes o subsistemas de más de un (1) fabricante.

Los oferentes deben presentar las evidencias físicas de que los dispositivos a suministrar cumplen con las normas y estándares establecidos. Los equipos tendrán identificadores de su respectiva marca para ser aceptados.

SWITCH 1

Switch Apilable de Alta Capacidad L3+	Los switches tienen una capacidad de 1.92 Terabits para eliminar cuellos de botella, garantizando una transmisión de video y todo el tráfico de grandes redes y con alta disponibilidad. Los switches cuentan con 24 x 1/10 Puertos Gigabit SFP + o 24 x 1 / 2.5 / 5/10 puertos de cobre Gigabit para permitir flexibilidad, mientras que cuentan con 4 puertos 40G / 100G que proporcionan backbone de alta velocidad, conectividad con una bahía de expansión adicional y la habilidad de apilar múltiples equipos.
Inteligencia	PSU duales intercambiables en caliente con redundancia 1 + 1 Soporte de alimentación dual: un circuito de alimentación separado puede alimentar cada fuente de alimentación proporcionando una fiabilidad adicional Módulo de expansión intercambiable en caliente (XEM) Módulos de ventilador intercambiables en caliente Control ambiental completo de fuentes de alimentación, ventiladores, Temperatura y tensiones internas, con SNMP.



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	<p>Alertas para alertar a los administradores de redes en caso de cualquier falla.</p> <p>Soporte para puertos 4 x 40G o 100G y una bahía de expansión para agregar más capacidad de conmutación.</p>
Seguridad avanzada	<p>Listas de control de acceso (ACL) basadas en las capas 3 y 4</p> <p>ACL configurables para el tráfico de gestión</p> <p>Fallo de autenticación y VLAN invitadas</p> <p>Autenticación, Autorización y Contabilidad (AAA)</p> <p>Bootloader (BIOS) puede estar protegido por contraseña para seguridad del dispositivo.</p> <p>Protección BPDU</p> <p>Detección DHCP, protección de IP Origen e Inspección Dinámica de ARP (DAI)</p> <p>Asignación dinámica de VLAN</p> <p>Filtrado de direcciones MAC y bloqueo de direcciones MAC</p> <p>Límites de aprendizaje basados en puerto (detección de intrusión)</p> <p>Las VLAN privadas proporcionan seguridad y aislamiento de puertos</p> <p>para múltiples clientes utilizando la misma VLAN</p> <p>Copia Segura (SCP)</p> <p>Cliente de Protocolo seguro de transferencia de archivos (SFTP)</p> <p>Seguridad de contraseña fuerte y cifrado</p> <p>Autorización de comando TACACS +</p>



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	<p>Tri-autenticación: basada en MAC, basada en web y IEEE 802.1x</p> <p>Autenticación basada en web</p> <p>Selección del grupo RADIUS por VLAN o puerto</p>
Servicios Avanzados	<p>Guest VLANs, Dynamic VLANs y Voice VLANs.</p> <p>8 colas de prioridad por puerto.</p> <p>Cuatro niveles de Servicios QoS.</p> <p>IEEE 802.1p basado en Clase de Servicio (CoS).</p> <p>LLDP-MED</p> <p>Double VLAN Tagging (Q-in-Q)</p> <p>Velocidad de cable (Wirespeed) en L2/L3/L4.</p> <p>Apilamiento a través de Enhanced Stacking hasta 24 switches.</p> <p>Ecologicamente amigables por eficiencia en el consumo de energía.</p>
Herramientas de diagnóstico	<p>El monitoreo activo de fibra detecta la manipulación en enlaces ópticos</p> <p>Detección automática de fallas de enlace y cierre de puerto</p> <p>Autoprueba incorporada (BIST)</p> <p>Localizador de fallas de cable (TDR)</p> <p>Localizador de dispositivos Find-me</p> <p>Monitorización del estado del hardware.</p> <p>Monitoreo óptico digital de diagnóstico (DDM)</p> <p>Ping de sondeo para IPv4 e IPv6</p> <p>Duplicación de puertos</p>



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	TraceRoute para IPv4 y IPv6 Detección de enlace unidireccional (UDLD)
Ruteo	Enrutamiento de agujero negro Reenvío de difusión dirigido Relay DNS Enrutamiento por rutas múltiples de igual costo (ECMP) Enrutamiento basado en políticas Mapas de ruta Redistribución de rutas (OSPF, BGP, RIP) Enrutamiento estático de unidifusión y multidifusión para IPv4 Ayudante de difusión UDP (ayudante de IP) Hasta 64 rutas virtuales y reenvío (VRF lite) dominios (con licencia) DHCPv6 cliente y reley Cliente DNSv6 y reley IPv4 e IPv6 dual stack IPv6 hardware ACLs Gestión de dispositivos a través de redes IPv6 con SNMPv6, Telnetv6 y SSHv6. Cliente y servidor NTPv6. Enrutamiento estático de unidifusión y multidifusión para IPv6. Inicie sesión en los hosts IPv6 con Syslog v6.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

<p>Calidad de Servicio (QoS)</p>	<p>8 colas con una jerarquía de alta prioridad, colas para el tráfico en tiempo real y la programación mixta para cada puerto de switch.</p> <p>Clasificación de tráfico Wirespeed con baja latencia esencial para aplicaciones de VoIP y medios de transmisión en tiempo real.</p> <p>Limitación del ancho de banda (ancho de banda virtual).</p> <p>Limite el ancho de banda por puerto o por clase de tráfico descendente a 64kbps.</p> <p>Soporte IPv6 QoS y protección contra tormentas compatible con IPv6</p> <p>QoS basada en VLAN, puerto, MAC y clasificadores de paquetes generales</p> <p>Opciones de programación de cola para prioridad estricta, Round robin ponderada o programación mixta.</p>
<p>Administración y Monitoreo</p>	<p>Permite una gestión centralizada potente, instalación y recuperación de dispositivos sin contacto.</p> <p>Puerto de administración de la consola en el panel frontal para facilidad de acceso</p> <p>El modo ecológico permite que los puertos y los LED sean desactivados para ahorrar energía</p> <p>Interfaz gráfica de usuario (GUI) basada en la web</p> <p>CLI estándar de la industria con ayuda sensible al contexto</p> <p>Puerto de gestión de Ethernet 10/100 / 1000T fuera de banda</p> <p>Potente motor de scripting CLI</p> <p>Compatibilidad total con SNMP MIB para estándares de gestión de dispositivos</p>



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	<p>Editor de texto incorporado</p> <p>Los activadores basados en eventos permiten que los scripts definidos por el usuario sean ejecutados en eventos seleccionados del sistema</p> <p>interfaz USB permite archivos de versión de software, configuraciones y otros archivos para ser almacenados para copia de seguridad y distribución a otros dispositivos.</p>
Estándares Ethernet	<p>IEEE 802.2 Logical Link Control (LLC)</p> <p>IEEE 802.3 Ethernet</p> <p>IEEE 802.3ab 1000BASE-T</p> <p>IEEE 802.3ae 10 Gigabit Ethernet</p> <p>IEEE 802.3an 10GBASE-T</p> <p>IEEE 802.3az Energy Efficient Ethernet (EEE)</p> <p>IEEE 802.3ba 40GBASE-X</p> <p>IEEE 802.3bj 100GBASE-X</p> <p>IEEE 802.3bz 2.5GBASE-T and 5GBASE-T</p> <p>IEEE 802.3x Flow control - full-duplex operation</p> <p>IEEE 802.3z 1000BASE-X</p>
Estándares de Seguridad	<p>SSH remote login</p> <p>SSLv2 and SSLv3</p> <p>TACACS+ accounting and authentication (AAA)</p> <p>IEEE 802.1X authentication protocols (TLS, TTLS, PEAP and MD5)</p> <p>IEEE 802.1X multi-suplicant authentication</p> <p>IEEE 802.1X port-based network access control</p> <p>RFC 2818 HTTP over TLS (“HTTPS”)</p>



