FUERZA AÉREA COLOMBIANA

JEFATURA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

DIRECCIÓN DE SEGURIDAD INFORMÁTICA Y ELECTRÓNICA

ANEXO TÉCNICO SISTEMAS ELECTRÓNICOS DE SEGURIDAD

RENOVACIÓN MEDIDAS ACTIVAS ELECTRONICAS DE SEGURIDAD CCOFA ALTERNO, DE ACUERDO CON ANEXO TÉCNICO

2024

CONTENIDO

ANEXO TÉCNICO 3
ESPECIFICACIONES TÉCNICAS JETIC SISTEMAS ELECTRÓNICOS DE SEGURIDAD 3
DESCRIPCIÓN DE ELEMENTOS Y/O SERVICIO 3
ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO 4
CONDICIONES GENERALES DE IMPLEMENTACIÓN 4
ISS SOR-CAM LICENCIA PARA CÁMARA VMS SECUROS 5
UBICACIÓN UNIDADES MILITARES FUERZA AEROESPACIAL COLOMBIANA 7
ESPECIFICACIONES TÉCNICAS RENOVACIÓN MEDIDAS ACTIVAS ELECTRÓNICAS DE SEGURIDAD CCOFA ALTERNO 7
AXIS M3115–LVE CAMARA DOMO DE 1080P ... **¡Error! Marcador no definido.**
HANWHA QNV-C8011R MINI DOMO CON IA IR DE 5MP .. **¡Error! Marcador no definido.**
LECTORA DE BLUETOOTH Y TARJETA NFC 10
CONTROLADOR DE ACCESO RBHUNC5825RM- RBHUNC5825RM- 4-KIT-PB * Y ACCESORIOS 15
AXIS P1465-LE CAMARA – LENTE 29 mm ..... **¡Error! Marcador no definido.**
HANWHA CAMARA DOMO ANTIVANDÁLICO DE 5MP ..... **¡Error! Marcador no definido.**
GENERALIDADES POSTERIORES A LAS FICHAS TECNICAS 28
CONDICIONES DE INSTALACIÓN CÁMARAS DE SEGURIDAD / VMS SECUROS 28
CONDICIONES DE INSTALACIÓN CÁMARAS EVITE PROCESOS DENEGADOS DE RMA 30
CONDICIONES DE INSTALACIÓN PERIFERICOS AXIOM XA 32
OBSERVACIONES SITE SURVEY 35
PRUEBAS DE ACEPTACIÓN, PROTOCOLOS Y PUESTA EN SERVICIO EQUIPOS 36
REQUERIMIENTOS PROPONENTES 36
GARANTIAS 36
MERCADO DE PARTES Y ACTUALIZACIONES 37
TRANSPORTE Y SEGUROS 37
ESTUDIOS DE SEGURIDAD 38
CONDICIONES PARA RECEPCIÓN DE HARDWARE Y SOFTWARE 39
CONDICIONES AMIENTALES 40

COMPROMISO DE CONFIDENCIALIDAD 40
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA FAC 40

ANEXO TÉCNICO

ESPECIFICACIONES TÉCNICAS JETIC SISTEMAS ELECTRÓNICOS DE SEGURIDAD

Debido a que los equipos, sus características y capacidades hacen parte de los Sistemas Electrónicos De Seguridad que se tiene estandarizado en la Fuerza Aérea Colombiana, los cuales apoyan la seguridad física de las Unidades, manteniendo una alerta temprana ante alguna novedad que se pueda presentar, el anexo técnico goza de reserva legal de conformidad a lo establecido en la ley 1712 de 2014, Decreto 1081 de 2015 y la Ley 2195 de 2022.

La ley 1712 de 2014 en su artículo 6 indica que *"d) Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley".*

Así mismo, el artículo 19. *"Información exceptuada por daño a los intereses públicos. Es toda aquella información pública reservada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional: a) La defensa y seguridad nacional; (…)"*

Por lo anterior, para conocer el contenido del anexo técnico el interesado deberá seguir lo descrito para tal fin en el anexo al pliego de condiciones.

OBJETO: "RENOVACIÓN MEDIDAS ACTIVAS ELECTRONICAS DE SEGURIDAD CCOFA ALTERNO, DE ACUERDO CON ANEXO TÉCNICO"

DESCRIPCIÓN DE ELEMENTOS Y/O SERVICIO
El contratista deberá suministrar, transportar, instalar, configurar y poner en servicio los siguientes elementos hardware y software (licencias) con el fin de realizar conectividad del conjunto de cámaras y equipos hasta agotar presupuesto, siendo la cantidad expresada en la tabla la máxima por adquirir.

ESPECIFICACIONES TÉCNICAS RENOVAVIÓN MEDIDAS ACTIVAS ELECTRONICAS DE SEGURIDAD.				
ÍTEMS	**ELEMENTOS DE HARDWARE Y SOFTWARE PARA CONECTIVIDAD**	**CANT**	**NO DE PARTE**	**UNIDAD DE MEDIDA**
01	SUMINISTRO E INSTALACIÓN CAMARA FIJA INTERNA	8	M3115 LVE O QNV-C8011R	UNIDAD
02	LECTOR DE CREDENCIALES	4	RBH – N86-DNB-D-O	UNIDAD
03	CONTROLADORA DE ACCESO	1	RBH-UNC5825RM-4-KIT-PB	UNIDAD
04	SUMINISTRO E INSTALACIÓN CAMARA FIJA EXTERNA	7	P1455 O QNV-C8083R	UNIDAD

ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO

CONDICIONES GENERALES DE IMPLEMENTACIÓN

El contratista debe garantizar y entregar las referencias descritas con sus respectivas especificaciones, para garantizar un único punto de soporte la infraestructura con la misma referencia o superior para mantener la uniformidad y homogeneidad en la plataforma tecnológica que la FAC tiene estandarizando en las UMAs, ya que es crecimiento de la infraestructura actual.

Adquisición y uso de la ductería prevista en la obra, para que garantice las conexiones requeridas de energía y datos, dejando todo funcionado correctamente, las conexiones deben llegar hasta los cuartos de equipos o gabinetes, donde se debe conectar tanto energía como datos de los equipos solicitados. Es de recalcar que deben tener compatibilidad 100% con el sistema electrónico de seguridad de la UMA VMS SecurOS estandarizado por JETIC.

Los equipos solicitados deben ser suministrados, instalados, puesta en servicio con todos los accesorios y fuentes de fábrica. Así mismo, es importante resaltar que la renovación de equipos para las instalaciones solicitadas en la Unidad del Comando Aéreo de Combate No 01 se debe contemplar el licenciamiento requerido para las cámaras de seguridad VMS.

Los equipos de acuerdo con su clasificación deben contar con garantía de fábrica y garantía por parte del contratista de la siguiente manera:

Equipos	Garantía fabrica y/o contratista
Cámaras de Seguridad y soportes	05 años
Dispositivos Bluetooth Control de Acceso	03 años
Controladoras de Control de Acceso	03 años

Suministro Instalación y Puesta en servicio del contratista	02 años

“El proponente debe contar con carta que lo habilite como un canal autorizado, certificado y con experiencia en la comercialización, instalación y mantenimiento de productos de VMS, integración y video analítica de la marca ISS SecurOS implementado en la entidad, y que además cuenta con el apoyo comercial y técnico de ISS para desarrollar y soportar este proyecto”.

“El proponente debe contar con carta que lo habilite como un canal autorizado, certificado y con experiencia en la comercialización, instalación y mantenimiento de productos de RBH, integración RBH AXIOM XA implementado en la entidad, y que además cuenta con el apoyo comercial y técnico de RBH para desarrollar y soportar este proyecto”.

“El Proponente debe estar certificado por casa fabricante en distribución, venta, instalación, mantenimiento y soporte técnico Nivel II (anexarla a la propuesta) en las plataformas estandarizadas por la FAC: ISS y RBH.

ISS SOR-CAM LICENCIA PARA CÁMARA VMS SECUROS	
	El contratista deberá suministrar, instalar, configurar y poner en servicio las siguientes licencias con el fin de realizar conectividad del conjunto de cámaras y equipos que se encuentran en el Servidor de SecurOS – ISS de las unidades de la Fuerza Aérea Colombiana. Es de recalcar que deben tener compatibilidad 100% con el sistema electrónico de seguridad de la UMA SecurOS Premium estandarizado por JETIC. **1.1** licencias - SOR-CAM que incluyen: SecurOS TM Premium - Camera license (per channel) cantidad Licencia para integrar y configura cámaras de seguridad en el VMS SecurOS de la unidad, lo cual permite visualizar en el CMOSD y su respectivo almacenamiento en la NSM. Licenciamiento ISS - VMS SecurOS Premium, deben soportar características tipo servidor que le permitan ejecutar procesos de analíticas de video, generar reportes, tener registro y alertas del estado de los equipos, integrarse con diferentes sistemas como control de acceso, intrusión, sistemas de información, analíticas de reconocimiento de placas, reconocimiento facial, bases de datos de terceros, placas y conjunto de detectores de analíticas situacional.

	El licenciamiento debe ser perpetuo para las funciones y características del sistema y con actualización sobre la plataforma y versión que se adquiera. El sistema no debe requerir de pagos anuales para su operación, y tanto los desarrollos como el licenciamiento necesario para el desarrollo del proyecto deben ser propiedad de la Fuerza Aeroespacial Colombiana. El licenciamiento debe operarse y soportar como mínimo los siguientes sistemas operativos de Windows: • Windows 8.1 • Windows 8.1 Pro • Windows 8.1 Enterprise • Windows 10 Home • Windows 10 Pro • Windows 10 Enterprise • Windows Server® 2012 R2 Foundation • Windows Server® 2012 R2 Essentials • Windows Server® 2012 R2 Standard • Windows Server® 2012 R2 Datacenter • Windows Server® 2016 Essentials • Windows Server® 2016 Standard • Windows Server® 2016 Datacenter • Windows Server® 2019 Essentials • Windows Server® 2019 Standard • Windows Server® 2019 Datacenter **Incluye** a) Módulo de mapas b) Canales de E / S ilimitados c) Conexiones web ilimitadas (SecurOS WebConnect) d) Conexiones ilimitadas de aplicaciones móviles (SecurOS Mobile) e) Conexiones ilimitadas de la estación de trabajo del operador (cliente de visualización o de administración) f) Soporte para todos los módulos de análisis de ISS (con licencia por separado) g) Soporte para todas las opciones ISS SDK / API (con licencia por separado) h) Subsistema de notificación i) Macros j) Motor de secuencias de comandos k) Archivado programado (con licencia por separado) l) Vigilancia de la salud m) Soporte de grabación de borde n) Soporte de zona horaria o) Gestión de derechos de usuario incorporada p) Soporte para Failover 1 to 1 y SecurOS Cluster (con licencia por separado) q) Integración con AD / LDAP (con licencia por separado)

	Funciones Generales a) Será una solución de licenciamiento de SecurOS Premium, altamente escalable y modular. b) Tendrá una arquitectura abierta, soportando integraciones similares con aplicaciones de terceros. c) Permite actualizar una versión a otra sin que el usuario tenga que desinstalar la versión previa. d) Tendrá la capacidad de grabar y visualizar cámaras análogas (a través de encoders IP) e IP de manera indistinta. e) El licenciamiento debe proporcionar acceso al VMS SECUROS del video en vivo y grabado y la capacidad realizar control PTZ sobre las cámaras a aplicaciones de terceros en cumplimiento con los estándares ONVIF Perfil G, Perfil S y perfil T, de tal forma que se pueda, por ejemplo, compartir esta información de ciertas cámaras con la fuerza pública. f) Idiomas soportados: Mínimo Español e ingles. g) El licenciamiento permite en el VMS SECUROS soportar todos los principales formatos de compresión de video: H.264, H.265, MJPEG, MPEG4, MxPEG. h) El licenciamiento permite en el VMS SECUROS soportar dispositivos IP que estén en concordancia con el Foro de Interfaz de Video en Red Abierta (ONVIF). i) El licenciamiento permite en el VMS SECUROS acceder al video de dispositivos IP que soporten el protocolo RTSP. j) El licenciamiento permite en el VMS SECUROS enviar streams de video en vivo y archivado a través del protocolo RTSP a los clientes que lo requieran. k) El licenciamiento permite en el VMS SECUROS grabar continuamente, en la detección de movimiento, según un horario o en un evento.

