

ANEXO 1

ESPECIFICACIONES TÉCNICAS MÍNIMAS Y ALCANCE OPERATIVO DE LOS SISTEMAS ELECTRÓNICOS DE SEGURIDAD DEL INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA — IDEA — VIGENCIA 2026

**“SUMINISTRO DE BIENES Y LA PRESTACIÓN DE SERVICIOS ESPECIALIZADOS
PARA EL MANTENIMIENTO, SOPORTE TÉCNICO, INSTALACIÓN E INTEGRACIÓN
DE COMPONENTES ASOCIADOS A LOS SISTEMAS ELECTRÓNICOS DE
SEGURIDAD DEL INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA —IDEA— Y
SUS DEMÁS PREDIOS.”**

Julio 2026

1. OBJETO DEL ANEXO TÉCNICO

El presente Anexo Técnico tiene por objeto establecer las condiciones técnicas mínimas que deberá cumplir el contratista para la ejecución del contrato relacionado con el suministro, instalación, configuración, integración, puesta en funcionamiento y soporte técnico de componentes, licencias y elementos puntuales asociados a los Sistemas Electrónicos de Seguridad —SES— del Instituto para el Desarrollo de Antioquia —IDEA—, así como para la prestación de servicios especializados de mantenimiento preventivo, predictivo y correctivo de los sistemas existentes de control de accesos, videovigilancia —CCTV—, detección de incendios, intrusión, gestión de edificios —BMS— y demás sistemas asociados.

Este anexo hace parte integral de los documentos del proceso contractual y deberá ser observado por el contratista durante todas las etapas de ejecución, incluyendo planeación, suministro, instalación, configuración, integración, pruebas, puesta en funcionamiento, mantenimiento, soporte técnico, capacitación, entrega de informes y cierre contractual.

La contratación para la vigencia 2026 se estructura bajo el enfoque de **mantenimiento especializado, soporte técnico, conservación funcional y complementación puntual** de los Sistemas Electrónicos de Seguridad existentes, teniendo en cuenta que durante la vigencia 2025 el IDEA adelantó la actualización e implementación de componentes críticos de control de accesos, CCTV y BMS, así como mantenimiento preventivo de los sistemas de intrusión y detección de incendios.

2. ALCANCE GENERAL DEL ANEXO

El contratista deberá ejecutar las actividades requeridas para garantizar la continuidad operativa, disponibilidad, interoperabilidad, trazabilidad y confiabilidad funcional de los Sistemas Electrónicos de Seguridad del IDEA, mediante:

- a. El suministro de componentes, licencias, periféricos, elementos de autenticación, infraestructura y demás bienes puntuales definidos por la Entidad.
- b. La instalación, configuración, integración y puesta en funcionamiento de dichos componentes.
- c. La prestación de servicios especializados de mantenimiento preventivo, predictivo y correctivo.
- d. El soporte técnico sobre los sistemas existentes y sobre los componentes que se incorporen durante la ejecución contractual.
- e. La realización de pruebas funcionales, pruebas de integración y validaciones operativas.
- f. La capacitación al personal designado por el IDEA.
- g. La entrega de informes técnicos, evidencias, actas, registros de pruebas y documentación aplicable.

El alcance técnico comprende, entre otros, los siguientes frentes: control de accesos, gestión de visitantes, control peatonal mediante pasillos motorizados, videovigilancia — CCTV—, detección de incendios, intrusión, infraestructura asociada, cableado, licenciamiento, soporte mensual, mantenimiento general y atención de predios del Instituto.