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	<p>RFC 2865 RADIUS authentication</p> <p>RFC 2866 RADIUS accounting</p> <p>RFC 2868 RADIUS attributes for tunnel protocol support</p> <p>RFC 3280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) profile</p> <p>RFC 3546 Transport Layer Security (TLS) extensions</p> <p>RFC 3579 RADIUS support for Extensible Authentication Protocol (EAP)</p> <p>RFC 3580 IEEE 802.1x RADIUS usage guidelines</p> <p>RFC 3748 PPP Extensible Authentication Protocol (EAP)</p> <p>RFC 4251 Secure Shell (SSHv2) protocol architecture</p> <p>RFC 4252 Secure Shell (SSHv2) authentication protocol</p> <p>RFC 4253 Secure Shell (SSHv2) transport layer protocol</p> <p>RFC 4254 Secure Shell (SSHv2) connection protocol</p> <p>RFC 5246 TLS v1.2</p>
Estándares de VLAN	<p>Generic VLAN Registration Protocol (GVRP)</p> <p>IEEE 802.1ad Provider bridges (VLAN stacking, Q-in-Q)</p> <p>IEEE 802.1Q Virtual LAN (VLAN) bridges</p> <p>IEEE 802.1v VLAN classification by protocol and port</p> <p>IEEE 802.3ac VLAN tagging</p> <p>LLDP-MED ANSI/TIA-1057</p> <p>Voice VLAN</p>
Certificaciones Eléctricas/Mecánicas	<p>EMC: EN55032 class A, FCC class A, VCCI class A</p> <p>Immunity: EN55024, EN61000-3-levels 2</p>



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	(Harmonics), and 3 (Flicker) Standards: UL60950-1, CAN/CSA-C22.2 No. 60950-1-03, EN60950-1, EN60825-1, AS/NZS 60950 Certification: UL, cUL, TUV
Especificaciones Eléctricas	Voltaje CA: 100 a 240V (rango automático de +/- 10%) Frecuencia: 47 a 63Hz
Especificaciones ambientales	Rango de temperatura de funcionamiento: 0 ° C a 50 ° C (32 ° F a 122 ° F)

SWITCH 2

Switch L2/L3/L4+	24 10/100/1000BASE-T, con versatilidad con PoE+ 30Watts por puerto (802.3at). 4 puertos SPF+ 10G o 1Gbps para fibra óptica..
Confiabilidad	Fuente de Poder Redundante disponible para compartir carga con fuente de alimentación interna proporcionando energía ininterrumpida y una mayor fiabilidad. Monitoreo de ambiente completo de PSUs, ventiladores, Temperaturas y voltajes internos. SNMP traps, Alertas de administradores de red en caso de cualquier falla.
Características de Poder o Energía Eléctrica	Voltaje AC: 90 to 260 VAC (auto rango) Frecuencia: 47 to 63Hz
Rango de Consumo de Energía	Sin Carga PoE+ 67 Watts Con carga total PoE+: 530 Watts Máxima disipación de calor 229 BTU/h



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

Especificaciones de Energía	Rango de Temperatura de Operación: 0°C a 45°C (32°F to 113°F).
Flexibilidad y Compatibilidad	4 Ranuras SFP+ para puertos de 1 y 10 Gigabit soportarán cualquier combinación de 10GBase-SR, 10GBase-LR, 1000Base-T, 1000BaseSX, 1000Base-LX, o 1000Base-ZX SFPs Cable Directo SFP+. Cables de Apilamiento:
Soporte de VLAN	Soporta 4096 VLANs VLAN Double Tagging
Seguridad	Active Fiber Monitoring para prevenir desviaciones de señal en comunicaciones sobre fibra óptica. Private VLANs, proporcionando seguridad y aislamiento de Puerto de múltiples usuarios usando la misma VLAN. Asignación Dinámica de VLAN NAC Soporta 802.1x, con multi-suplicante Autenticación basada en MAC. DHCP Snooping Autenticación basada en Web Protección BPDU. STP Root Guard Strong Passwords Bloqueo de ataques DoS ACLs Autenticación TACACS+ Servidor Local RADIUS



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

Calidad de Servicio	<p>Nuevas características en políticas basadas en QoS</p> <p>Altamente configurable la clasificación de tráfico.</p> <p>Amplia destacando las capacidades.</p> <p>Plano de control de priorización de tráfico</p> <p>Programación Mixta</p> <p>8 colas QoS por puerto.</p> <p>Baja latencia de conmutación esencial para la voz sobre IP (VoIP) y transmisión en tiempo real de aplicaciones multimedia.</p>
Administración	<p>Puerto de consola de gestión en el panel frontal para facilitar el acceso.</p> <p>La interfaz gráfica de usuario simplifica la monitorización de red y el rendimiento de la red de tiro evento problemas.</p> <p>Una ranura de la tarjeta de memoria USB en el panel frontal, permitiendo que los archivos versión de software, configuraciones y otros archivos a guardar la copia de seguridad y de distribución a otros switches.</p> <p>Port mirroring</p> <p>SSH and SNMPv3 para administración de switches.</p> <p>Autenticación RADIUS</p> <p>RMON (4 grupos)</p> <p>Desvío de difusión para que el interruptor de paquetes de difusión para llegar a través de subredes.</p> <p>Ayuda de IP permite a las emisiones de los clientes en diferentes subredes se retransmitan a su destino, en vez de ser bloqueados con el interruptor.</p> <p>Políticas Basadas en Routing (PBR)</p>



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) sFlow
Aprobaciones eléctrica y cumplimiento de normas	EMC: EN55022 class A, FCC class A, VCCI class A, ICES-003 class A Inmunidad: EN55024, EN61000-3-levels 2(Harmonics), and 3 (Flicker)
Seguridad	Estándares: UL60950-1, CAN/CSA-C22.2 No. 60950-1-03, EN60950-1, EN60825-1, AS/NZS 60950.1 Certificación en: UL, cUL, TUV
Cumplimiento de normas en sustancias peligrosas	EU Cumplimiento de normas en RoHS
Herramientas de Diagnóstico	Built-In Self Test (BIST) Ping Polling Port Mirroring Trace Route
Ethernet	IEEE 802.1AX - 2008 Link Aggregation IEEE 802.2 Logical Link Control IEEE 802.3 Ethernet CSMA/CD IEEE 802.3ab 1000BASE-T IEEE 802.3ad Link Aggregation (static & LACP-based dynamic) IEEE 802.3ae 10 Gigabit Ethernet IEEE 802.3af Power over Ethernet (PoE) IEEE 802.3at Power over Ethernet (PoE+) IEEE 802.3u 100BASE-T