UBICACIÓN UNIDADES MILITARES FUERZA AEROESPACIAL COLOMBIANA
• CACOM-1 PUERTO SALGAR CUNDINAMARCA

ESPECIFICACIONES TÉCNICAS RENOVACIÓN MEDIDAS ACTIVAS ELECTRÓNICAS DE SEGURIDAD CCOFA ALTERNO

Para el presente proyecto de renovación e instalación de Cámaras de seguridad y control de acceso para el Comando Aéreo de Combate No 01, se debe contemplar la ducteria y cableado no superior a los 100 metros por cada equipo, los cuales deben quedar por encima del cielo raso existente o en su defecto muy bien presentado con una estética impecable, en caso de que se realice obra civil o algún

desmonte de láminas de techo debe quedar perfectamente instalada nuevamente, toda actividad realizada en las instalaciones para el cumplimiento de la misión deben ser supervisadas y autorizadas por el supervisor del contrato.

Se requiere el suministro instalación, licenciamiento y puesta en servicio en el software del VMS Centralizado SecurOS de la Unidad de CACOM1, el almacenamiento de video debe quedar configurado por movimiento y no grabación continua. Adicional, no es requerida la visualización por los operadores en el CMOSD.

Distribución de los equipos:

- SUMINISTRO E INSTALACIÓN CAMARA FIJA INTERNA M3115 LVE (04)
- LECTOR DE CREDENCIALES RBH – N86-DNB-D-O (04)
- CONTROLADORA DE ACCESO (01) RBH-UNC5825RM-4-KIT-PB
- SUMINISTRO E INSTALACIÓN CAMARA FIJA EXTERNA (04)
- Lectora De Bluetooth Y Tarjeta NFC (02) P1455

Con relación al control de acceso el contratista debe prever el cableado y ducteria de la instalación desde el cuarto de equipos hasta las puertas designadas para el control de acceso. Contemplar el suministro e instalación, puesta en servicio de los equipos relacionados previamente, la configuración se debe realizar por personal capacitado de la marca, puesto que se realizará la parametrización en el servidor central de la institución.

SUMINISTRO E INSTALACION CÁMARA FIJA INTERIOR QNV-C8011R	
	Caracteristicas principales • resolución de 5MP • Lente fija de 3,0 mm (H:100°/V: 73°) • 30 fps en todas las resoluciones (H.265/H.264) • Códec triple H.265/H.264/MJPEG con Wisestream III (basado en motor AI), WiseNRII (basado en motor AI), WDR 120dB • Día y noche (ICR), WDR (120 dB) • Detección de desenfoque, aparecer/desaparecer, manipulación, detección de movimiento basada en motor de IA, detección de objetos con IA - Tipo de objeto clasificado: persona/vehículo (tipo de vehículo: automóvil/autobús/camión/moto/bicicleta); Eventos de IVA basados en motor de IA: Línea virtual (Cruce/Dirección), Área virtual (Merodear/Intrusión/Entrar/Salir)

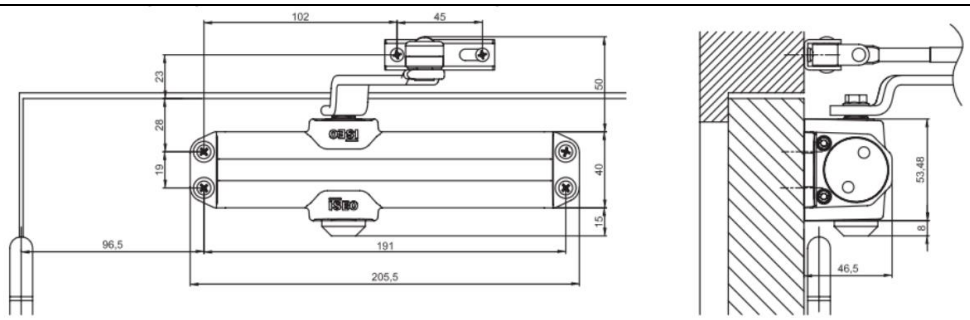
	• Conteo de personas, mapa de calor, gestión de colas y conteo de vehículos • Ranura de memoria micro SD (256 GB), PoE / 12 V CC • Longitud visible por infrarrojos 20 m (65 pies) • IP66, IK10 • Soporte para vista de pasillo • Compatibilidad con LDC (corrección de distorsión de lente) • USB para fácil instalación, plataforma abierta • Temperatura de funcionamiento -40°C~+55°C(-40°F ~ +131°F), color blanco
	Video • Dispositivo de imagen CMOS de 1/2,8" • Resolución 2592x1944, 2560x1440, 1920x1080, 1280x960, 1280x720, 800x600, 800x448, 720x576, 720x480, 640x480, 640x360, 320x240 • Máx. Cuadros por segundo H.265/H.264: Máx. 30 fps/25 fps (60 Hz/50 Hz) MJPEG: máx. 30 fps(@5MP máx. 5 fps) • NETO Ninguno • Tamaño de píxel Ninguno • Mín. Iluminación Color: 0,03 Lux (F1.6, 1/30 s) BW: 0,003 Lux (F1.6, 1/30 s, 30 IRE), 0 Lux (LED IR encendido) • Salida de video USB: Micro USB Tipo B, 1280x720 para instalación • Distancia de transmisión de vídeo Ninguno
	Lente • Longitud focal (relación de zoom) Focal fija de 3,0 mm • Máx. Relación de apertura F1.6 • Campo de visión angular Alto: 100°/ V: 73°/ Profundidad: 129° • Mín. Distancia del objeto 0,5 m (1,64 pies) • Control de enfoque Fijado • Tipo de lente IRIS fijo • Tipo de montaje M12 • Lente opcional Ninguno
	Panoramica Inclinación Rotación • Rango de giro / inclinación / rotación 0°~350° / -35°~70° / 0°~355
	Red • Ethernet RJ-45(10/100BASE-T) • Compresión de video H.265/H.264: Principal/Alto, MJPEG • Compresión de audio Ninguno • Códec inteligente Manual (área 5ea), WiseStream Ⅱ

	• Ajuste de calidad de vídeo H.264/H.265: control del nivel de velocidad de bits objetivo MJPEG: control del nivel de calidad • Control de velocidad de bits H.264/H.265: CBR o VBR MJPEG: VBR • Transmisión Unicast (20 usuarios) / Multicast Transmisión múltiple (hasta 5 perfiles) • Protocolo IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP,RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/ v3(MIB-2), ARP, DNS, DDNS, QoS, UPnP, Bonjour, LLDP, SRTP (TCP, UDP unidifusión) • Interfaz de programación de aplicaciones Perfil ONVIF S/G/T/M SUNAPI (API HTTP)
	Seguridad • Protección del sistema operativo/firmware Arranque seguro, firmware firmado, cifrado de firmware • Autenticacion de usuario Autenticación implícita, prevención de ataques de fuerza bruta • Autenticación de red Autenticación 802.1X (EAP-TLS, EAP-LEAP, EAP-PEAP MSCHAPv2) • Comunicación segura HTTPS, SRTP, WSS (Websocket seguro) • Control de acceso Control de acceso basado en dirección IP • Protección de datos Cifrado de información de autenticación, cifrado de compresión ZIP • Auditoría Acceso de usuario/Sistema/Gestión de registros de eventos • ID del dispositivo Certificado de dispositivo (CA raíz privada de Hanwha) • Almacenamiento seguro Cifrar partición de tarjeta SD • Certificado de seguridad Seguro por defecto
	ISS SOR-CAM LICENCIA PARA CAMARA VMS SECUROS (1)

LECTORA DE BLUETOOTH Y TARJETA NFC RBH-N86-DNB-D-O	
	De acuerdo con especificaciones técnicas, donde debe incluir la instalación a todo costo, contemplando el uso de la ducteria prevista en la estructura de comunicaciones en la obra, para que garantice las conexiones requeridas de datos utilizando cable 18 - 22 AWG, 6-7 hilos conductor blindado no trenzado para conectar la lectoras de acceso tipo bluetooth, cable Duplex 2x16 para conectar boton no touch, cable 18 - 22 AWG, 6-7 hilos conductor blindado no trenzado para conectar el detector de apertura,cable Duplex 2x16 para conectar el electroiman. Incluye todos los elementos para la puesta en operación de los mismo (conectorización, certificación, marquillado, diagramación, amarres, velcros, etc). Garantizando la organización del cableado a través de electroestática, dejando todo en funcionando correctamente, las conexiones deben llegar hasta la controladora, ubicada en el cuarto de equipos tanto el cable de datos como

	el de energia, es de recalcar que deben tener compatibilidad 100% con el sistema electrónico de seguridad de la UMA estandarizado por JETIC. Lector de tarjeta y bluetooth compatible con credenciales DESFire (EV1 y EV2) para los más altos estándares de seguridad. La comunicación con los controladores puede ser utilizando Wiegand estándar u OSDP v1 o v2 para mayor seguridad donde se requiere la máxima integridad y detección de manipulación.
	El lector debe manejar el protocolo UHSC a través de NFC o Bluetooth. UHSC es una credencial virtual gratuita para Android e iOS donde la APP crea una credencial virtual en el Smartphone, con la posibilidad de eliminar la posibilidad de piratería o duplicación de credenciales virtuales. UHSC es una forma más alta de seguridad. Tipo Caja electrica Lector SECTOR. Tecnologia DESFire (EV1 & EV2) / Bluetooth / NFC Frecuencia 13.56 MHz Montaje Muro Dimensiones "4.75” X 3.125” X .75” (119mm X 80mm X 20mm)" Carcasa ABS Peso 5.29 oz. (150 g) Voltaje DC 9~15 V Consumo de Corriente 80 mA @ 12 VDC Rango de lectura 2 cm - 20 cm Dependiendo del tipo de credencial. Comunicación Wiegand / OSDP version 1&2 Conector "Pigtail" de 18 pulgadas Cableado 500’ (152m) max, 18 - 22 AWG, 6-7 cable conductor blindado Temperatura de operación -40º F to +158º F (-40º C to + 70º C) Color Negro Tono de Audio Anunciador Piezoelectrico incorporado Anunciacion visual LED Tricolor Certificaciones Grado proteccion IP-68 Panel Analógico de Alarma incluye batería y Bocina
	El lector bluetooh debe traer los respectivos accesorios para su puesta en funcionamiento. **Cerraduras Electromagnéticas Para Puerta 600-Lb Con Accesorios Y Cargador** Caracteristicas: Fuerza de retención: 600 libras • UL 10C, USA y CANADA, UL 294 (Unidades del sistema de control de acceso), UL 1034 (Mecanismo de bloqueo eléctrico resistente a robos), UL 864 (Alarma contra incendio) USA solamente • Caja de aluminio anodizado (US 28) • 12/24 V.C.C seleccionable