SISTEMAS ELECTRÓNICOS DE SEGURIDAD IDEA 2026					
ITEM	DESCRIPCIÓN	UNID AD	CANT	MARCA	REFERENCIA
Lectoras de tarjetas sistema de control de accesos					
1	Lector de proximidad RFID de doble frecuencia para control de acceso, compatible con montaje en caja tipo Gang Box o equivalente. Debe operar como mínimo en frecuencias de 125 kHz y 13,56 MHz, con soporte para credenciales de proximidad de baja frecuencia y tarjetas inteligentes sin contacto de alta frecuencia bajo estándares ISO/IEC 14443 A/B o equivalentes, incluyendo tecnologías seguras tipo DESFire, EV1 o equivalentes. Debe contar con compatibilidad NFC o equivalente, grado de protección mínimo IP67 y resistencia al impacto mínimo IK08. Compatible con tarjetas inteligentes sin contacto de 13,56 MHz bajo estándar ISO/IEC 14443 A/B, incluyendo tecnologías tipo MIFARE, DESFire, EV1 o equivalentes.	UND	41		
Tarjetas sistema de control de acceso					
2	Tarjeta inteligente sin contacto para control de acceso físico, con operación en frecuencia de 13,56 MHz, compatible con estándar ISO/IEC 14443 tipo A o equivalente. Deberá contar con mecanismos de seguridad criptográfica mediante cifrado AES de 128 bits o superior, autenticación segura entre tarjeta y lector, comunicación mediante canales cifrados, protección contra lectura no autorizada, clonación o suplantación, e identificador dinámico, aleatorio o no trazable. Deberá permitir almacenamiento seguro de datos de credencial mediante diversificación de llaves, firmas de autenticación, cifrado o mecanismos equivalentes, y ser compatible con los lectores y controladores del sistema de control de acceso existente o a implementar.	UND	500		
Terminales Biométricas, Reconocimiento Facial					

3	Terminal biométrico de reconocimiento facial para control de acceso físico, con lector RFID integrado de doble frecuencia, compatible con credenciales de 125 kHz y 13,56 MHz. Debe soportar tarjetas de proximidad de baja frecuencia y tarjetas inteligentes sin contacto de alta frecuencia bajo estándares ISO/IEC 14443 A/B, ISO/IEC 18092 o equivalentes, así como tecnologías NFC y Bluetooth de baja energía o equivalentes. El equipo deberá contar con detección de rostro vivo o mecanismo anti-suplantación, velocidad de reconocimiento facial máxima de 0,3 segundos, capacidad mínima para 50.000 usuarios, alimentación a 24 VDC o rango equivalente, pantalla mínima de 5,5 pulgadas tipo IPS LCD o equivalente con resolución mínima de 720 x 1280 píxeles, compatibilidad con protocolos RTSP, ONVIF perfil S y VoIP o equivalentes, y grado de protección mínimo IP65. Debe incluir pedestal, base, soporte o accesorio equivalente para fijación segura sobre pasillo motorizado, junto con todos los elementos necesarios para su instalación, configuración y correcto funcionamiento.	UND	4	SUPREMA	BS3-DB
Cableado anunciador Sistema de Detección de Incendios					
4	Cable de incendios para comunicación de anunciador en portería	ML	1200	FPLR	2x16
Elementos complementarios de CCTV HANWHA					
5	IP/Analog Hybrid Keyboard Controller	UND	1	HANWHA	SPC-7000
6	Cámara domo antivandálica para exteriores Wisenet Q, 5 MP a 30 fps, lente varifocal motorizada de 3,2~10,2 mm (H: 95°~29° / V: 69°~21°), triple códec H.265/H.264/MJPEG con Wisestream III (basado en mo	UND	2	HANWHA	QNV-C8083R
7	Cámara tipo bala antivandálica para exteriores en red Wisenet Q, 5MP a 30 fps, lente varifocal motorizada de 3,2 ~10,2 mm (H: 95°~29° / V: 69°~21°), códec triple H.265/H. 264/MJPEG con Wisestream III	UND	2	HANWHA	QNO-C8083R
8	Licencia Virtual WAVE Professional License Enables one 1 IP stream recording	UND	2	HANWHA	WAVE-PRO-01
9	Monitor industrial o pantalla profesional de mínimo 55 pulgadas, apto para uso en videowall o visualización continua, con brillo típico mínimo de 500 nits, bisel ultradelgado para continuidad visual en arreglos multipantalla y profundidad máxima de 93,1 mm o inferior, sin incluir soporte.	UND	1		