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	IEEE 802.3x Flow Control - Full Duplex Operation IEEE 802.3z Gigabit Ethernet
Ruteo en General	RFC 768 User Datagram Protocol (UDP) RFC 791 Internet Protocol (IP) RFC 792 Internet Control Message Protocol (ICMP) RFC 793 Transmission Control Protocol (TCP) RFC 826 Address Resolution Protocol (ARP) RFC 894 Standard for the transmission of IP datagrams over Ethernet networks RFC 919 Broadcasting Internet Datagrams RFC 922 Broadcasting Internet datagrams in the presence of subnets RFC 932 Subnetwork addressing scheme RFC 950 Internet Standard Subnetting Procedure RFC 951 Bootstrap Protocol (BootP) RFC 1027 Proxy ARP RFC 1035 DNS Client RFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks RFC 1071 Computing the Internet checksum RFC 1122 Internet Host Requirements RFC 1191 Path MTU discovery RFC 1256 ICMP Router Discovery Messages RFC 1518 An Architecture for IP Address Allocation conCIDR



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	<p>RFC 1519 Classless Inter-Domain Routing (CIDR)</p> <p>RFC 1542 Clarifications & Extensions for the Bootstrap Protocol</p> <p>RFC 1591 Domain Name System (DNS)</p> <p>RFC 1812 Requirements for IPv4 Routers</p> <p>RFC 1918 IP Addressing</p> <p>RFC 2581 TCP Congestión Control</p>
Administración	<p>AT Enterprise MIB</p> <p>SNMPv1, v2c and v3</p> <p>IEEE 802.1AB Link Layer Discovery Protocol (LLDP)</p> <p>RFC 1155 Structure and Identification of Management Information for TCP/IP-based Internets</p> <p>RFC 1157 Simple Network Management Protocol (SNMP)</p> <p>RFC 1212 Concise MIB definitions</p> <p>RFC 1213 MIB for Network Management of TCP/IP-based internets: MIB-II</p> <p>RFC 1215 Convention for defining traps for use with the SNMP</p> <p>RFC 1227 SNMP MUX protocol and MIB</p> <p>RFC 1239 Standard MIB</p> <p>RFC 1493 Bridge MIB</p> <p>RFC 2011 SNMPv2 MIB for IP using SMIPv2</p> <p>RFC 2012 SNMPv2 MIB for TCP using SMIPv2</p> <p>RFC 2013 SNMPv2 MIB for UDP using SMIPv2</p> <p>RFC 2096 IP Forwarding Table MIB</p>



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	<p>RFC 2578 Structure of Management Information v2 (SMIv2)</p> <p>RFC 2579 Textual Conventions for SMIv2</p> <p>RFC 2580 Conformance Statements for SMIv2</p> <p>RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and VLAN Extensions</p> <p>RFC 2741 Agent Extensibility Protocol</p> <p>RFC 2787 Definitions of Managed Objects for VRRP</p> <p>RFC 2819 RMON MIB (groups 1,2,3 and 9)</p> <p>RFC 2863 Interfaces Group MIB</p> <p>RFC 3164 Syslog Protocol</p> <p>RFC 3176 sFlow: A Method for Monitoring Traffic in Switched and Routed Networks</p> <p>RFC 3411 An Architecture for Describing SNMP Management Frameworks</p> <p>RFC 3412 Message Processing and Dispatching for the SNMP</p> <p>RFC 3413 SNMP Applications</p> <p>RFC 3414 User-based Security Model (USM) for SNMPv3</p> <p>RFC 3415 View-based Access Control Model (VACM) for SNMP</p> <p>RFC 3416 Version 2 of the Protocol Operations for the SNMP</p> <p>RFC 3417 Transport Mappings for the SNMP</p> <p>RFC 3418 MIB for SNMP</p> <p>RFC 3635 Definitions of Managed Objects for the Ethernetlike Interface Types</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	<p>RFC 3636 IEEE 802.3 MAU MIB</p> <p>RFC 4188 Definitions of Managed Objects for Bridges</p> <p>RFC 4318 Definitions of Managed Objects for Bridges with RSTP</p> <p>RFC 4560 Definitions of Managed Objects for Remote Ping Traceroute, and Lookup Operations</p> <p>RFC 6527 Definitions of Managed Objects for VRRPv3</p>
Soporte de Multicast	<p>IGMP Query Solicitation</p> <p>IGMP Snooping</p> <p>IGMP/MLD Multicast Forwarding (IGMP/MLD Proxy)</p> <p>MLD Snooping (v1 & v2)</p> <p>RFC 2236 Internet Group Management Protocol v2 (IGMPv2)</p> <p>RFC 3376 IGMPv3</p>
Quality of Service	<p>IEEE 802.1p Priority Tagging</p> <p>RFC 2211 Specification of the Controlled-Load Network Element Service</p> <p>RFC 2474 DiffServ Precedence for 8 queues/port</p> <p>RFC 2475 DiffServ Architecture</p> <p>RFC 2597 DiffServ Assured Forwarding (AF)</p> <p>RFC 2697 A Single-Rate Three-Color Marker</p> <p>RFC 2698 A Two-Rate Three-Color Marker</p> <p>RFC 3246 DiffServ Expedited Forwarding (EF)</p>
Seguridad	<p>SSH remote login</p> <p>SSLv2 and SSLv3</p> <p>TACACS+ Accounting, Authentication, Authorization (AAA)</p>



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	<p>IEEE 802.1X authentication protocols (TLS, TTLS, PEAP and MD5)</p> <p>IEEE 802.1X multi-suplicant authentication</p> <p>IEEE 802.1X port-based network access control</p> <p>RFC 2560 X.509 Online Certificate Status Protocol (OCSP)</p> <p>RFC 2818 HTTP over TLS (“HTTPS”)</p> <p>RFC 2865 RADIUS authentication</p> <p>RFC 2866 RADIUS accounting</p> <p>RFC 2868 RADIUS attributes for tunnel protocol support</p> <p>RFC 2986 PKCS #10: certification request syntax specification v1.7</p> <p>RFC 3546 Transport Layer Security (TLS) extensions</p> <p>RFC 3579 RADIUS support for Extensible Authentication Protocol (EAP)</p> <p>RFC 3580 IEEE 802.1x RADIUS usage guidelines</p> <p>RFC 3748 PPP Extensible Authentication Protocol (EAP)</p> <p>RFC 4251 Secure Shell (SSHv2) protocol architecture</p> <p>RFC 4252 Secure Shell (SSHv2) authentication protocol</p> <p>RFC 4253 Secure Shell (SSHv2) transport layer protocol</p> <p>RFC 4254 Secure Shell (SSHv2) connection protocol</p> <p>RFC 5246 Transport Layer Security (TLS) v1.2</p> <p>RFC 5280 X.509 certificate and Certificate Revocation List (CRL) profile</p> <p>RFC 5425 Transport Layer Security (TLS) transport mapping for Syslog</p> <p>RFC 5656 Elliptic curve algorithm integration for SSH</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