	• Protección contra sobretensiones MOV • Soporte de montaje ajustable • Accesorios de montaje completo para instalaciones típicas • Soporte en "L" y soportes en "Z" disponibles para facilita LED bicolor y sensor de retención para indicación de estado de cierre • Verde Puerta cerrada y asegurada • Rojo Puerta no cerrada y/o asegurada • Apagado Puerta en uso / Sin alimentación **Brazo Hidraulico 80 Kg Y Sensor De Apertura** Aplicación • Para puertas de acción simple en los tipos de puertas más comunes. (apertura derecha e izquierda), en la hoja o en el marco. • Rápido y fácil de instalar. • Este cierrapuertas es adecuado para una gran variedad de tipos de puertas. • Es adecuado para puertas resistentes al fuego según lanorma UL. • Dispone de dos válvulas para ajustar la velocidad de cierre. • Su pequeño tamaño hace que sea fácil de almacenar. Fuerza • 2/3 • Para puertas ancho máximo 950 mm • Peso de la puerta máximo 80kg • Cambio de fuerza girando la válvula de fuerza del brazo. • Brazo Estándar • Apertura • 180° Valvulas de ajuste: • Velocidad de cierre (180°-15°) • Acción de Enganche (15°-0°) Color: • Plata



Boton no touch

- Botón de salida no touch con sensor de proximidad.
- Modelo TH-040.
- Marco metálico.
- Rango para accionar el botón con la mano es de 1 a 10 cm.
- Voltaje de entrada 12v
- Capacidad del relé 120v AC 30v DC / 3 Amp
- Consumo en Standby / operación <33mA / <200 mA
- Dimensiones en mm (70mm An x 115mmAl x 30mmPr)
- Peso del producto de 125 gramos
- color gris plata
- Temperatura de trabajo -15ºC/+50 ºC

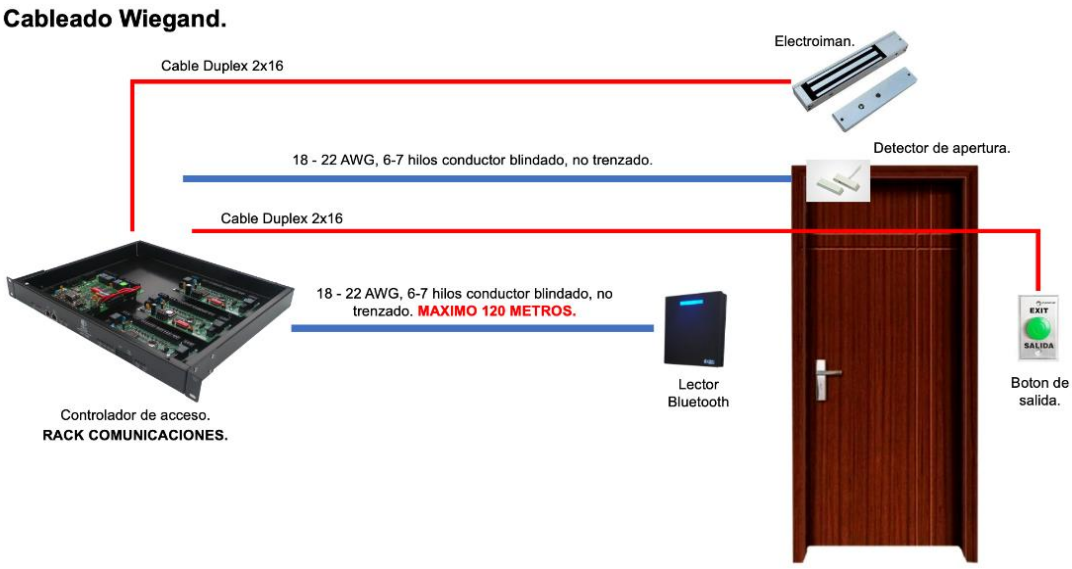
Sensor Magnetico para Puertas

Sensor magnético para puertas, ventanas, etc. El sensor y el imán cierran o abren el circuito de acuerdo a si están cerca uno del otro. Estos sensores se utilizan en proyectos de seguridad del hogar. De fácil integración con Arduino o Raspberry Pi, con lo cual es posible construir un completo sistema de seguridad. Cuenta con cinta doble en la cara inferior para poder instalarse fácilmente.

- Compatible con Arduino, Raspberry, PIC etc.
- Cuenta con orificios para atornillar a superficie plana
- Cuenta con pegamento en la parte inferior para pegar a superficie plana
- Uno de los sensores cuenta con cables
- Aplicaciones: Seguridad

ESPECIFICACIONES:

- Tipo: Sensor magnético y vibración
- Salida del sensor: Analógico
- Voltaje de alimentación máximo: 100 V-
- Corriente máxima: 0.5 A

	• Potencia nominal: 3 W • Mecanismo: NA (Normalmente abierto) • Distancia de activación mínima: 15 mm • Distancia de activación máxima: 25 mm • Largo del cable: 25 cm • Dimensiones: 34 mm X 41 mm X 6.5 mm • Material: Plástico ABS • Color: Blanco • Modelo: MC-38
	Observación sobre la topologia de conexión  La conexión debe ir dentro de una misma ducteria EMT independiente al de la red de datos UTP, desde la controladora hasta la lectora de bluetooth, electroiman, sensor de apertura, boton no touch contemplando el siguiente cableado: • Cable 22 AWG, 6-7 hilos conductor blindado, no trenzado hasta 120 metros para el lector bluetooth • Cable 22 AWG, 6-7 hilos conductor blindado, no trenzado para el sensor de apertura • Cable duplex 2x16, para el electroiman • Cable duplex 2x16, para el boton de salida Esta conexión se puede implementar dentro de la misma ducteria para una o dos puertas maximo, en caso de ser mas puertas seperar la ducteria de electroimanes con la ducteria del lector bluetooth, boton no touch y sensor de apertura. Entre mayor mumero de cables de voltaje haya en la ducteria puede ocacionar interferencia y calentamiento del cable.

	El electroiman tiene un limite para ser energizado de 50 metros con 12 voltios y 01 amperio. Si la conexión supera la distancia previamente mencionada, se debe incluir 01 modulo relevador auxiliar, el cual va ser energizado por el mismo cable duplex 2x16. El electroiman si supera los 50 metros debe contemplar una toma de corriente regulada doble posterior al ingreso de la puerta, sobre el cielo razo con una caja de inspección para futuro mantenimiento.

CONTROLADOR DE ACCESO RBH-UNC5825RM-4-KIT-PB Y ACCESORIOS	
	De acuerdo con las condiciones físicas e infraestructura de los controles de acceso de la FAC, este equipo de acuerdo con su tecnología realiza una función específica de identificación dentro de la plataforma integrada de VMS y Control acceso RBH, basado en la Ubicacion establecida en el estudio de seguridad de la UMA y la cantidad de dispositivos mecanicos que se van a integrar. Controlador para 4 lectoras wiegand u OSDP, permite configuracion 2 puntos de acceso lector de entrada y salida, o 4 puntos de accesos con lector de entrada y boton de salida, montaje en RACK 19", incluye fuente de alimentacion tanto para el controlador como electroimanes y lectores y 2 baterias 7Ah/12v. El equipo debe ser compatible e integrable, debe ser entregado, probado, configurado y puesto en funcionamiento de acuerdo con sus características técnicas y licenciamiento en el VMS existente en la UMA, sistema de control acceso RBH, software AXIOM y controlador tipo rack RBH existente en la Unidad Militar Aérea. El Kit se conforma con: • Controlador para montaje en RACK 19", 4 puertos wiegand. • Montaje para RACK 19" • Fuente de poder
	CONTROLADORA IP (WIEGAND), INCLUYE ACCESORIOS. Las tarjetas electrónicas de control para integración de los equipos mecánicos (puertas, torniquetes, talanqueras) deben ser de tecnología WIEGAND u OSDP con protocolo IPv4 o IPv6, permitiendo enlazar estos equipos con el sistema VMS “SECUROS” de administración de analíticas y control acceso “RBH” existente en la Unidad Militar Aérea.

	MINIMO SOPORTE PARA 4 LECTORAS WIEGAND. Debe incluir la instalación a todo costo, con el cableado (incluye Electroimán, botón de salida notouch, sensor de apertura, base pedestal para equipos, entre otros necesarios para la correcta operación del equipo). • Capacidad de memoria: Tarjetas: 100,000 Eventos: 100,000. • Firmware : Flash. • Puertos nativos de comunicación TCP/IP: 4 x TCP/IP, 10/100 Ethernet (2PoE) / 6 x RS-485 programables. • Requerimiento cable de comunicación: Minimo Cat6, blindado, par trenzado, 20 - 22 AWG; 1,200 m total. • Puertos lector Wiegand : 4 incluidos, hasta 5 formatos de tarjeta por puerto (expandible a 16) Control piezo, y LEDs verde/rojo del lector. • Requerimiento cable lector Wiegand : Blindado, multiflar de 6 u 8 conductores, 20 - 22 AWG; Max 150m 20 AWG). • Chapas inalámbricas : Programable para agregar hasta 28 chapas inalámbricas totalmente supervisadas. • Entradas programables : 12 • Tipo circuito entradas : N.A. o N.C con o sin supervisión de línea. • Salidas programables : 12 (6/6) • Salidas de relevador : Relevador tipo C, SPDT, 5A 30 V AC/DC, contactos secos. • Salidas de voltaje: Colector electrónico abierto, 12 VDC 100 mA MAX. • Entradas/Salidas adicionales: Totalmente programables y expandibles hasta 4,320. • Panel de alarma integrado : Agrega hasta 508 teclados LCD de 4 zonas (SafeSuite). • Entrada Tamper : 2 entradas para tamper del gabinete. • Alimentación eléctrica : 1A a 12 VDC max • PoE : PoE Dual, redundante y de alta potencia (25W c/u) • Circuitos de protección : Fusibles restaurables - entrada, salida, lectora. • Dimensiones: 1U rack 19” : 1.75” H x 19” W x 15” D • Condiciones de operación : Temperatura: 0 a 70°C; Humedad: 20 a 80% RH (sin condensación)