	Debe contar como mínimo con interfaces HDMI, DisplayPort o equivalente, DVI-D o equivalente, USB, RS-232C o equivalente y RJ45/Ethernet para comunicación o administración en red. El suministro deberá incluir soporte de pared compatible con el equipo, así como los accesorios, cables y elementos necesarios para su instalación y correcto funcionamiento.				
Sistema de gestión de visitantes					
10	Solución integral de software para gestión y control de acceso de visitantes y contratistas, orientada a uso institucional o gubernamental, con administración centralizada y operación en puntos de portería o recepción. Debe incluir como mínimo una licencia o instancia principal de servidor, tres licencias o estaciones operativas para puntos de portería, y motor de base de datos relacional incluido, sin costo adicional de licenciamiento, compatible con SQL o equivalente. La solución deberá permitir el registro, autorización, validación, seguimiento y trazabilidad de visitantes y contratistas, administración de usuarios, perfiles y permisos, generación de reportes, consultas históricas, parametrización de sedes y puntos de acceso, e integración con la infraestructura tecnológica de control de acceso existente Schneider.		1		
11	Licencia, módulo o componente de integración entre la plataforma de gestión de visitantes y contratistas y el sistema de control de acceso físico existente Schneider. Debe permitir la interoperabilidad entre ambos sistemas mediante servicios web, API, protocolo SOAP, REST o mecanismo equivalente, para el intercambio seguro de información relacionada con visitantes, contratistas, credenciales, autorizaciones, horarios, permisos de acceso y eventos. El suministro deberá incluir las licencias, conectores, servicios, interfaces o componentes necesarios para la instalación, configuración, pruebas, puesta en funcionamiento y operación integrada con la plataforma de control de acceso de la entidad Schneider.		1		

12	Licencia, módulo o usuario operativo para gestión móvil de ingreso y salida de visitantes y contratistas, compatible con dispositivos móviles con sistema operativo Android 8.0 o superior. Debe permitir el registro, consulta, validación y trazabilidad de visitantes y contratistas desde punto de acceso móvil, incluyendo autenticación del usuario operador, validación de autorizaciones, registro de fecha, hora, punto de ingreso y sincronización con la plataforma central de gestión de visitantes y contratistas. El suministro deberá incluir activación, configuración y puesta en funcionamiento.		2		
13	Tableta electrónica portátil para uso institucional, nueva, no remanufacturada, con pantalla táctil de alta resolución entre 8,7" y 14,6", tasa de refresco mínima de 90 Hz, procesador multinúcleo tipo octa-core o superior, memoria RAM mínima desde 4 GB y almacenamiento interno mínimo desde 64 GB, cámara posterior mínima de 8 MP, cámara frontal mínima de 5 MP, batería recargable mínima desde 5.100 mAh, conectividad Wi-Fi y opción de conectividad móvil 4G o 5G según configuración requerida, debe incluir case industrial. El dispositivo deberá contar con reconocimiento facial o mecanismo biométrico equivalente, diseño delgado y portátil, chasis metálico o material resistente, compatibilidad con accesorios de productividad como teclado, cubierta protectora o lápiz óptico cuando aplique, y sistema operativo móvil compatible con herramientas de productividad, administración y seguridad empresarial.		2		
14	Horas de soporte para instalación, capacitación, parametrización, pruebas y puesta en marcha del sistema de manera remota.		30		
15	Actualizaciones por licencia y soporte técnico remoto ante fallas funcionales del software, vigencia un (1) año.		1		
16	1. Cámara web externa Full HD, con resolución mínima de 1920 x 1080 píxeles, conectividad USB o equivalente, compatible con equipos de cómputo institucionales y sistemas operativos de uso común. Debe incluir base o soporte para instalación sobre monitor, escritorio o superficie equivalente, y todos los accesorios necesarios para su instalación y correcto funcionamiento. (Se deben suministrar 2 cámaras)		2		