	<p>RFC 6125 Domain-based application service identity within PKI using X.509 certificates with TLS</p> <p>RFC 6614 Transport Layer Security (TLS) encryption for RADIUS</p> <p>RFC 6668 SHA-2 data integrity verification for SSH</p>
Servicios	<p>RFC 854 Telnet protocol specification</p> <p>RFC 855 Telnet Option Specifications</p> <p>RFC 857 Telnet Echo Option</p> <p>RFC 858 Telnet Suppress Go Ahead Option</p> <p>RFC 1091 Telnet terminal-type option</p> <p>RFC 1350 Trivial File Transfer Protocol (TFTP)</p> <p>RFC 1985 SMTP Service Extension</p> <p>RFC 2049 MIME</p> <p>RFC 2131 DHCPv4 (Server, Relay and Client)</p> <p>RFC 2132 DHCP Options and BOOTP Vendor Extensions.</p> <p>RFC 2554 SMTP Service Extension for Authentication</p> <p>RFC 2616 Hypertext Transfer Protocol - HTTP/1.1</p> <p>RFC 2821 Simple Mail Transfer Protocol (SMTP)</p> <p>RFC 2822 Internet Message Format</p> <p>RFC 3046 DHCP Relay Agent Information Option (DHCP Option 82)</p> <p>RFC 3315 DHCPv6 (Server, Relay and Client)</p> <p>RFC 3633 IPv6 Prefix Options for DHCPv6</p> <p>RFC 3646 DNS Configuration options for DHCPv6</p> <p>RFC 3993 Subscriber-ID Suboption for DHCP Relay Agent Option</p>



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

	RFC 4330 Simple Network Time Protocol (SNTP) version 4 RFC 5905 Network Time Protocol (NTP) version 4
Interfaz de Usuario	Event-based Triggers Graphical User Interface (GUI) Industry-standard CLI with built-in Help Powerful CLI scripting tool
VLAN	Private VLANs IEEE 802.1ad Provider Bridges (VLAN stacking, Q-in-Q) IEEE 802.1Q Virtual LANs IEEE 802.1v VLAN classification by protocol & port IEEE 802.3ac VLAN tagging
VoIP	LLDP-MED ANSI/TIA-1057 Voice VLAN

ADICIONALES SISTEMA DE RED SWITCHES

- Bandeja ventilada de 19" 1 U de rack con material en acero laminado en frío SPCC, debe cumplir con certificaciones ISO 9001:2008.
- Kit de ventilación para gabinete de red de dos ventiladores.
- SFP+ 10G Direct Attach Cable, Twinax, 1 Meter, SFF-8431 MSA compliant, temperatura de funcionamiento 0 a 70 grados centígrados.
- QSFP+/SC SR4, Multi-Mode (150m), Compliant con 40Gbe especificación IEEE802.3ba, estándar industria SFF-8436, cumple RoHS (SR4), RoHS-6 (LR4), temperatura funcionamiento 0 a 70 grados centígrados.
- TAA, SFP+/LC 10G Multi-Mode 300m, 850nm, SFP+Electrical MSA SFF-8431, SFF-8472 MSA, Temperatura funcionamiento 0 a 70 grados centígrados.
- QSFP+ 40G Direct Attach Cable, Twinax, 3 Meter, Compliant con 40Gbe especificación 802.3ba MSA, SFF-8431 y SFF-8436, temperatura funcionamiento 0 a 70 grados.



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

- QSFP+ 40G Direct Attach Cable, Twinax, 1 Meter, compliant con 40GbE especificación IEEE802.3ba MSA, SFF-8431 y SFF-8436, temperatura funcionamiento) a 70 grados centígrados.



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

VIDEO WALL

Tecnología de Visualización	Tamaño Pantallas	• 55"
	Resolución Nativa	• 1920x1080
	LED	• Direct-lit LED
	Orientación Display	• 50,000 hrs (50% brillo)
	Pixel	• Portrait and landscape
	Brillo	• 500 nits (cd/m2) típico
	Relación de Contraste	• 4000:1
	Angulo de Visión (CR10:1)	• 178° h/v
	Frecuencia de refresh	• 50/60Hz
	Tiempo Respuesta	• 8 ms
	Espacio Color (CIE 1931)	• 72%
Colores	• 16.7 millón, 8 bit	
Señal	Inputs	• DisplayPort (Ver 1.2, HDCP) • 2 x HDMI (Ver 1.4, HDCP) • DVI-D (HDCP) • VGA
	Outputs	• Puertos Display (daisy chains DisplayPort, HDMI, and DVI inputs hasta 16 panels desde una sola fuente). Procesamiento integrado permita escalonamiento a video walls hasta de 10x10
Control	Inputs	• RS-232 vía D-Sub9 • Ethernet vía RJ45 • RS485 vía RJ45 • Teclado • IR window • IR wire extender
	Outputs	• RJ-45 for control looping
Power	Input rating Consumo energético	• 100-240 VAC @ 50/60Hz • 195W typical • 220W maximum • <= 0.5W standby
Ambiente	Temperatura de operación	• 32-104°F (0-40°C)
	Operación Humedad	• 20-90% RH sin condensación
	Temperatura almacenamiento	• -4-140°F (-20-60°C)



Departamento de Compras y Contrataciones
“Año de la Innovación y la Competitividad”

Físico	Panel solamente (sin manijas)	• Dimensions (WxHxD) 47.8 x 26.9 x 3.6" (1215 x 684.3 x 92.6mm).
	Puntos de montura	• VESA standard (WxH) 400 x 400mm, M8
Runtime	• Diseñado para operación 24/7, con Sistema de energía confiable y sistema de enfriamiento	
Características	• LCD Nivel Comercial con LED backlight • Tamaño standard OPS	
	• Built-in processing supports video walls up to 10x10	
	• Transporte Multi-Stream soportado hasta 4 paneles (UHD at 60 fps)	
	Garantía : 36 Meses	



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

VMS

SISTEMA VMS

GENERAL

El sistema deberá ser de arquitectura abierta, soportando integración con aplicaciones de terceros. Por arquitectura abierta también se entiende que el sistema no debe condicionar a la institución al uso de algún tipo de hardware específico y/o propietario para la ejecución de alguna función, como por ejemplo servidores, NVRs, almacenamiento o cámaras de marcas específicas. Esta ausencia de restricción de tipo de hardware a usar se debe verificar para el funcionamiento del sistema como un todo, o en cualquiera de sus módulos, como por ejemplo módulos de analíticas de video, de integración con terceros, etc. Tampoco se aceptarán ofertas de sistemas que condicionen el soporte al tipo de hardware actual o futuro a usar, a consideraciones comerciales o políticas propias del fabricante y ajenas a la institución.

Suministro, instalación y configuración de una solución de software de nivel enterprise, escalable y modular.

El sistema debe permitir un ilimitado número de sitios y cámaras para visualizarse como un único sitio al usuario final.

Debe ser capaz de integrar las cámaras IP actualmente existentes al menos a nivel de estándar abierto ONVIF, en el entendido que las cámaras IP existentes soporten ese estándar.

Tener la capacidad de integrar y configurar un ilimitado número de servidores de video unificados en una red, estaciones de trabajo, cámaras y cuentas de usuarios desde una única interface de usuario (GUI)– cada servidor debe ser capaz de comunicarse con otros servidores; el video y los eventos deben ser visibles desde otros servidores.