	• -El Controlador Maestro de Acceso deberá ser tipo montaje RACK que no requiera gabinete para ser instalado, cubierta de aluminio o similar, no PCB (Protoboard Circuit Board) con entradas o conexiones mínima para 2 lectoras por medio de conexión Wiegand. • -El Controlador Maestro de Acceso deberá poseer arquitectura modular, dos (2) puertos de red Ethernet 10/100 uno (1) de ellos debe ser puerto PoE con estándar IEEE 802.3at. • -El Controlador Maestro de Acceso deberá poder crecer hasta por lo menos 120 lectoras por red local de arreglo de controladores de ser necesario. • -El Controlador Maestro de Acceso deberá contar con al menos 3 puertos de comunicación tipo RS485. • -El Controlador Maestro de Acceso deberá poder enrolar hasta 100.000 usuarios y poseer memoria para históricos en desconexión de al menos 50.000 en caso de pérdida de conexión con el Software de gestión de control de acceso. • -El Controlador Maestro de Acceso deberá 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. • -El controlador Maestro de Acceso deberá 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. • -El Controlador Maestro de Acceso deberá 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. • -El Controlador Maestro de Acceso deberá permitir la utilización de formatos de tarjeta de 48 Bits o superior. • -El controlador Maestro de Acceso deberá poseer comunicación wiegand u OSDP hacia sus lectores. • -El Controlador Maestro de Acceso debe ser compatible con lectores tipo código de barra, QR y PDF417 para leer la trama de la cedula colombiana y ser utilizada como método de autenticación de acceso según corresponda a la institución. • -El Controlador Maestro de Acceso deberá contar con un tamper embebido a él mismo, sin dependencia de ningún elemento externo o de terceros y que no ocupe una de sus entradas para esta función,

	teniendo así la facultad de enviar una alerta hacia el software de gestión de control de acceso, cuando el gabinete o encerramiento donde se encuentra contenido ha sido vulnerado o abierto. • -El Controlador Maestro de Acceso deberá ser de la misma marca y fabricante que el sistema de gestión de control de acceso y módulo de visitantes, estandarizado para la Fuerza Aerea “RBH”. • -El Controlador Maestro de Acceso deberá contar con protección térmica embebida en Alimentación de Entrada, Salida y en la Alimentación hacia las Lectoras. • -El Controlador Maestro de Acceso 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. • -El Controlador Maestro de Acceso deberá contar con una conexión de batería directamente embebido a él, conexión que deberá ser supervisada hacia el servidor de acceso, teniendo así la facultad de enviar una alerta hacia el software de gestión de control de acceso. • -El Controlador Maestro de Acceso deberá poseer por lo menos poseer tres (3) diferentes leds en total para la visualización de estado y funcionamiento. Por lo menos dos (2) leds de diferente color por cada puerto RS-485 - seis (6) en total - para visualización de operación de transmisión y recepción (conectividad con el software de gestión de control de acceso y/o con arreglos de controladores). • El Controlador Maestro de Acceso deberá de manera local de ser necesario operar la misma cantidad mínima de lectoras por modulo controlador en configuración puerta esclusa local. • -Este equipo debe ser instalado en el Rack principal del edificio ubicado en el segundo piso en el cuarto tecnico, operando de manera óptima. • -El sistema se entregará completamente en operación e integrado al 100% con el sistema de control acceso “RBH” de la UMA. • El Controlador Maestro de Acceso deberá poder utilizar para su comunicación Wiegand y Serial el cable tipo AWG 20 - 22, trenzado y blindado. Esto debe estar indicado en la hoja de datos del equipo proveniente directamente del fabricante. • -El Controlador Maestro de Acceso deberá 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.

	• -El controlador Maestro deberá 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.

SUMINISTRO E INSTALACIÓN CÁMARA FIJA EXTERNA QNV-C8083R	
	DESCRIPCIÓN GENERAL <u>Compresión y transmisión de video: la cámara tendrá las siguientes propiedades relacionadas con las señales de video que produce.</u> 1. Compresión H.265, H.264 y MJPEG, cada una derivada de un codificador dedicado y capaz de transmitirse de forma independiente y simultánea. a. H.265 y H.264: máx. 30/25 fps (60 Hz/50 Hz) en todas las resoluciones b. MJPEG – Máx. 30 fps(@5MP máx. 5 fps) 2. La cámara podrá configurar hasta 10 perfiles de transmisión de video independientes con diferentes configuraciones de codificación, calidad, velocidad de fotogramas, resolución y velocidad de bits. 3. La cámara podrá configurar varias selecciones de resolución. a. Relación de aspecto 16:9: 2560x1440, 1920x1080, 1280x720, 800x448, 640x360 b. Relación de aspecto 4:3: 2592x1944, 1280x960, 800x600, 640x480, 320x240 C. Relación de aspecto 5:4: 720x576 d. Relación de aspecto 3:2: 720x480 4. La cámara admitirá transmisión de video unidifusión hasta 20 usuarios. 5. La cámara deberá admitir transmisión de vídeo multidifusión.

	6. La cámara podrá configurar DNS dinámico (DDNS). El DDNS será proporcionado sin coste adicional por parte del fabricante. 7. La cámara deberá proporcionar WiseStream Ⅱ, Dynamic GOV y Dynamic fps para administrar eficientemente la velocidad de bits de la transmisión de video y reducir el almacenamiento. 8. La cámara deberá proporcionar WiseNR Ⅱ que funcione según el motor de IA para reducir el ruido y la borrosidad de la imagen. <u>Cámara: el dispositivo de la cámara deberá tener las siguientes propiedades físicas y de rendimiento:</u> 1. Clasificación IP66, IK10 para protección contra impactos 2. Verdadero funcionamiento día/noche con filtro de corte IR extraíble 3. La cámara deberá poder producir imágenes claras en escenas de alto contraste con un amplio rango dinámico de exposición múltiple de hasta 120 dB. 4. La cámara admitirá la reducción de ruido digital utilizando tecnología de reducción de ruido 2D y 3D. 5. La cámara podrá configurar 32 áreas de enmascaramiento de privacidad con zonas cuadrangulares de 4 puntos. 6. La cámara proporcionará visualización de video en un teléfono inteligente (iPhone, Android) para ajustar el ángulo de visión, la rotación y el enfoque. <u>Inteligencia y análisis: la cámara tendrá un conjunto de funciones analíticas inteligentes.</u> 1. Análisis a. Eventos de análisis basados en motor de IA (Persona, Vehículo) 1) Detección de movimiento

	2) Detección de objetos: Persona/Vehículo ((Coche/Autobús/Camión/Motocicleta/Bicicleta) 3) Línea virtual (Cruce/Dirección), 4) Área virtual (Merodear/Intrusión/Entrar/Salir) b. Eventos de análisis 1) Detección de desenfoque 2) manipulación 3) Área virtual (Aparecer/Desaparecer) 2. Detección de movimiento con 8 áreas de detección definibles con zonas poligonales de 8 puntos y tamaño de objeto mínimo/máximo 3. Detección de desenfoque: ese evento se puede crear cuando se detecta el desenfoque de la lente de la cámara 4. Detección de manipulación, ese evento se puede crear cuando se bloquea la pantalla o se cambia la posición de la cámara 5. Los tipos de objetos clasificados son Persona y Vehículo. 6. Tipo de vehículo de soporte de atributos (coche/autobús/camión/moto/bicicleta) 7. La cámara admiteDetectionShot <u>D. Interoperabilidad: la cámara deberá ser compatible con ONVIF Profile S, G, T y M.</u> E. La cámara deberá poseer las siguientes características adicionales: 1. Servidor web integrado, al que se accede a través de navegadores sin complementos, incluidos Google Chrome, IE11, MS Edge, Mozilla Firefox y Apple Safari.

	2. Tarjeta de memoria Micro SD/SDHC/SDXC con intervalos de grabación configurables antes y después de la alarma 3. Opción de grabación NAS con intervalos de grabación configurables antes y después de la alarma 4. Alarmas y notificaciones a. activadores de notificación de alarma: 1) Entrada de alarma 2) Detección de movimiento 3) Análisis de vídeo 4) Desconexión de la red b. medios de notificación disponibles al activarse: 1) Carga de archivos mediante FTP y correo electrónico 2) Notificación vía correo electrónico 3) Almacenamiento local (SD / SDHC / SDXC) o grabación NAS en eventos desencadenantes 4) Salida de alarma 5) Entrega (PTZ preestablecido, Enviar mensaje por HTTP/HTTPS/TCP) 6) Reproducción de clips de audio 5. Contador de píxeles disponible en el visor web. 6. Capacidad PoE, incluido calentador mediante PoE 7. IP66, compatible con IK10
	ESPECIFICACIONES DETALLADAS <u>A Video:</u>

	1. Dispositivo de imagen: CMOS de 1/2,8" 2. Escaneo: Progresivo 3. Iluminación mínima a. Color: 0,07 lux (F1,6, 1/30 s) b. Ancho de banda: 0,007 lux (F1,6, 1/30 s, 30 IRE) C. 0Lux (LED IR encendido) <u>B. Lente:</u> 1. Longitud focal: varifocal motorizada de 3,2~10,2 mm (3,2x) 2. Máx. Relación de apertura: F1.6 (gran angular) ~ F3.1 (teleobjetivo) 3. Campo de visión a. Alto: 95°(Gran angular)~29°(Teleobjetivo) b. V: 69°(Gran angular)~21°(Tele) C. Profundidad: 126°(Gran angular)~36°(Teleobjetivo) 4. mín. Distancia del objeto: 1,2 m (3,93 pies) 5. Control de enfoque: enfoque simple 6. Tipo de lente: DC auto iris (corregido por IR) <u>C. Panorámica, inclinación y rotación</u> 1. Rango: 0°~350° / -35°~70°/ 0°~355° <u>D. Funciones operativas</u> 1. Título de la cámara: Desactivado/Activado (se muestra hasta 85 caracteres) 2. Configuración día/noche: Automático (ICR) / Color / B/N / Horario 3. Longitud visible por infrarrojos: 30 m (98,42 pies) 4. Compensación de retroiluminación: Apagado/BLC/WDR 5. WDR: 120dB 6. Reducción de ruido digital: SSNRⅤ, WiseNRⅡ (basado en motor AI) 7. Estabilización de imagen digital: ninguna 8. Desempañamiento: Ninguno 9. Detección de movimiento: 8ea, zonas poligonales de 8 puntos 10. Enmascaramiento de privacidad: 32 unidades, zonas cuadrangulares de 4 puntos 11. Control de ganancia: Apagado/Bajo/Medio/Alto 12. Balance de blancos: ATW / AWC / Manual / Interior / Exterior 13. Corrección de la distorsión de la lente: soporte 14. Velocidad del obturador electrónico: Mín. / Máx. / Antiparpadeo (1/5 ~ 1/12.000 s) 15. PTZ digital: soporte (preestablecido, grupo)