	2. Lector de códigos de barras 1D y 2D para lectura de documentos de identificación, carnés, etiquetas y códigos impresos o digitales. Debe ser compatible como mínimo con códigos PDF417, QR, Data Matrix o equivalentes, contar con tecnología de lectura tipo área imager 2D o equivalente, conectividad USB o equivalente, diseño ergonómico y compatibilidad con la solución de gestión de visitantes, registro o control de acceso de la entidad. (Se deben suministrar 2 lectores). 3. Tabla digitalizadora de firmas con pantalla integrada de mínimo 5 pulgadas y resolución mínima de 800 x 480 píxeles, destinada a la captura electrónica de firmas manuscritas. Debe incluir lápiz óptico o stylus compatible, conectividad USB o equivalente, compatibilidad con sistemas operativos de uso común e integración con la solución de gestión de visitantes, control de acceso, registro documental o aplicaciones administrativas de la entidad. (Se deben suministrar 2 tablas digitalizadoras)				
Pasillos Motorizados para Acceso Peatonal					
17	Pasillo Lateral Pasillo motorizado tipo swing gate elaborado en aluminio, aletas en acrílico de 100 cm de altura, incluye pictogramas de flujo con leds multicolor (Paso 600/900 mm).		2		
18	Pasillo Central Pasillo motorizado tipo swing gate elaborado en aluminio, aletas en acrílico de 100 cm de altura, incluye pictogramas de flujo con leds multicolor (Paso 600/900 mm).		1		
Infraestructura y cable accesos					
19	Electroimán 600Lb con detector de apertura	UND	30		
20	Cableado periféricos accesos e intrusión	ML	1000		
21	Tubería emt 3/4	ML	500		
Mano de obra					
22	Mano de obra (debe incluir herramientas, elevadores, escaleras, andamios, etc)		1		
23	Ingeniería		1		
24	SISO		1		
Mantenimiento General a Sistemas Electrónicos de Seguridad					

25	Servicio y Logística para realizar Mantenimiento Preventivo para el <u>sistema de control de acceso Schneider - Security Expert</u> conformado por los siguientes componentes. Incluye los siguientes elementos: * 10 Controladoras Security Expert ACX PCB Controller * 5 Tarjeta Expansora (XPOD) 4 salidas digitales, para ampliar la capacidad de la controladora * Software de Control de Acceso Security Expert * 1 Estación de trabajo (control acceso) * 16 Lectoras Biométricas Suprema BEW2OAP, * 41 lectoras RFI HID Access, * 26 Electroimán YALE . Incluye mantenimiento y depuración de base de datos de usuarios, actualización de políticas de acceso, verificación de accesos por huella y tarjeta. Incluye Capacitación del manejo y configuración del sistema		1		
26	Servicio y logística para realizar Mantenimiento preventivo a <u>control de incendios Notifier Honeywell</u> incluye: * 1 Panel de incendio principal NOTIFIER NFS - 320. * 86 Detectores de humo fotoeléctricos FSP-851. * 40 Detectores térmicos FST-851. * 14 Pulsadores manuales direccionables, de acción dobles rojos NBG-12LX. * 49 Parlantes estrobos NOTIFIER SPSCRL (cielo o pared) * 3 Detector de humo Tipo Beam, emisor y receptor. Verificación de todos los sensores, sirenas, luces estroboscópicas, audio evacuación, zonificación, sistema de altavoces. Incluye modulo monitor. Incluye verificación de activación de módulos detectores, mensajes de error. Incluye Capacitación del manejo y configuración del sistema.		1		