Soportar bases de datos PostgreSQL o similar. El objeto de este requerimiento es evitar que la solución propuesta condicione a la institución al pago de licenciamiento adicional de cualquier tipo por efecto de bases de datos. Esta condición aplica también para las futuras expansiones del sistema.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

Tener la capacidad de grabar y visualizar directamente cámaras análogas (incorporando encoders) e IP.

Las licencias del sistema no deben estar atadas a la dirección MAC de las cámaras IP, para que en caso que haya que hacer algún cambio de cámaras por efecto de mantenimiento de las mismas o por cualquier otra razón, la institución no tenga que incurrir en costos adicionales de licenciamiento.

El sistema deberá permitir una arquitectura de base de datos distribuida. Cada servidor/NVR y estación de administración deben poder almacenar una copia activa, y actualizable en tiempo real, de la configuración total de todo el sistema, pudiendo incluso recuperar toda la configuración si al menos 1 máquina sobrevive a un siniestro.

Tener la capacidad de activar/desactivar los módulos de analíticos propios en cualquiera de las cámaras IP del sistema, presentando un pool de licencias de módulos de analíticas que puedan activarse en cualquier momento en cualquier cámara IP en función de la necesidad de la operación diaria.

Proporcionar una solución tipo “Fail Over” en los servidores de video, permitiendo que en caso de falla en la operación de un servidor, de manera automática, el servidor de FailOver tome toda la configuración del servidor en falla en cuanto a cámaras, grabación, logs de eventos, base de datos, y posterior a la recuperación no sea necesario buscar video en otra ubicación de discos.

Proporcionar la opción de módulos propios para video analítica y no solamente dar la opción de módulos de analíticos de 3eras empresas. Sin embargo, debe ser capaz de integrar analíticas de video de terceros, de forma de no condicionar a la institución a un solo proveedor de analíticas de video. Este requerimiento tiene que ver con minimizar la probabilidad de detenciones de servicio del sistema o mal funcionamiento del mismo derivado de incompatibilidad de versiones entre los fabricantes del sistema y de los fabricantes de los módulos de video analíticos.

El sistema debe incluir la opción de agregar un paquete de analíticas situacionales (cruce de línea, merodeo, detección de multitudes, detección de movimiento, conteo de objetos) que puedan ser activadas en cualquier cámara en función de las necesidades del contexto en el que se aplicarían las analíticas.



Departamento de Compras y Contrataciones

“Año de la Innovación y la Competitividad”

CONFIGURACIÓN DEL SISTEMA

- El sistema no debe requerir un servidor dedicado principal y este rol puede ser tomado por cualquier servidor de video o estación de administración; además debe permitir realizar cambios en la configuración desde cualquier Servidor de Video o Estación de Administración.
- Debe brindar la posibilidad de incorporar estaciones de Administrador y/o Operador en forma ilimitada, sin que esto signifique un costo adicional para la institución en términos de licenciamiento del sistema. Esto aplica para cualquier futura ampliación de estaciones de trabajo.
- Deberá tener la capacidad de configurar individualmente cada objeto en el sistema (capturadoras de video, cámaras, sensores, relays, escritorios, monitores, etc...).
- Los servidores deben tener la habilidad de trabajar junto con servidores de diferentes sitios y estos múltiples sitios deben mostrarse al usuario como un único sitio. Los usuarios tienen la capacidad de cambiar entre los distintos sitios sin tener que cambiar la dirección IP, configuración o repetir el inicio de sesión.
- Debe proporcionar una herramienta de detección automática de cámaras en la red, para poder ser agregadas al sistema directamente.
- Permitir realizar un backup (respaldo) de toda la configuración del sistema en un único archivo (XML o SQL).
- El sistema deberá proporcionar una herramienta para extraer logs, bases de datos y demás información necesaria en caso de soporte sin necesidad de apagar la aplicación.
- El sistema debe proporcionar una herramienta de failover interna para efectos de redundancia del sistema, sin necesidad de incorporar herramientas de virtualización de terceros. La herramienta de failover debe soportar el traslado automático o manual de los servicios en operación desde un servidor físico a otro de respaldo de las mismas características presente en la red, con un tiempo de conmutación de los servicios de menos de un minuto, de modo que la grabación de las cámaras asignadas a este servidor



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

se interrumpa el menor tiempo posible. El sistema debe también proporcionar una herramienta de fallback, para que los servicios trasladados se vuelvan a asignar al servidor original que presentó una falla o mantenimiento programado, cuando este se vuelva a colocar en servicio en la misma red.

CARACTERÍSTICAS DEL SISTEMA

SOPORTE GENERAL

- El sistema deberá soportar los principales formatos de compresión: Wavelet, MJPEG, MPEG4, H.264, H265 y MxPEG.
- El sistema deberá soportar cámaras que son compatible con ONVIF, y deberá soportar el protocolo RTSP para recibir flujos de video desde cámaras que soporten el protocolo RTSP y deberá soportar drivers de HTTP para obtener video desde cualquier dispositivo que soporte protocolo HTTP.
- Deberá soportar la mayoría de los fabricantes de cámaras IP reconocidos mundialmente.
- Debe incorporar funcionalidades de monitoreo de la salud de las cámaras y servidores conectados a mismo, de forma que se emitan en tiempo real y de forma gráfica, las alarmas de desconexión o mal funcionamiento de las cámaras y/o servidores.
- Debe proveer un servidor de video RTSP y ONVIF, que pueda proveer flujos de video en vivo y grabados a sistemas de terceros externos, tales como VMSs o CADs externos. El servidor de video RTSP y ONVIF debe tener la capacidad de proveer a los sistemas externos la capacidad de visualizar y mover (PTZ) las cámaras administradas por el sistema. Esta capacidad se solicita para efectos de no condicionar en un futuro a la institución a una única plataforma de video para eventuales ampliaciones del sistema a otros edificios y/o instalaciones.
- Incorporar la capacidad de emitir alarmas en protocolo SNMP (MIB Traps) para efectos de conexión a sistemas de monitoreo centralizados basados en este protocolo.
- Incorporar funcionalidades de monitoreo de la salud de las cámaras y servidores conectados a mismo, de forma que se emitan en tiempo real y de



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

forma gráfica, las alarmas de desconexión o mal funcionamiento de las cámaras y/o servidores.

- El sistema debe proveer conexiones seguras a las cámaras IP mediante protocolo https. La misma conexión segura debe operar cuando el sistema recupera información de las tarjetas SD de las cámaras (edge storage).

GRABACIÓN DE VIDEO

- El sistema debe tener la capacidad de configurar grabación continua, por movimiento, por calendario o por evento.
- Cada resolución de cámara, cuadros por segundo, anchos de banda deben ser configurados independientemente en cada cámara y estos cambios no afectarán la grabación y configuración de visualización de las otras cámaras.
- El sistema deberá soportar múltiples modelos y marcas de cámaras / dispositivos IP.
- Deberá soportar flujos de video directamente desde cámaras IP y cámaras análogas conectadas a encoders IP.
- Capacidad de proteger con una clave la grabación de cada cámara.
- El sistema deberá tener la capacidad de grabar de al menos 1Gbps de video por servidor, basados en las capacidades del procesador del servidor.
- Capacidad de grabar a un frame rate distinto del cual es transmitido.
- El sistema deberá tener un botón en la visualización de la cámara para fácilmente iniciar/detener la grabación de alguna cámara en particular.
- El sistema deberá poder grabar con un frame rate cuando no hay movimiento y otro distinto cuando hay movimiento para optimizar espacio en disco.
- Tener la opción de configurar la cantidad mínima y máxima de días de retención de video por cámara.
- Capacidad de grabaciones por pre y post alarma a full frame rate.
- El sistema deberá tener la capacidad de mantener espacio suficiente en disco para la operación de video, sin que tenga que haber intervención humana para liberar espacio.
- Capacidad de desplegar un video pregrabado como si fuese una cámara del sistema (El video deberá estar en formato nativo y AVI).