	16. Rotación de imagen: Voltear, Espejo, Vista de pasillo (90°/270°) 17. E/S de alarma a. Entrada 1ea b. Salida 1ea C. La E/S de alarma se admite a través de un cable opcional (SPP-C7400) 18. Activadores de alarma: análisis, desconexión de red, entrada de alarma 19. Eventos de alarma (cuando se produjo la activación de la alarma) a. Carga de archivos (imagen): correo electrónico/FTP b. Notificación: correo electrónico C. Grabación: grabación SD/SDHC/SDXC o NAS en activadores de eventos d. Salida de alarma mi. Entrega (preestablecido PTZ, enviar mensaje por HTTP/HTTPS/TCP) F. Reproducción de clips de audio 20. Contador de píxeles: soporte 21. Almacenamiento: Micro SD/SDHC/SDXC 256 GB (1 ranura), soporte NAS 22. Análisis inteligente con IA a. Detección de movimiento b. Detección de objetos: Persona/Vehículo ((Coche/Autobús/Camión/Motocicleta/Bicicleta) C. Línea virtual (Cruce/Dirección), d. Área virtual (Merodear/Intrusión/Entrar/Salir) 23. Eventos analíticos a. Detección de desenfoque b. manipulación C. Área virtual(Aparecer/Desaparecer) 24. Salida de vídeo (instalación) a. USB: Micro USB Tipo B, 1280x720 para instalación 25. Memoria: 2 GB de RAM, 1 GB de memoria flash
	<u>Transmisiones de vídeo</u> 1. Compresión de vídeo: H.265, H.264, MJPEG 2. Resolución: 2592x1944, 2560x1440, 1920x1080, 1280x960, 1280x720, 800x600, 800x448, 720x576, 720x480, 640x480, 640x360, 320x240 3. Velocidad de fotogramas máxima a. H.265/H.264: Máx. 30 fps en todas las resoluciones b. MJPEG: máx. 30 fps(@5MP máx. 5 fps)

	4. Códec inteligente: modo manual (basado en área: 5EA), WiseStream Ⅱ: compatible 5. Método de control de la tasa de bits a. H.265/H.264: CBR o VBR b. MJPEG: VBR 6. Capacidad de transmisión: transmisión múltiple (hasta 5 perfiles) 7. Método de transmisión: Unicast/Multicast 8. Usuarios Simultáneos: 20 máximo (Unicast) 9. Conjunto de perfiles: máx. 10 unidades 10. Almacenamiento y grabación a. La cámara tendrá almacenamiento en tarjeta SD integrado. 1) Tipo de tarjeta: Micro SD/SDHC/SDXC 2) Capacidad: Hasta 256 GB (1 ranura) b. NAS 11. Interoperabilidad: Perfil ONVIF S / G / T/ M, SUNAPI
	<u>Audio</u> 1. Entrada de audio a. Seleccionable (entrada de micrófono/entrada de línea) b. La entrada de audio se admite a través de un cable opcional (SPP-C7400) 2. Salida de audio a. Fuera de la linea b. Máx. nivel de salida 0,5 Vrms C. La salida de audio se admite a través de un cable opcional (SPP-C7400) 3. Compresión de audio a. G.711 u-law /G.726 Seleccionable b. G.726 (ADPCM) 8KHz, G.711 8KHz C. G.726: 16 Kbps, 24 Kbps, 32 Kbps, 40 Kbps d. AAC-LC: 48 Kbps a 16 KHz
	<u>Red</u> 1. Conectividad: Ethernet 10/100 Base-T mediante conector RJ-45 2. Protocolo a. IPv4/v6, TCP, UDP b. Configuración: DHCP, LLDP C. Servicio web: HTTP, HTTPS d. Servicio de red: ARP, Bonjour, DNS, ICMP, NTP, SNMP v1/2c/3 – MIB-2, UPnP mi. Medios: RTP, RTCP, RTSP F. Unidifusión: SRTP gramo. Multidifusión: IGMP

	h. Notificaciones: FTP, SMTP i. Acceso remoto: PPPoE 3. DDNS: la cámara deberá admitir los servicios DDNS ofrecidos por el fabricante y otras ofertas de servicios disponibles públicamente. 4. QoS – DSCP de capa 3 5. Característica de seguridad a. Protección de contraseña de usuario b. El dispositivo no proporcionará una contraseña predeterminada de fabricación. Será necesario cambiar la contraseña predeterminada para acceder a la cámara. C. La cámara deberá exigir un nivel mínimo de complejidad de contraseña. d. La cámara no tendrá una contraseña de puerta trasera de fabricación. mi. El fabricante deberá proporcionar una herramienta que permita realizar cambios de contraseña en varias cámaras al mismo tiempo. F. Filtrado de direcciones IP: lista de direcciones IP permitidas o bloqueadas gramo. Comunicación de vídeo segura SRTP para multidifusión. h. Autenticación de inicio de sesión implícita. i. Registro de acceso de usuarios. j. Autenticación 802.1X (EAP-TLS, EAP-LEAP) k. Certificado de dispositivo (CA raíz de Hanwha Vision) l. Autenticación de inicio de sesión HTTPS (SSL/TLS) y comunicación de vídeo segura con TLS v1.3 metro. m Cifrado de disco en grabación en tarjeta SD (AES-256) norte. n Cifrado de archivos en grabación en disco local mediante navegador web (AES-256) o Autenticación mutua (Autenticación de cliente) para una comunicación segura pag. p Sistema operativo seguro y arranque de seguridad 6. Descubrimiento: el fabricante ofrecerá un programa de descubrimiento para identificar todos sus dispositivos en la red. 7. Configuración: el fabricante deberá ofrecer un programa de configuración que permita de forma remota a los usuarios cambiar la configuración de varias cámaras simultáneamente.

	8. Actualización de firmware: el fabricante deberá ofrecer un programa capaz de actualizar varias cámaras al mismo tiempo (sin requerir acceso a cámaras individuales). 9. Configuración de copia de seguridad de la cámara: el fabricante deberá proporcionar un programa que brinde la capacidad de guardar múltiples configuraciones de la cámara en un archivo y restaurar estas configuraciones de la cámara si es necesario. 10. Informes: el fabricante deberá proporcionar una herramienta que pueda generar un informe que incluya una vista en miniatura, dirección MAC, dirección IP, número de serie y otras configuraciones de la cámara.
	<u>Eléctrico</u> 1. poder a. Voltaje/corriente de entrada: PoE (IEEE 802.3af, Clase 3) b. Consumo de energía: Máximo 12,95 W, típico 5,3 W
	<u>Mecánica y ambiental</u> 1. Color/Material: Blanco/Aluminio a. Burbuja: cúpula con revestimiento duro 2. Dimensiones (ancho x alto): ø140x110,2 mm (ø5,51x4,34") 3. Peso: 875 g (1,93 libras) 4. Orificio de conducto compatible: Ninguno 5. Gangbox: simple, doble, octágono de 4” 6. Caja posterior: SBO-140BW 7. Montaje colgante (domo): SBP-140HMW 8. Temperatura y humedad a. En funcionamiento: 30°C~+55°C(-22°F ~ +131°F) / 0~95% RH (sin condensación) 1) Las puestas en marcha deben realizarse por encima de -30°C 2) Control de humedad/con ventilación de aire b. Almacenamiento: -50°C~+60°C(-58°F ~ +140°F) / 0~95% HR 9. Protección mecánica (vandálica): IK10 10. Protección de ingreso: IP66
	<u>Distancia de J. DORI</u> 1. Detección (25 PPM/ 8 PPF): Ancho: 42,7 m (140,20 pies) / Tele: 186,9 m (613,28 pies) 2. Observar (63 PPM/ 19 PPF): Ancho: 17,2 m (56,08 pies) / Tele: 75,4 m (245,31 pies)

	3. Reconocer (125 PPM/ 38 PPF): Ancho: 8,5 m (28,04 pies) / Tele: 37,4 m (122,66 pies) 4. Identificar (250 PPM/ 76 PPF): Ancho: 4,3 m (14,02 pies) / Tele: 18,7 m (61,33 pies)
	EMC y seguridad 1. FCC a. 47 CFR Parte 15 Subparte B (ANSI C63.4a-2017 Clase A) b. ICES-003 Edición 7 (ANSI C63.4a-2017 Clase A) 2.CE a. Directiva EMC 2014/30/UE (EN 55032:2015/A11:2020 Clase A, EN 50130-4:2011) 3. UKCA a. Normativa 2016 (EN 55032:2015/A11:2020 Clase A, EN 50130-4:2011) 4. RCM AS/NZS CISPR 32:2015 AMD 1:2020 Clase A 5. VCCI CISPR 32:2016 Clase A 6. KS C 9832 Clase A, KS C9835 7. UL 62368-1, CSA C22.2 62638-1:19, CEI 62471 8. CE EN IEC 63000:2018 (sustancias peligrosas)
	ISS SOR-CAM LICENCIA PARA CAMARA VMS SECUROS (1)

GENERALIDADES POSTERIORES A LAS FICHAS TECNICAS

CONDICIONES DE INSTALACIÓN CÁMARAS DE SEGURIDAD / VMS SECUROS
El contratista debe garantizar y entregar las referencias descritas con sus respectivas especificaciones, para garantizar un único punto de soporte a la infraestructura con la misma referencia o superior para mantener la uniformidad y homogeneidad en la plataforma tecnológica que la FAC tiene estandarizando en las UMAs, ya que es crecimiento de la infraestructura actual. Suministro, instalación y puesta en servicio de los equipos solicitados en la Descripción de elementos y/o servicios, para instalar en la guardia principal, cuarto de equipos entre otros lugares de las diferentes unidades de la Fuerza Aérea Colombiana. De acuerdo con especificaciones técnicas, donde debe incluir la instalación a todo costo, contemplando el uso de la ductería prevista en la obra, para que garantice las conexiones requeridas de energía y datos, dejando todo funcionado correctamente, las conexiones deben llegar hasta los cuartos de equipos o gabinetes, donde se debe

conectar tanto energía como datos de los equipos solicitados. Es de recalcar que deben tener compatibilidad 100% con el sistema electrónico de seguridad SecurOS estandarizado por JETIC.

Todos los materiales y equipos que suministrará el proveedor, deberán ser nuevos y de primera calidad, libres de defectos e imperfecciones, de los últimos diseños o modelos existentes en el mercado en el momento de ejecución del contrato y deben desempeñar las funciones mínimas requeridas por la Fuerza Aérea Colombiana.

Todos los equipos, software, sistemas o subsitemas a suministrar por el contratista deben tener la información, técnica precisando las normas que a continuación se relacionan para el correcto funcionamiento del equipo.