27	Servicio y logística para realizar Verificación y mantenimiento preventivo de <u>sistema de intrusión RISCO</u>. Esto incluye: * Panel de intrusión LIGHTSYS+ DE GRADO 3 CON CAPACIDAD DE 512 ZONAS, INCLUYE FUENTE DE ALIMENTACIÓN Y TECLADO LCD * KNX/Modbus Module. Gateway that enables RISCO alarm panels to communicate with systems using the KNX or Modbus protocols. * 10 Tarjeta expansora de 8 zonas CABLEADAS PARA LIGHTSYS. * 16 Fuente externa protección de ondas RJ45, CAT5E DIKET DTEKMRJPOE. * 53 Magnéticos Livianos DSC SM -200W. * 7 Botón de pánico fijo SECOLARM SS -078 * 7 Sirena de intrusión 30W interior DSC SD 30W. * 3 Teclado alarma intrusión ROKONET con sensor RPKELOWT000A. * 2 Sensor rotura de vidrio DSC AC -100 sensible a las altas frecuencias. * 40 Sensor infrarrojo de movimiento secolarm LC 100 (PIR) * 1 Sensor sísmico DSC SS-102 * 6 Sensores de puerta magnético CONTAC/TERM SCLRM SM-200Q/W. * 13 Teclado alarma de intrusión RISCO ROKONET RPKELPWT000A. Incluye verificación de funcionamiento del sistema, conectividad de software de monitoreo y alarmas, actualización de usuarios y contraseñas. Incluye Capacitación del manejo y configuración del sistema		1		
28	Servicio y logística para realizar Mantenimiento preventivo de sistema de <u>circuito cerrado de televisión HANWHA</u> compuesto por: * 25 cámaras de seguridad fijas HANWHA. * 6 cámara de seguridad Domo PTZ HANWHA. * 5 Cámara PTZ 8MP 30x con inteligencia artificial y seguimiento de objetos automático * 1 software gestor de video para HANWHA. * 1 Estación de trabajo * 2 Televisores de 55" tipo industrial 24/365 * 2 monitores de 24" * Joystick para CCTV * Mantenimiento a Rack de comunicaciones Limpieza, retiro de polvo, verificación de grabaciones, Backups de video, identificación de tiempo de grabación, parametrización del sistema para generación de alertas por pérdida de video y detección de movimiento. Incluye Capacitación del manejo y configuración del sistema.		1		

29	Mes de mantenimiento Predictivo o Correctivo (julio a diciembre 2026) de los sistemas de seguridad electrónica en jornada diurna L-V de 7:00am a 5:00pm (Soporte). Incluye un mínimo de 6 visitas mensuales de 2 horas por visita, para actualización de bases de datos de usuarios, configuración y ajustes del sistema, según necesidad. Sede principal IDEA.		6		
30	Servicio y logística para realizar Mantenimiento Preventivo/Correctivo de sistemas electrónicos de seguridad en <u>predios IDEA:</u> * Funza Cundinamarca - Casa Blanca. * 01 Monitor Samsung de 21". * 01 DVR marca: DAHUA de 8 puertos. * 07 cámaras tipo Bala. * 01 cámaras tipo Domo.		2		
31	Servicio y logística para realizar Mantenimiento Preventivo/Correctivo de sistemas electrónicos de seguridad en <u>predios IDEA:</u> * Parque Tecnológico Manantiales - Alto de las Palmas - Antioquia. * DVR 16CH1 080P 1BAHIA / 12TB H265+ 30FR S4854CH RECONOCIMIENTO FACIAL ACUSENSE METAL HIKVISION3 00229166 * DISCO DURO 4TB HDD 3.5IN 60MB5 400RPM 6GBS 256MBS PURPLEW ESTERN DIGITAL WD43PURZ * GABINETE RACK 9 U * MULTITOMA * CAMARA IP 4MP BALA H265+ DWDRD /N F2.8 IR30m IL20M SMARTH YBRID LIGHT MIC INCORPORADOIP 67 SEMIMETAL ACUSENSEH IKVISION x 5 unidades * CAMARA IP 4MP DOMO H265+ DWDRD /N F2.8 IR30m IL20M SMARTH YBRID LIGHT MIC INCORPORADOIP 67 SEMIMETAL ACUSENSE. x 2 unidades * Cable UTP Cat 5E o 6, flexible, para conectar las cámaras. * EN POSTE CABLE FO AUTOSOPORTADO 6 HILOS, FIBRA. * CONECTOR LC FUSIONLESS PARA FIBRA MONOMODO PARA CABLES 0.9 Y 0.25MM COLOR AZUL * CAJA LIU EN PLASTICO ABS PARA FIBRA ÓPTICA CAPACIDAD DE 4 ADAPT. DUPLEX SC/LC SM/MM/ ADAPTADOR FIBRA ÓPTICA PARA CAJA LIU PUERTOS DUPLEX LC-LC MONOMODO. * CONVERTIDORES DE MEDIO 10/100/1000MBPS FIBRA DUAL CONECTOR SC MONOMODO SOPORTA HASTA 20KM.		2		