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- El sistema deberá tener la capacidad de almacenamiento a largo plazo en medios distintos a los conectados directo a los servidores.
- El sistema deberá poder grabar con una reducción de cuadros por segundo referente a los enviados por la cámara. Esta funcionalidad debe ser programable por software, de modo que se pueda configurar una grabación con cierta resolución en un periodo de tiempo inicial, y una grabación con una resolución menor en un periodo de tiempo adicional. Esta grabación debe poder realizarse en sistemas de respaldo distintos al medio de respaldo original. El objetivo de esta funcionalidad es que se pueda mantener grabaciones por un periodo mayor de tiempo, sin incurrir en costos elevados por este concepto.
- El sistema deberá tener la capacidad de exportar el video en formato nativo y proveer una aplicación para visualización remota.
- El sistema debe permitir el uso de hardware de almacenamiento no propietario permitiendo futuros upgrades de capacidad de grabación.

DESPLIEGUE DE VIDEO

- El sistema debe ser capaz de usar en las estaciones de trabajo equipos de cómputo estándar de bajo costo que usen procesadores Intel i3, i5 y/o i7 como máximo, sin necesidad de incorporar equipamiento de alto costo como por ejemplo equipamiento con procesadores Intel Xeon.
- Deberá proporcionar la habilidad de visualizar imágenes de cámaras localmente en el servidor de video, estación de administración, estación de operador y por Web Browser.
- El sistema no deberá presentar retardos entre los flujos de video que se vean en una Estación de Trabajo de Operador o Administrador y los que se vean en el Video Wall.
- El sistema deberá permitir la adición de texto sobre el video como marca de agua, desde cualquier procedencia del sistema interno o sistemas o aplicaciones externas y no limitándose a horas, fechas y nombres de cámaras. El sistema deberá tener la suficiente flexibilidad para la adición de texto sobre el video desde cualquier aplicación existente o futura,

Departamento de Compras y Contrataciones

“Año de la Innovación y la Competitividad”

asumiendo que el proveedor/desarrollador de las aplicaciones no restrinja la entrega del texto al sistema.

REPRODUCCIÓN / BÚSQUEDA DE ARCHIVOS DE VIDEO

- El sistema deberá tener la capacidad de proporcionar una línea de tiempo de alarma de eventos en todos sus canales. La línea de tiempo deberá soportar reproducción de al menos 32 cámaras en simultáneo sin afectar el desempeño del sistema y debe poder diferenciar claramente de las grabaciones por detección de movimiento, y las que no son por detección de movimiento.
- Proporcionar la habilidad de reproducir / revisar videos grabados en un Video Server localmente o desde estaciones de trabajo y un Web-Browser.
- El sistema deberá proporcionar un calendario para la búsqueda fácil de videos grabados.
- Tener la capacidad de enmascarar áreas no esenciales de video y realizar solo búsquedas en áreas de interés (“búsquedas inteligentes”).

EXPORTACIÓN DE VIDEO

- El sistema deberá proporcionar la opción de proteger con clave los archivos exportados por seguridad.
- El sistema deberá tener la capacidad de exportar varios videos a la vez desde diferentes cámaras.
- El sistema deberá tener la opción de exportar video y audio sincronizado en un mismo archivo.

AUDIO

El sistema deberá soportar grabaciones de audio desde dispositivos IP que tenga esta capacidad, no estando restringido al audio de las cámaras solamente.

El sistema deberá soportar audio en vivo desde cada uno de los dispositivos IP de audio por individual.

El sistema deberá soportar grabaciones sincronizadas entre audio de cámaras o de micrófonos independientes de las cámaras y video.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

El sistema deberá soportar reproducción de audio y video sincronizados, desde la misma interfaz gráfica de visualización de video.

DETECCIÓN DE MOVIMIENTO / ZONAS DE MOVIMIENTO

- El sistema deberá tener la capacidad de soportar múltiples zonas de movimiento en cada cámara.
- El sistema deberá incorporar la capacidad de detección de movimiento en todas las cámaras administradas por el mismo, para efectos de optimización del almacenamiento necesario para la grabación de las cámaras. Esta funcionalidad debe estar incluida en el costo de adquisición del sistema, independiente de las cámaras que se conecten en un futuro al mismo.
- Cada zona deberá tener la posibilidad de configurar individualmente para la detección de movimiento la tasa de cuadros de video, calidad del video y cuadros en memoria.
- Cada zona deberá ser direccionable de manera única y tener la posibilidad de configurar reacciones personalizadas a cada una, basadas en la alarma generada.
- Cada zona deberá tener la opción de ser armada o desarmada individualmente
- Cada zona deberá tener la opción de poner en ella una máscara de privacidad.
- El sistema deberá desplegar la zona de movimiento en un color diferente cuando el movimiento es detectado.

SOPORTE DE VIDEOWALL

El sistema deberá soportar una solución de videowall nativa del mismo fabricante, así como contar con capacidades de integración con videowall de terceros.

CARACTERÍSTICAS DE INTEGRACIÓN CON SISTEMAS /MÓDULOS DE TERCEROS.

El sistema deberá tener la capacidad de soportar dispositivos externos de alarmas, sensores y relés a través de capacidades de I/O entradas y salidas.

El sistema deberá tener la capacidad de llamar aplicaciones externas desde la misma interface.

El sistema deberá tener la capacidad de enviar notificaciones de alarmas a clientes del sistema específicos.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

El sistema deberá tener la capacidad de notificaciones de alarma audibles.

El sistema deberá tener la capacidad de programación de Macros.

El sistema deberá tener la capacidad de construir scripts programables basados en lenguajes como C/C++, JavaScript o VBScript.

El sistema deberá proporcionar la opción de crear Zonas de tiempo con el propósito de agendar eventos/reacciones en el sistema.

El sistema deberá ser capaz de notificar al administrador si una cámara falla, la cámara es cegada, la cámara es desenfocada u ocurre un problema de conectividad contra el servidor. El porcentaje del área cegada o desenfocada que origine una alarma debe ser configurable con el objeto de evitar lo máximo posible las falsas alarmas. Esta funcionalidad debe estar disponible para todas las cámaras actuales y futuras, sin que esto represente un costo adicional para la institución.

FUNCIONES REMOTAS

El sistema deberá soportar administración remota a todas las funcionalidades y herramientas de administración, incluidos los analíticos propios del sistema o de terceros.

El sistema deberá proporcionar posibilidad de habilitar/deshabilitar remotamente o modificar derechos de acceso de cuentas de usuarios sin la necesidad de estar presente un operador en el sitio o empresa.