La IEEE

- VHDL
- POSIX
- IEEE 1394
- IEEE 488
- IEEE 802
- IEEE 802.11
- IEEE 754

ISO

- ISO 8859
- ISO 9000
- ISO 9001
- ISO 09004
- ISOIEC 9126
- IS9 9660
- ISO 9899
- ISO 10279
- IS0 10646
- ISO/IEC 11172

ITU

- RTF (Rich Text Format)
- TIFF (Tagged Image File Format)
- RIFF (Resource Image File Format)
  - –WAV (Waveform Audio File Format)
  - –MIDI File Format for Standard MIDI files
  - –AVI Audio Video Interlaced
  - –PAL Palette File Format for colors represented by RGB values.
- JPEG
- MPEG
- Otros: BMP, GIF, AVI

La empresa contratista debe suministrar los elementos necesarios para la protección eléctrica de los equipos que se pretenden adquirir dentro del anexo técnico, los equipos que tengan puerto ethernet, se debe instalar protectores de datos de acuerdo a la norma técnica con las siguientes características:

Dimensiones	91 x 61 x 32,5 mm (3,58 x 2,4 x 1,28 ")
Peso	80 g (2,82 onzas)
Conexiones de interfaz	(2) Conectores hembra RJ45
Protección ESD / EMP	Absorción de corriente transitoria con respuesta a sobretensión de 100V / sa 1kV / us
Voltaje DC de chispa	90 V a 100 V / s
Impulso máximo Voltaje de chispa	700 V a 1 kV / nosotros
Corriente de descarga	5kA (máximo) 0,5 kA (normal)

Aislamiento máximo Resistencia	1G ohmios a 50 V
Capacitancia máxima	1,0 pF a 1 MHz
Protección de línea de datos	Ethernet RJ45 10/100/1000
IEEE 802.3af PoE Apoyo	sí
Choque y vibración Certificación	Estándar ETSI300-019-1.4
Operando Temperatura	- 30 a 65 ° C (-22 a 149 ° F)
Humedad de funcionamiento	10 a 90% sin condensación

Todos los gabinetes a intervenir que requieran protectores contra sobretensiones DPS deben ser suministrados e instalados por el contratista.

- Especificaciones: material: PC.
- Material: PC. Material ignífugo.
- Número de polos: 3P
- Tiempo de respuesta: Menos e igual a 25ns
- Voltaje nominal: 420 V
- Corriente de descarga máxima: 40KA
- Hasta: Menos e igual a 1.8kv
- Peso: Aprox.359g/12.7oz

CONDICIONES DE INSTALACIÓN CÁMARAS EVITE PROCESOS DENEGADOS DE RMA

Para la instalación de cámaras de seguridad el contratista debe seguir las siguientes instrucciones las cuales deben ser documentadas y entregados digitalmente a la supervisión del contrato para futuros procesos de garantía con la casa fabricante RMA.

1.- El problema o análisis de las fallas y/o comportamiento errático de los equipos, deberá realizarse extensivamente por parte nuestra con su ayuda. Pues es usted como institución deben informar con detalle las novedades que se puedo presentar durante su funcionamiento.
2.- Cuando se trata de equipos para exteriores -E considere documentar siempre la instalación, ya sea nueva o de algún equipo de reemplazo. La casa fabricante de las cámaras va a solicitar fotografías e incluso vídeos.
3.- Se debe usar accesorios originales y ensamblarlos correctamente. Ejemplo: Algunos modelos para exteriores con este caso, requieren un conector IP66 RJ45 Tipo Push Pull. Este accesorio debe armarse bien. El tipo de cable que deben utilizar es STP/SFTP. Con forro liso y no corrugado, para que el sello IP66 se mantenga en perfecto estado y no entre polvo, humedad/agua y/o insectos al interior del equipo donde existen componentes eléctricos y/o electrónicos.
4.- Algunos modelos usan juntas de goma o glándulas o empaques que ayudan a brindar la protección IP66. Igualmente deben ser ensamblados adecuadamente. Deben revisar bien dichas instalaciones. Las juntas de goma no deben estar rotas, fisuradas o en mala posición (no torcidas o fuera de su lugar)

5.- Asegúrese de apretar adecuadamente todos los tornillos de los equipos en las partes donde llevan este tipo de accesorios. Por ejemplo, la base de esta cámara donde llega el cable de red y hay empaques o juntas que intervienen en brindar una protección IP66.
6.- Todos los Midspans que utilicen deben estar debidamente protegidos si cuentan con zapata de tierra física y no estar expuestos a la intemperie o humedad o agua.
7.- Cuando energice cualquier cámara para exteriores y las alimente con los Midspans o switchs, debe forzosamente usar cable STP o S/FTP desde los mismos. Algunos Midspans deben ser aterrizados. (Verifique si cuentan con zapata de tierra física y aterrícelos)
8.- La mayoría de los equipos que comercializamos y fabricamos, tienen un Manual de usuario. En el manual de usuario hay una sección específica para resolución de problemas. Es importante que antes de que nos contacten, la revisen. También existe una sección donde puede ver la forma en cómo se deben instalar y/o ensamblar los equipos y uno o varios diagramas donde se localizan las partes de los mismos, así como los LEDS. (También hay Guías de instalación - revíselas minuciosamente) Es necesario revisar la sección de los LED's. En dicha sección se pude observar el comportamiento u operación correcta o incorrecta del equipo con base a la información que emite el LED.
9.- Todos los equipos y accesorios de montaje que incluyan una zapata de tierra física, deben aterrizar cerdos sin excepción alguna. Usualmente el personal de contratista, se puede observar que no aterrizan correctamente. (Por lo tanto, las zapatas de tierra física de las cámaras, se observa intacta durante procesos de RMA, ya que no fueron utilizadas)
10.- El LED de la cámara debería encenderse siempre y mostrar un código de error u operación normal. La mayoría de las veces, si no encienden es o porque no los están energizando bien, o porque los equipos sufrieron un daño por corto circuito, sobre carga eléctrica, golpes o agua. Esos daños no están cubiertos por la garantía.
11.- La garantía cubre cualquier defecto de fábrica. Sin embargo, como no tenemos manera de revisar básicamente los equipos antes de enviarle un reemplazo, siempre la casa fabricante va a solicitar que realice cierto tipo de pruebas y/o nos envíe Reportes del Servidor de los mismos e incluso fotografías y/o vídeos del sitio de instalación.
12.- Deben reportar las fallas de los equipos y generar los Reportes del servidor cuando éstos estén montados y no después de haberlos desmontado. Se sugiere reportarlos con nosotros y hacernos llegar la información, tan pronto como los inconvenientes sucedan. Utilice el sistema de Helpdesk o Mesa de ayuda para reportarlos.
13.- En los modelos Q60XX-E, Q61XX-E, P56XX-E existen protecciones IP66 RJ45 en plástico rígido al rededor del conector de red. Dichas protecciones o sus tornillos, por ningún motivo deben ser removidos o aflojados. Debe asegurarse que antes de instalarlos y/o configurarlos; Los técnicos en laboratorio o en campo siempre utilizan cableado de color rojo con el conector IP66 RJ45 Tipo Push Pull. Eso ayudará a evitar daños a las cámaras, falsos contactos y/o daño a las protecciones de las mismas o conectores, o a su red y/o demás equipos conectados.
14.- Siempre vamos a solicitar una copia de la factura de compra. Considere conseguirlas cuando exista la posibilidad de que requiera se procesar un RMA.
15.- Posiblemente posterior al finalizar la garantía del contratista directamente, la institución tiene otros años de garantía con la casa fabricante, por lo tanto, se deben

seguir todas las recomendaciones de fabrica para instalación de las cámaras de seguridad.
16.- Se debe documentar todo el proceso de instalación con toma de fotografías y videos, los cuales deben ser entregadas digitalmente. Adicional, de un acta por cámara instalada, esto con facilitar los proceso de RMA.

CONDICIONES DE INSTALACIÓN PERIFERICOS AXIOM XA

El contratista debe garantizar y entregar las referencias descritas con sus respectivas especificaciones, para garantizar un único punto de soporte a la infraestructura con la misma referencia o superior para mantener la uniformidad y homogeneidad en la plataforma tecnológica que la FAC tiene estandarizando en las UMAs, ya que es crecimiento de la infraestructura actual.

Suministro, instalación y puesta en servicio de los equipos solicitados en la Descripción de elementos y/o servicios, para instalar en la guardia principal, cuarto de equipos entre otros lugares de las diferentes unidades de la Fuerza Aérea Colombiana. De acuerdo con especificaciones técnicas, donde debe incluir la instalación a todo costo, contemplando el uso de la ductería prevista en la obra, para que garantice las conexiones requeridas de energía y datos, dejando todo funcionado correctamente, las conexiones deben llegar hasta los cuartos de equipos o gabinetes, donde se debe conectar tanto energía como datos de los equipos solicitados. Es de recalcar que deben tener compatibilidad 100% con el sistema electrónico de seguridad de la UMA RBH estandarizado por JETIC.

Todos los materiales y equipos que suministrará el proveedor, deberán ser nuevos y de primera calidad, libres de defectos e imperfecciones, de los últimos diseños o modelos existentes en el mercado en el momento de ejecución del contrato y deben desempeñar las funciones mínimas requeridas por la Fuerza Aérea Colombiana.

Todos los equipos, software, sistemas o subsitemas a suministrar por el contratista deben tener la información, técnica precisando las normas que a continuación se relacionan para el correcto funcionamiento del equipo.

La IEEE

- VHDL
- POSIX
- IEEE 1394
- IEEE 488
- IEEE 802
- IEEE 802.11
- IEEE 754

ISO

- ISO 8859
- ISO 9000
- ISO 9001
- ISO 09004
- ISOIEC 9126
- IS9 9660
- ISO 9899
- ISO 10279
- IS0 10646
- ISO/IEC 11172

ITU

- RTF (Rich Text Format)

- TIFF (Tagged Image File Format)
- RIFF (Resource Image File Format)
  - –WAV (Waveform Audio File Format)
  - –MIDI File Format for Standard MIDI files
  - –AVI Audio Video Interlaced
  - –PAL Palette File Format for colors represented by RGB values.
- JPEG
- MPEG
- Otros: BMP, GIF, AVI

La empresa contratista debe suministrar los elementos necesarios para la protección eléctrica de los equipos que se pretenden adquirir dentro del anexo técnico, los equipos que tengan puerto ethernet, se debe instalar protectores de datos de acuerdo a la norma técnica con las siguientes características:

Dimensiones	91 x 61 x 32,5 mm (3,58 x 2,4 x 1,28 ")
Peso	80 g (2,82 onzas)
Conexiones de interfaz	(2) Conectores hembra RJ45
Protección ESD / EMP	Absorción de corriente transitoria con respuesta a sobretensión de 100V / sa 1kV / us
Voltaje DC de chispa	90 V a 100 V / s
Impulso máximo Voltaje de chispa	700 V a 1 kV / nosotros
Corriente de descarga	5kA (máximo) 0,5 kA (normal)