	* PATCH CORD FIBRA ÓPTICA SM G652 DUPLEX LC DUPLEX A SC SIMPLEX CHAQUETA AMARILLA 2.0 MM LSZH 3M.				
32	Servicio y logística para realizar Mantenimiento Preventivo/Correctivo de sistemas electrónicos de seguridad en <u>predios IDEA:</u> * Hacienda Santa Teresa - Santa Elena - Antioquia. piso 1 : 1 panel incendio firelite ES-50X 8 sensores de humo 2 sirena estrobo de cielo 2 estación manual Piso 2: 6 sensores de humo 1 sirena estrobo cielo 1 estación manual		2		
33	Bolsa (Inmodificable)		1		

3. CONDICIONES TÉCNICAS GENERALES

Todos los bienes, componentes, licencias, equipos, periféricos, accesorios y elementos que suministre el contratista deberán cumplir, como mínimo, con las siguientes condiciones:

- Ser nuevos, originales, de primera calidad y aptos para uso institucional.
- No se aceptarán equipos, componentes, licencias o accesorios remanufacturados, reconstruidos, usados, reacondicionados o de procedencia no verificable.
- Ser compatibles con la arquitectura tecnológica existente del IDEA.
- Contar con la documentación técnica, manuales, fichas, certificados o soportes exigidos por la Entidad.
- Cumplir con las condiciones de garantía ofrecidas por el fabricante o proveedor autorizado.
- Ser instalados, configurados y puestos en funcionamiento por personal idóneo.
- Contar con soporte técnico durante la ejecución contractual.
- No afectar la operación de los sistemas existentes ni la interoperabilidad alcanzada en vigencias anteriores.

El contratista deberá validar previamente con la supervisión cualquier actividad que implique sustitución, instalación, integración, parametrización, modificación de configuración, intervención de bases de datos, acceso a plataformas, cambios en credenciales o conexión a redes institucionales.

PRECISIONES CON RESPECTO A LAS ESPECIFICACIONES TÉCNICAS

El alcance técnico allí definido se estructura bajo el enfoque de mantenimiento especializado, soporte técnico, conservación funcional y complementación puntual de los sistemas existentes, teniendo en cuenta que durante la vigencia 2025 el Instituto adelantó la actualización e implementación de componentes críticos de control de accesos, videovigilancia —CCTV— y gestión de edificios —BMS—, así como mantenimiento preventivo de los sistemas de intrusión y detección de incendios.

En consecuencia, los bienes, licencias, componentes, periféricos, servicios y actividades requeridas para la vigencia 2026 deberán garantizar compatibilidad con la arquitectura tecnológica existente, interoperabilidad con los sistemas actualmente instalados, continuidad operativa, trazabilidad, confiabilidad funcional y cumplimiento de las condiciones técnicas previstas en el Anexo Técnico No. 1 y en el estudio de mercado correspondiente.

Todos los elementos suministrados por el contratista deberán ser nuevos, originales, de primera calidad, aptos para uso institucional y compatibles con los Sistemas Electrónicos de Seguridad existentes. No se aceptarán equipos, componentes, accesorios, licencias o elementos remanufacturados, usados, reconstruidos, reacondicionados o de procedencia no verificable.

El contratista deberá disponer del personal técnico, profesional, operativo y de apoyo necesario para la correcta ejecución del contrato, incluyendo las herramientas, equipos, instrumentos de medición, elementos de protección personal, medios de acceso seguro, transporte, logística y demás recursos requeridos para cumplir las actividades de suministro, instalación, configuración, mantenimiento, soporte y puesta en funcionamiento.

Las hojas de vida, certificaciones, acreditaciones de experiencia, constancias de capacitación o documentos del personal requerido deberán ser presentados a la supervisión cuando corresponda, conforme a las condiciones establecidas en los documentos del proceso. El personal asignado deberá contar con idoneidad técnica suficiente para intervenir sistemas electrónicos de seguridad multimarcas, incluyendo plataformas y componentes asociados a control de accesos, CCTV, intrusión, detección de incendios, BMS, gestión de visitantes y demás sistemas relacionados.