El sistema deberá proporcionar la posibilidad de habilitar/deshabilitar remotamente o modificar las configuraciones de cámara sin la necesidad de estar presente un operador en el sitio o empresa.

El sistema deberá soportar almacenamiento remoto en tiempo real

El sistema deberá proporcionar múltiples clientes remotos y administradores según sea necesario, sin que esto signifique un licenciamiento con costo adicional para la institución.

El sistema deberá tener la capacidad de utilización eficiente de ancho de banda usando TCP/IP.

El sistema deberá contar con una solución de centralización (Federación) de cámaras de distintos sitios en un sitio central. Esta solución debe soportar también la centralización del audio, de los mapas y de analíticos de video de los sitios remotos.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

La solución de centralización debe incorporar facilidades de optimización de ancho de banda para evitar que varios operadores accedando a cámaras remotas saturen el ancho de banda disponible entre el sitio central y los sitios remotos, restringiendo a solamente un flujo de video por cámara remota, independiente de la cantidad de operadores y/o administradores que quieran visualizar/grabar la misma cámara de un sitio remoto.

El sistema deberá soportar control remoto de alarmas de servidores y administrar dispositivos de I/O.

El sistema deberá contar con una aplicación de visualización de cámaras instalable en dispositivos móviles como Smartphones o Tabletas.

INFRAESTRUCTURA

El sistema deberá correr sobre Sistemas Operativos de Windows, pero debe tener la opción de una versión de VMS que corra sobre Linux, en caso que la institución opte por esta alternativa por un tema de seguridad o de economía.

El sistema deberá tener la opción de funcionar como un servicio de Windows.

El sistema deberá soportar herramientas básicas de diagnóstico de Windows.

El sistema deberá restablecerse cuando la conexión de red es perdida sin la necesidad de un operador.

El sistema deberá soportar ambientes virtualizados.

El sistema debe tener la capacidad de soportar throughputs de 1.3Gbps por servidor, con el objeto de minimizar el uso de recursos de cómputo de la institución.

SOFTWARE DEVELOPMENT KIT (SDK)

El sistema deberá proporcionar un kit de integración de desarrollo.

El sistema deberá proporcionar APIs de integración con aplicaciones de terceros pudiendo enviar mensajes al sistema y recibir mensajes desde el sistema.

El sistema deberá proporcionar un kit de desarrollo para integración con video.

- Para controlar sistemas de Cámaras/Video desde aplicaciones de terceros.
- Pueden ser utilizados con C++, Visual Basic, C#, y lenguajes similares.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

CAPTURADOR FACIAL Y MÓDULO DE RECONOCIMIENTO FACIAL

GENERAL

- El sistema deberá detectar simultáneamente y capturar múltiples rostros por segundo.
- El sistema debe ser capaz de enrolar rostros en la base de datos en tiempo real desde el video de la cámara, o a través de fotos digitales, con una resolución mínima de 80 píxeles de distancia interpupilar.
- El sistema debe ser capaz de detectar, capturar y reconocer los rostros de las personas en tiempo real y de manera forense en videos pregrabados.
- La solución debe ser basada únicamente en software, y correr sobre cámaras comercialmente disponibles. No se aceptarán soluciones que condicionen a la institución a usar hardware propietario.
- Las licencias de la solución deben ser activables/desactivables en cualquier cámara IP conectada al VMS, sin necesidad de incorporar hardware propietario para ese efecto.
- El sistema debe ser capaz de detectar y capturar simultáneamente múltiples caras desde la misma vista de cámara (suponiendo que la resolución de la cámara y los requisitos de los píxeles de cara se cumplan).
- El sistema seleccionará automáticamente el marco de vídeo optimizado para la localización del rostro.
- El sistema debe registrar y archivar en la base de datos de facial al menos los siguientes datos: imagen, fecha, hora y cámara de captura.
- Proporcionará capacidad para ajustar parámetros y umbrales de reconocimiento.
- El sistema deberá tener la capacidad de hacer clic en la cara de una persona desde la interfaz gráfica de usuario y mostrar el vídeo asociado con la imagen facial capturada.
- El sistema debe poder registrar un evento / alarma si así se ha programado para una persona reconocida.
- Ignorar las tasas de reconocimiento de índice de baja exactitud.
- El sistema deberá poder mostrar en la GUI la tasa de reconocimiento (%) y el nombre de cada persona reconocida.
- Tener la capacidad de bloquear el acceso por el operador humano.
- Localizar y capturar caras desde múltiples canales de vídeo en tiempo real.
- El sistema tendrá la capacidad de ser administrado remotamente y estar completamente integrado en la solución de centralización (Arquitectura Federada) del VMS.
- El sistema deberá tener un nivel de precisión del 90% o superior (si se han seguido las directrices para la correcta configuración de la cámara / software).



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Proporcionará un índice de calidad de las caras reconocidas.
- Crear perfiles de varias personas en la base de datos de reconocimiento.
 1. Cada perfil de persona permitirá múltiples imágenes de esa persona.
 2. Cada perfil de persona debe tener al menos un nombre y apellido o alias.
 3. Cada perfil de persona debe tener un campo Identificador del Sistema de Control de Acceso.
 4. Cada perfil de persona tendrá un campo de Comentarios opcional.
 5. Cada perfil de persona tendrá una opción que se agregará a una "lista negra".
- Ser capaz de reconocer a una persona con el vello facial, incluso si su foto registrada no tiene vello facial.
- Debe reconocer individuos usando sombreros o gorros siempre y cuando el sombrero o gorro no sea un obstáculo para visualizar los ojos del individuo.
- El sistema debe poder reconocer a una persona que usa gafas graduadas, incluso si en su foto registrada no están usando gafas (suponiendo que sus gafas no crean un reflejo y son claras).
- El sistema debe ser capaz de alarmar y / o realizar reacciones complejas en sistemas propios o de terceros, basadas en caras reconocidas.
- El sistema deberá contar con un módulo de reporte que pueda presentar la información de las bases de datos del sistema en forma de tableros y gráficos personalizables hacia el usuario final. El módulo debe ser provisto por el mismo fabricante del analítico de reconocimiento facial, y deberá estar integrado al sistema del VMS para la eventualidad que tenga que desplegar el video de cámaras conectadas al VMS y relacionado con los datos del reconocimiento facial recolectados en bases de datos.

BÚSQUEDA

- El sistema tendrá la capacidad de buscar a una persona basada en la cámara por la que pudo haber pasado.
- El sistema tendrá la capacidad de buscar a una persona en base al nombre o apellido de la persona.
- El sistema tendrá la capacidad de buscar a una persona en función de la hora y fecha.
- El sistema deberá tener la capacidad de buscar a una persona en base a una imagen tomada previamente de la persona.
- Todos los resultados de búsqueda deberán ser asociados a una foto de la persona y con opción de reproducir la secuencia de video en el que la persona pasó. El sistema deberá permitir proporcionar una fotografía y validar si dicha persona pasó por alguna cámara con reconocimiento facial en un periodo seleccionable de días y horas. La persona podría estar



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

o no en la base de datos.