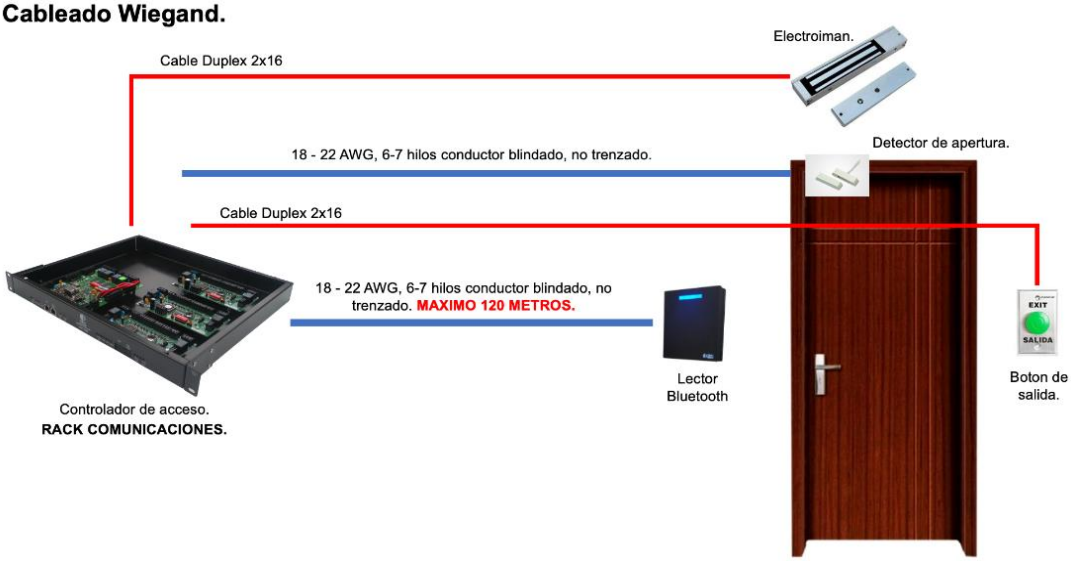
Aislamiento máximo Resistencia	1G ohmios a 50 V
Capacitancia máxima	1,0 pF a 1 MHz
Protección de línea de datos	Ethernet RJ45 10/100/1000
IEEE 802.3af PoE Apoyo	sí
Choque y vibración Certificación	Estándar ETSI300-019-1.4
Operando Temperatura	- 30 a 65 ° C (-22 a 149 ° F)
Humedad de funcionamiento	10 a 90% sin condensación

Todos los gabinetes a intervenir que requieran protectores contra sobretensiones DPS deben ser suministrados e instalados por el contratista.

- Especificaciones: material: PC.
- Material: PC. Material ignífugo.
- Número de polos: 3P
- Tiempo de respuesta: Menos e igual a 25ns
- Voltaje nominal: 420 V
- Corriente de descarga máxima: 40KA
- Hasta: Menos e igual a 1.8kv
- Peso: Aprox.359g/12.7oz

Observación sobre la topologia de conexión

Cableado Wiegand.



La conexión debe ir dentro de una misma ducteria EMT independiente al de la red de datos UTP, desde la controladora hasta la lectora de bluetooth, electroiman, sensor de apertura, boton no touch contemplando el siguiente cableado:

- Emplee un cable de calibre 20 o 22 AWG con 6-8 hilos, blindado, pero no trenzado, para conectar la controladora y la lectora, con una distancia máxima de 150 metros entre ambas.
- Emplee un cable de calibre 20 o 22 AWG con 2 hilos para conectar el sensor magnético, asegurándose de que la distancia entre la controladora y el sensor no exceda los 300 metros.
- Para la conexión del electroimán, elija un cable de calibre 20 o 22 AWG con 2 hilos, teniendo en cuenta una distancia máxima de 300 metros entre la controladora y el electroimán. Este último deberá ser alimentado mediante una fuente externa.
- Emplee un cable de calibre 20 o 22 AWG con 2 hilos, considerando un alcance de hasta 300 metros entre la controladora y el botón. Si el botón requiere energización, asegúrese de contar con dos hilos adicionales para suministrar dicha energía a través de una fuente externa.
- Para el funcionamiento óptimo del electroimán, es fundamental alimentarlo con una fuente externa, tal como se detalla en su hoja de datos. Se recomienda la instalación de un diodo de protección en las proximidades del electroimán, a fin de salvaguardar la controladora contra posibles fluctuaciones de energía. Además, es importante respetar la distancia máxima de 300 metros entre la controladora y el electroimán para asegurar su funcionamiento confiable.

Esta conexión se puede implementar dentro de la misma ducteria para una o dos puertas maximo, en caso de ser mas puertas seperar la ducteria de electroimanes con la ducteria del lector bluetooth, boton no touch y sensor de apertura. Entre mayor mumero de cables de voltaje haya en la ducteria puede ocacionar interferencia y calentamiento del cable.

Consideraciones generales para los cableados de Control de Acceso

1. Todos los cables que lleven más de 12V y 0,5A debe obligado ir por cable dúplex con el calibre calculado versus la distancia del dispositivo.

2. Todos los contactos secos deben ser por cable de control pero deben ir reforzados llegado a las borneras, para 4 hilos en total mínima.

3. Para el cableado wiegand el cual se utiliza en los lectores de iris como bluetooth si la distancia supera el 60% del estándar debe ser blindado, 6 u 7 conductores, multifilar, 18-22 AWG; Máximo 500 pies (150 m @20 AWG). El RS-485 debe ser de Cable Par trenzado blindado, 20-22 AWG; 4,000 pies (1.200 m) total.

4. Verificar que todos los sistemas tengan respaldo de UPS o Baterías de respaldo al interior de la caja de la controladora.

5. Colocar el diodo de protección a las salidas que sea el caso.

6. Todos los cables deben estar marquillados en sus extremos y organizados en cada gabinete.

7. No se realizarán garantías cuando las fuentes estén alteradas o no sean de marca reconocida.

8. Todos los gabinetes deben estar aterrizados de forma adecuada según la norma técnica que aplique.

9. Se recomienda tener dicterio separada para el cableado de control de acceso y otros como red de datos, dado la posibilidad de saboteo o corte de dichos cableados por error.

10. Se debe utilizar cable de automatización para la comunicación ya sea wiegand u OSDP.

11. Todos los tableros deben contar con su respectivo DPS.

OBSERVACIONES SITE SURVEY	
	Posterior a la adjudicación del contrato se requiere hacer una visita a las unidades para validar todas las instalaciones propuestas, esta visita se debe realizar con el personal de JESED/JETIC. El contratista debe levantar acta en la Unidad, donde se adjuntara las imágenes correspondientes de los puntos a intervenir y la propuesta que realizara para la instalación del equipo en mención la cual será autorizada por la supervisión del contrato.

PRUEBAS DE ACEPTACIÓN, PROTOCOLOS Y PUESTA EN SERVICIO EQUIPOS
Todas las partes, equipos, sistemas o subsistemas objeto del contrato estarán sujetos a pruebas en campo sobre su operación, con el fin de comprobar su adecuado funcionamiento, montaje e instalación y cumplimiento de las especificaciones técnicas.

REQUERIMIENTOS PROPONENTES
El contratista debe suministrar la totalidad del material, herramienta, equipo y la maquinaria requerida que sea necesaria para la ejecución del contrato en las instalaciones donde se tiene proyectado instalar los equipos de Sistema Electrónicos de Seguridad.
El personal que designe el contratista y todo el equipo de trabajo bajo la aprobación del supervisor del contrato, deberá suscribir un compromiso de confidencialidad a todos sus empleados, con relación a la información y documentación que tenga acceso. Al igual deberá suscribir una autorización para efectuar Estudio de Seguridad por parte de la Dirección de Inteligencia de la FAC, el cual podrá ser realizado en cualquier momento y cuantas veces sea necesario.
Los gastos debidos a embalaje, transporte, exportación, importación, impuestos y demás a que haya lugar durante el proceso de instalación, suministro, puesta en servicio, garantía de los equipos y partes serán asumidos por el contratista sin costo extra para la FAC. .

GARANTIAS
El contratista durante el periodo de la garantía responderá por la reparación dentro de los términos establecidos de los equipos y módulos que se envíen para esta actividad; así como los datos de contacto para que la entidad los pueda localizar, la garantía cuenta a partir de recibo a satisfacción e instalación de los equipos del proceso contractual.
Es responsabilidad del contratista garantizar que todos los equipos y partes adquirir sean nuevos y de primera calidad, de acuerdo con las especificaciones descritas en este documento, así mismo, se obliga a reparar o reemplazar a sus expensas aquellos, materiales e instalaciones que resulten de mala calidad, con defectos de fabricación o que fallen durante la operación, por un plazo mínimo de dos (02) años contado a partir de la fecha de la instalación y del recibo a satisfacción por parte del supervisor del contrato, incluido el tiempo de garantía de las empresas fabricantes.
El contratista deberá comprometerse durante el tiempo de garantía a cambiar por nuevos aquellos materiales y suministros que fallen en caso de no poder reemplazar o reparar la(s) pieza(s). Para cualquier caso el mantenimiento debe ser sin ningún costo para la FAC. El contratista por cada equipo o elemento suministrado que sea enviado a garantía, se debe entregar un equipo que cumpla con todas las especificaciones y funcionalidades que garanticen el servicio, debido a que la Fuerza Aérea Colombiana no debe ser la afectada en los tiempos o trámites de garantía que se vea inmerso el contratista. Es responsabilidad del contratista efectuar la reparación de los elementos de hardware y software descritos en el anexo técnico y contará con un máximo de 30 días calendario

cuando se lleve a cabo en el país o máximo 90 días calendario para reparación en el exterior. El plazo en tiempo para la reparación en el exterior incluye transporte y trámites de exportación, importación y nacionalización a que haya lugar, sin costo extra para FAC. Si el contratista no actúa en respuesta a la reclamación de garantía dentro del período de quince (15) días, el contratista reembolsara al Comprador todos los costos asociados con el reemplazo o reparación del producto defectuoso.

MERCADO DE PARTES Y ACTUALIZACIONES
El contratista debe garantizar al Ministerio de Defensa – Fuerza Aérea Colombiana por mínimo cinco (5) años, el suministro en el mercado de partes y actualización del software para los equipos suministrados, de acuerdo con el desarrollo de la tecnología.

TRANSPORTE Y SEGUROS
El transporte, seguros de los equipos, herramientas, elementos del software y hardware a instalar de acuerdo con el presente documento, debe incluir el personal técnico durante su traslado dentro del país hasta el lugar de instalación, son responsabilidad del contratista, sin costo extra para la FAC.
El personal contratista debe cumplir con las normas de seguridad, bioseguridad y salvaguardar la integridad de sus empleados, al igual que respetar las normas de movilidad, protocolo de bioseguridad de la FAC dentro las instalaciones de la Fuerza Aérea Colombiana.
El personal de obra del Contratista, para su protección, deberá mantener durante el tiempo de trabajo una dotación adecuada a la labor desempeñada, botas, casco y overol, y demás elementos de seguridad industrial necesarios para la ejecución de las actividades referentes al contrato.
El supervisor del contrato debe revisar los contratos de trabajo que el contratista de obra y los subcontratistas suscriban con cada uno de sus trabajadores; revisar las planillas de pagos de salarios, reportes de tiempo, liquidaciones y reclamaciones laborales, seguro colectivo de vida, llevando estricto control de pago de los aportes a la EPS, al fondo pensiones, a la administradora de riesgos profesionales, a la promotora de salud, al Instituto Colombiano de Bienestar Familiar - ICBF, al Servicio Nacional de Aprendizaje - SENA, a las respectivas cajas de compensación familiar; verificar el cumplimiento de todos aquellos aspectos que involucra la contratación de personal, incluyendo lo establecido en el programa de contratación de mano de obra, preparado por el contratista de obra y aprobado por la FAC Y/O SUPERVISIÓN. Verificará el cumplimiento del pago de salarios, prestaciones sociales, indemnizaciones y demás obligaciones laborales, así como con las obligaciones parafiscales del personal vinculado en la ejecución del contrato.
El supervisor del contrato debe controlar y verificar por intermedio del comité técnico y las oficinas se seguridad y salud en el trabajo de las unidades el nivel de riesgo de los trabajadores que ejecutan el contrato y el pago correspondiente por dicho concepto de conformidad con el decreto 768 de 2022.