Disponer del personal con titulación técnica, tecnológica o profesional en ingeniería electrónica, ingeniería eléctrica, ingeniería de sistemas o afines, con mínimo un año de experiencia en labores relacionadas con el objeto del contrato, además de contar con las certificaciones por parte de los fabricantes que avalen la idoneidad del personal para intervenir los sistemas electrónicos en funcionamiento, entre las cuales se pueden encontrar:

- **Certificación Schneider – SmartStruxure Building Operation WorkStation and System Design**
- **Certificación Schneider – SmartStruxure Building Operation BACnet with b3 devices**
- **Certificación Schneider – EBO 2023: Engineering.**
- **Certificación Schneider – EcoStruxure Security Expert Engineering.**
- **Certificación Schneider – Ecostruxure Building: SmartX Engineering 3.x.**
- **Certificación Honeywell – Entrenamiento Plataforma CLSS Connected Life Safety Services**
- **Certificación NOTIFIER Honeywell – NOTIFIER ONYX UNIVERSITY LATIN AMERICA**
- **Certificación NOTIFIER Honeywell – NFS-320, NFS2-640 & NFS-3030 Fire Alarm Control Panels**
- **Certificación Suprema – Certificación Intermedia BioStar 2 (Español)**
- **Certificado Hanwha – Video Profesional, curso de formación autorizado por Hanwha Vision ofrecido a través del Centro de Aprendizaje de Hanwha Vision.**

Nota_1: El instituto cuenta con equipos de las marcas Schneider Electric, Notifier Honeywell, Risco, Suprema, por lo tanto, se solicitará las certificaciones respectivas de todos los fabricantes incluyendo la del nuevo sistema CCTV de la marca Hanwha, que acrediten la capacitación del personal para la intervención de los sistemas.

Nota_2: Los certificados deben estar actualizados según las condiciones de fabricante o en su defecto se debe presentar constancia que acredite inscripción de su personal técnico y de ingeniería para próximas actualizaciones de capacitaciones dentro de la vigencia 2026.

Nota_3: Es importante señalar que el personal certificado en cada una de las marcas debe encontrarse vinculado a la empresa que presente la propuesta mediante contrato laboral o de prestación de servicios. Los oferentes que no logren demostrar la vinculación del personal certificado no será tenido en cuenta dentro del proceso de evaluación, por este criterio.

El contratista deberá garantizar que cualquier intervención sobre los sistemas existentes se realice de manera controlada, coordinada con la supervisión y sin afectar la operación normal del Instituto. Para ello, deberá validar previamente las actividades que impliquen instalación, sustitución, configuración, integración, parametrización, acceso a plataformas, modificación de bases de datos, cambios de credenciales, intervención de redes, pruebas de alarmamiento o ajustes sobre sistemas en operación.

El IDEA, por razones de necesidad del servicio, seguridad institucional, austeridad del gasto público, conveniencia técnica y disponibilidad presupuestal, podrá solicitar ajustes, priorizaciones, supresiones o modificaciones dentro del marco del objeto contractual, siempre que dichas actuaciones se encuentren debidamente justificadas, no alteren la naturaleza del contrato y se ajusten a las condiciones legales y contractuales aplicables.

El contratista deberá cumplir las políticas, lineamientos y procedimientos definidos por el IDEA en materia de seguridad de la información, protección de datos personales, confidencialidad, control de accesos lógicos, gestión segura de credenciales y coordinación con las áreas responsables de tecnología y ciberseguridad, especialmente cuando las actividades involucren registros de acceso, datos biométricos, imágenes de videovigilancia, logs, usuarios, perfiles, bases de datos o información sensible.

Garantizar que el personal técnico cumpla con los respectivos uniformes de caracterización, así mismo que porten la respectiva identificación de la empresa y los carnés de afiliación al Sistema de Seguridad Social actualizado.

El recibo a satisfacción de los bienes, servicios, instalaciones, configuraciones, mantenimientos o soportes ejecutados estará condicionado a la verificación por parte de la supervisión del cumplimiento de las especificaciones técnicas, pruebas funcionales, compatibilidad, interoperabilidad, evidencias, informes y entregables establecidos en el ANEXO TÉCNICO No. 1, el estudio de mercado, el contrato y demás documentos del proceso.