INTEGRACIÓN

- El sistema deberá estar completamente integrado al VMS. El fabricante deberá entregar una carta en la que garantice que no habrá problemas de compatibilidad con el VMS en caso de cambios y/o upgrades de versión del módulo facial y/o del VMS, durante todo el período de garantía.
- El sistema tendrá la capacidad de integrar e intercambiar datos en tiempo real con bases de datos externas.
- El sistema deberá tener la capacidad de integrarse con otros dispositivos, tales como control de puertas usando contactos secos y cualquier control de acceso o sistemas de tarjetas.
- El sistema proporcionará el SDK de la plataforma que permitirá a los sistemas de terceros recibir todos los eventos del sistema de reconocimiento facial.
- El sistema deberá tener la capacidad de importar imágenes de caras en la base de datos del sistema, siempre y cuando las imágenes faciales cumplan con los requisitos mínimos de importación. Las imágenes de caras podrán importarse una por una o en un lote.

MÓDULO AUTOMÁTICO DE RECONOCIMIENTO DE PLACAS.

GENERAL

- Suministro, instalación y configuración de la solución debe estar basada únicamente en software y deberá ser compatible con cámaras IP comercialmente disponibles, desde que cumplan con las características mínimas necesarias para proporcionar una imagen en color en el que la placa se distinga claramente, sin distorsión ni borrosa. No se aceptarán soluciones basadas en hardware propietario que condicionen a la institución a un proveedor de hardware en particular.
- La solución debe contar con una opción de licenciamiento para dispositivos móviles, para que el reconocimiento de placas se pueda hacer en terreno por personal de seguridad del recinto. La solución debe poder conectarse a bases de dato de terceros para poder arrojar alarmas cuando se cruce la



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

información de la placa leída remotamente con las plazas registradas en las bases de datos de terceros.

- El sistema debe tener la capacidad de activar/desactivar los módulos de reconocimiento de placas en cualquiera de las cámaras del sistema VMS, presentando un pool de licencias de módulos de reconocimiento de placas que puedan activarse en cualquier momento en cualquier cámara en función de la necesidad de la operación diaria.
- Operar desatendidamente 24 horas al día, siete días a la semana.
- Permitir sincronizar el flujo de video del reconocimiento de placas con los flujos de video de un grupo ilimitado de cámaras.
- El sistema deberá automáticamente determinar el mejor cuadro de imagen desde el flujo de video.
- El sistema deberá simultáneamente detectar, capturar y comparar múltiples placas de vehículos en tiempo real y de manera forense en videos pregrabados.
- Proporcionar compensación contra distorsión y posición incorrecta de la placa patente capturada al vehículo.
- El sistema deberá detectar vehículos aproximándose o alejándose.
- El sistema deberá ser capaz de capturar múltiples líneas de tráfico (si la cámara/resolución usadas lo permiten).
- El sistema deberá ofrecer al menos 3 modos para almacenar la imagen de captura de placas en la base de datos: Fotografía completa de la escena, Fotografía del vehículo y su placa o sólo la imagen de la placa.
- El sistema deberá ser capaz de usar una base de datos central (o múltiples) en locaciones distintas o paralelas. Incluso con bajos anchos de banda comparar las placas capturadas en tiempo real con esta base de datos. Cuando se usen bases de datos distribuidas, el sistema debe tener la capacidad de replicar las bases de datos remotas en una base de datos central, de modo de que la información de las bases de datos remotas pueda estar respaldada en una base de datos central en el evento que se verifiquen fallas en la disponibilidad de las bases de datos remotas.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- Registrar y guardar en una base de datos la imagen, fecha, hora, placa patente, país/estado de la placa y la dirección del vehículo (relativo a la cámara).
- El sistema deberá ser capaz de reconocer placas patentes a no menos que 209km/h.
- El sistema deberá tener una precisión superior al 90% en reconocimiento de placas, medida sobre todo el universo de las placas legibles.
- El sistema deberá proporcionar una calidad de índice de capturas de placas patentes.
- El sistema deberá ser capaz de determinar el país/estado de origen de la placa patente.
- El sistema deberá ser capaz de determinar múltiples países/estados de placas patentes y determinar el país /estado del origen de cada una de las placas patentes.
- El sistema deberá ser capaz de realizar un filtro automático en los resultados de reconocimiento y descartar reconocimientos de baja precisión – definidos por el administrador.
- El sistema deberá proporcionar la capacidad de ajustar parámetros y umbrales de reconocimiento.
- El sistema deberá ser capaz de registrar un evento/alarma cuando la placa es reconocida o la placa es perdida.
- El sistema deberá poder configurarse para transmitir solo texto, texto e imágenes y texto y video, al momento de detectar una placa en listas negras o blancas.
- El sistema deberá tener la capacidad de ser editado por un operador humano.
- El sistema deberá tener la capacidad de ser configurado para evitar la edición por un operador humano.
- El sistema deberá tener la capacidad de administrar y reconocer placas patentes en vehículos desde múltiples canales de video en tiempo real.
- El sistema deberá tener la capacidad de ser administrado remotamente y estar completamente integrado en la solución de centralización (Arquitectura Federada) del VMS.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- El sistema deberá ser accesible con un PC cliente estándar con procesadores de bajo costo Intel Core i3, i5 o i7 para visualización remota.
- El sistema deberá ser capaz de usar estadísticas internas para ajustar el algoritmo de reconocimiento para mejorar el rendimiento definido en la cámara.
- El sistema deberá soportar listas internas de registro de placas (listas blancas, negras, de información).
- El sistema deberá soportar automatización de reacciones del sistema en eventos de reconocimiento de placas encontradas en listas internas o Bases de Datos Externas.
- El sistema deberá soportar reproducción de sonidos al reconocer placas.
- El sistema deberá operar tanto con cámaras de Color como en Blanco y negro sin ninguna afectación en el desempeño del módulo.

BÚSQUEDAS.

- El sistema deberá ser capaz de usar entradas de tipo genérico durante la búsqueda para caracteres desconocidos.
- El sistema deberá ser capaz de realizar búsquedas por cualquier cadena de caracteres conocidos.
- El sistema deberá tener la capacidad de realizar múltiples métodos de búsqueda, para placas capturadas, fechas, y/o tiempo y asociar los resultados con imágenes/Videos.
- El sistema deberá ser capaz de realizar búsquedas por múltiples vehículos si se ajustan a los criterios de búsqueda.
- El sistema deberá ser capaz de alarmar y/o realizar eventos complejos en sistemas propios y de terceros, basados en placas con parámetros predeterminados.

INTEGRACIÓN

- El sistema debe tener mecanismos de scripts internos para programar comportamientos lógicos de diferentes niveles de dificultad.



Departamento de Compras y Contrataciones **“Año de la Innovación y la Competitividad”**

- El sistema debe tener la capacidad de integrarse con otros dispositivos, como controles de accesos, controles de puerta usando contactos secos, radares de velocidad, sistemas de tags o RFID, CADs, otros VMSs, etc.
- El sistema debe tener la capacidad de integrarse e intercambiar información en tiempo real con bases de datos externas.
- El sistema debe proporcionar conexión SDK para integrarse con sistemas de terceros.
- El sistema debe proporcionar una API para sistemas de terceros que quieran integrarse al mismo. La API deberá soportar el envío de eventos, imágenes individuales obtenidas del video y secuencias de video.