Igualmente se debe tener en cuenta la Guía del sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST-FAC Versión 1, y la Guía Lineamiento Seguridad y Salud en el Trabajo para Contratistas y Proveedores al Servicio de la Fuerza Aérea Colombiana, así como aquellas que las adiciones, modifiquen o deroguen.

ESTUDIOS DE SEGURIDAD

De acuerdo al cumplimiento de la directiva permanente 056-2020 “Lineamiento para el desarrollo de estudios de seguridad en la FAC”, de igual manera por medio de la circular No FAC-S-2021-009942-CR del 28 de agosto de 2021 / MDN-COGFM-FAC-COFAC-JEMFA-COAES- JEINA se informa las siguientes pautas para tener en cuenta en el proceso de los tramites de estudios de seguridad.

- Los supervisores de cada contrato, deberán entregar los Estudios de Seguridad del personal de contratistas en físico, original y previo oficio de solicitud mediante Hermes, a la Jefatura de Inteligencia Aérea. Estos contaran con 20 días para su desarrollo a partir del momento en que lleguen a la Dirección de Contrainteligencia Aérea.
- En el oficio remisorio tramitado mediante Hermes no se deben anexar los formatos del ESP.
- Los formatos del ESP deberán estar diligenciados en su totalidad , en el formato correspondiente (Actualizado) y con los documentos anexos que se solicitan en cada uno de ellos.
- Teniendo en cuenta el tiempo de permanencia de los contratistas en cada UMA, se debe diligenciar el formato de Estudio de seguridad así: Formato No 1 " OA-JEINA- FR-131" para personal con permanencia mayor a 30 días, Formato No 2 " OA-JEINA- FR-132" para personal funcionario de la Fuerza que deba actualizar ESP, Formato No 4 " OA-JEINA-FR- 134" para personal cuyo contrato o permanencia sea inferior a 30 días y anexo, el Formato No 5 " OA-JEINA-FR-135" consentimiento previo expreso e informado el cual aplica para todos los casos.
- Se recomienda a los supervisores de contrato hacer previa revisión de estos items para evitar que estos sean devueltos por el no cumplimiento de los misos

El contratista debe dar cumplimiento a los instructivos de control de acceso en las bases Fuerza Aérea (BFA), hace referencia al área de las guardias principales donde el personal, material y equipo se identifica para su autorización. Con el objetivo de identificar, validar, autorizar y hacer seguimiento.

Es importante resaltar que las medidas de seguridad en los controles de acceso no solo abarcan para las guardias de las unidades, si no que las dependencias internas, áreas de sectores, zona operativas y restringidas.

El contratista debe asumir el costo de los ficheros correspondiente a cada unidad cuando por tiempo sean requeridos para los ingresos a las unidades de acuerdo al instructivo “GA-JES-INS-034 INSTRUCTIVO CONTROL ACCESO EN LAS BASES FUERZA AÉREA”, así:

2. Temporal.
Otorgado a personal militar en comisión o tránsito; también se puede entregar a personal civil que cumple actividades en la UMA, como contratistas o familiares de militares que residen en la BFA. Su vigencia es máxima 90 días, la cual puede ser renovada.

Dependiendo el area de trabajo las especificaciones generales para los ficheros corresponden al instructivo previamente mencionado asi:

- Rojo: Zona Operativa, Centro de comunicaciones Base Fuerza Aérea (CCOBA), salas VIP, Aeronaves.
- Amarillo: Grupo Técnico, Hangares de mantenimiento, almacenes aeronáuticos.
- Azul: instalaciones administrativas de la BFA, incluyendo los grupos/escuadrones de seguridad.
- Verde: dependencias anexas a la UMA, si existen.
- Gris: personal de contratos y servicio doméstico.
- Negro: personal extranjero.
- Azul – verde: Zona residencial.

CONDICIONES PARA RECEPCIÓN DE HARDWARE Y SOFTWARE
El contratista debe presentar al supervisor del contrato con anticipación antes de iniciar la implementación de hardware y software adquirido los protocolos de recepción de todos los elementos incluidos en el presente documento con el fin de ser revisados, modificados y aprobados.
El contratista debe realizar la entrega de la siguiente documentación en medio digital (02) originales, junto a las pruebas de aceptación, así: 1. Planos de instalación final. 2. Inventario de todos los equipos, módulos, tarjetas, software, licencias instaladas y adquiridos. 3. Documento con MAC, IP, Usuario y contraseña de equipo, Numero de Serie, Nombre del Swich y numero de puerto donde se conectó el equipo. Registros fotográficos (previo a instalaciones físicas, posterior a la instalación, interconexiones a red WAN y LAN, AP´s, servidores, control acceso, cámaras, y de más puntos de monitoreo críticos que se implementen).
Una vez realizados y firmados los protocolos, se deberá entregar al Supervisor del contrato (01) original impresos y dos (1) copias en medio digital de los protocolos, documentación, información técnica del contrato incluyendo, registros fotografías de instalación y de los equipos recibidos.

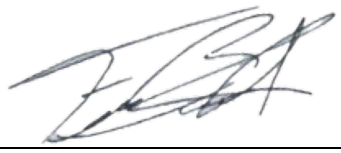
CONDICIONES AMIENTALES
Verificar el cumplimiento por parte del contratista de la ley 435 de 1998 y 842 de 2003, por las cuales se reglamenta el ejercicio de la arquitectura e ingeniería y profesiones auxiliares respectivamente, de la Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios, de la Ley 828 de 2003: por la cual se expiden normas para el control a la evasión del sistema de seguridad social y de la legislación ambiental y las normas de higiene y seguridad de la construcción.
El contratista debe comprometer a tomar las medidas necesarias para eliminar o minimizar los posibles efectos e impactos negativos sobre el medioambiente que se causen durante la ejecución y desarrollo del objeto contractual, de conformidad con lo establecido en las normas ambientales vigentes, los desechos de material provenientes del resultado final de las actividades a ejecutar, deberán ser transportados por el contratista a lugares autorizados y darle su disposición final, de igual forma el contratista deberá mantener en perfectas condiciones de aseo las áreas en las que realice implementaciones.
Se deben relacionar las obligaciones que debe cumplir el contratista en materia de gestión ambiental, como por ejemplo el cumplimiento a los planes de gestión ambiental, permisos y licencias ambientales, etc. Se debe tener en cuenta la Directiva Permanente FAC No 003-2021 “Plan de acción ambiental 2021-2022”, y la Guía de Gestión Ambiental código GA-OFGEA-GUI-002, así como aquellas que las adicionen, modifiquen o deroguen.

COMPROMISO DE CONFIDENCIALIDAD
El personal que designe el contratista y sea aprobado por el supervisor del contrato el cual participará durante la ejecución del contrato deberá suscribir un compromiso de confidencialidad, con relación a la información y documentación que tenga acceso. Al igual deberá suscribir una autorización para efectuar estudio de Seguridad por parte de la Dirección de Inteligencia de la Fuerza Aérea Colombiana, el cual podrá ser realizado en cualquier momento y cuantas veces sea necesario.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA FAC
La Fuerza Aérea Colombiana de acuerdo a la directiva permanente No 004 / 2022, informa por medio del radicado FAC-S-2022-000036-DR del 09 de febrero de 2022/MDN-COGFM-FAC-COFAC, los criterios y directrices para la implementación y divulgación de las políticas del (SGSI), para ser cumplidas por todos los funcionarios y terceros que por su relación contractual tengan acceso a los activos de información institucional. Es de carácter obligatorio que el supervisor le informe al personal contratista y trabajadores, las diferentes referencias que deben conocer con relación a las políticas del (SGSI) así:

1. Constitución política de Colombia 1991,
2. Ley 594 de 2000 “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.
3. Ley Estatutaria 12266 de 2008 “Por la cual se dictan las disposiciones generales del habeas data y se regía el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial de servicios y la proveniente de terceros países y se dictan otras disposiciones”.
4. Ley 1273 d e2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado-denominado “de la protección de la información y de los datos”-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
5. Ley 1448 de 2011 “Por la cual se dictan medidas de atención, asistencia y reparación integral a las víctimas del conflicto armado interno y se dictan otras disposiciones”.
6. Ley 1448 de 2011 “Por la cual se expide el código de procesamiento administrativo y de lo contencioso administrativo”.
7. Ley Estatutaria 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.
8. Ley Estatutaria 1621 de 2013 “Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones”.
9. Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la información Pública Nacional y se dictan otras disposiciones”.
10. Ley 1755 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
11. CONPES 3854 de 2016 Política Nacional de Seguridad digital.
12. Ley 2080 de 2021 “Por la cual se reforma el Código de Procedimiento Administrativo y de lo Contencioso Administrativo”.
13. Norma ISO/IEC 27001 – Estándar para la seguridad de la información.
14. Decreto 2578 de 2012 “Por el cual se reglamenta el sistema nacional de archivos, e establece la Red Nacional de Archivos, se deroga el Decreto número 4124 de 2004 y se dictan otras disposiciones relativas a la administración de los archivos del estado.
15. Decreto 1377 de 2013, decreto reglamentario de la ley 1581 de 2012.FAC-2020-07162-CI.
16. Decreto 1070 de 2015” por el cual se expide el decreto único reglamentario del sector administrativo de defensa.
17. Decreto 1081 de 2015 “Por medio del cual se expide el Decreto Reglamentario único del sector presidencia de la república”.
18. Decreto 0106 de 2015” por el cual se reglamenta el Titulo VIII de la 594 de 2000 en materia de inspección, vigilancia y control a los archivos de las entidades del Estado y a los documentos de carácter privado declarados de interés cultural y de dictan otras disposiciones”.

19. Resolución 3564 de 2015 “Por la cual se reglamentan algunos artículos del Decreto No 1081 de 2015”.
20. Directiva permanente 18 de 2014 “políticas de seguridad de la información para el sector de defensa”.
21. Directiva permanente 154 de 2014 “políticas de seguridad de la información FF.MM”.
22. Directiva permanente 167 de 2014 “procedimientos de seguridad militar en las fuerzas militares”.
23. Manual de contrainteligencia Aérea MACI FAC-2.2.0 Restringido de 2016.
24. Directiva permanente 014 de 2020 “políticas de seguridad y privacidad de la información para FAC”.

	
CT. BAUTISTA ROJAS FERNEY JOHANY	**T2. ARIEL MAURICIO VILLAMIL NIÑO**
Gerente del Proyecto	**Comité Estructurador Técnico**