En caso de discrepancia entre las condiciones técnicas generales contenidas en los Estudios Previos y las especificaciones detalladas en el Anexo Técnico No. 1, prevalecerán aquellas que garanticen mayor claridad, suficiencia técnica, compatibilidad, seguridad, continuidad operativa y adecuada ejecución del objeto contractual, siempre dentro del marco del presupuesto, objeto y alcance del proceso.

4. COMPATIBILIDAD E INTEROPERABILIDAD

El contratista deberá garantizar que los bienes, licencias, componentes y servicios suministrados sean compatibles e interoperables con los Sistemas Electrónicos de Seguridad existentes en el IDEA.

La interoperabilidad deberá verificarse, como mínimo, frente a los siguientes componentes:

- Sistema de control de accesos.
- Plataforma de administración de accesos.
- Sistemas de autenticación mediante tarjeta, biometría u otros mecanismos definidos.
- Sistema de videovigilancia —CCTV—.
- Software de gestión de video.
- Sistema de detección de incendios.
- Sistema de intrusión.
- Sistema de gestión de edificios —BMS—.
- Bases de datos, licencias, estaciones de operación, controladores, periféricos y dispositivos asociados.

Durante 2025 se incorporaron e integraron componentes como Security Expert, Automation Server, controladoras ACX, integración biométrica Suprema, módulo KNX/Modbus, cámaras Hanwha y licenciamiento WAVE, por lo que cualquier componente o servicio requerido en 2026 deberá preservar dicha arquitectura y no generar afectaciones operativas.

5. CONTROL DE ACCESOS Y AUTENTICACIÓN

El contratista deberá ejecutar las actividades relacionadas con el sistema de control de accesos, incluyendo suministro, instalación, configuración, integración, mantenimiento, pruebas y soporte técnico de los componentes requeridos.

Este frente podrá incluir, de acuerdo con el estudio de mercado y las necesidades definidas por la Entidad:

- Lectoras de tarjetas.
- Tarjetas o credenciales de acceso.
- Lectoras biométricas o faciales.
- Electroimanes.
- Cableado de periféricos.
- Tubería, canalización y elementos de instalación.
- Configuración de usuarios, perfiles, horarios, permisos y reglas de acceso.
- Verificación de eventos y trazabilidad.
- Capacitación sobre operación y administración básica del sistema.

Las actividades deberán ejecutarse garantizando que los mecanismos de autenticación queden correctamente integrados con la plataforma de control de accesos existente y que los eventos generados puedan ser consultados, auditados y trazados por el personal autorizado del IDEA.

6. SISTEMA DE GESTIÓN DE VISITANTES

El contratista deberá suministrar, instalar, configurar, parametrizar, integrar y poner en funcionamiento la solución de gestión de visitantes y contratistas, conforme a las condiciones técnicas y funcionales requeridas por el IDEA.

La solución deberá permitir, como mínimo:

- a. Registro de visitantes y contratistas.
- b. Administración de datos básicos de ingreso.
- c. Configuración de usuarios, roles y perfiles.
- d. Generación de registros o trazabilidad de ingreso.
- e. Operación desde puntos de portería o dispositivos autorizados.
- f. Integración funcional con el sistema de control de accesos, cuando aplique.
- g. Soporte técnico, capacitación y acompañamiento durante la puesta en marcha.

Este frente podrá incluir licenciamiento de servidor, licencias de portería, licencias móviles, tabletas, cámara web, lector de códigos, tabla digitalizadora de firmas, servicios de soporte, parametrización, capacitación, actualizaciones y soporte técnico remoto, según el alcance definido por la Entidad.

ESPECIFICACIONES TÉCNICAS DEL SISTEMA DE GESTIÓN DE VISITANTES

6.1. Objeto de la Solución

La Institución requiere una solución de software integral para la administración, control y trazabilidad de visitantes, contratistas, proveedores, periodistas, personal externo y demás usuarios autorizados, que permita optimizar los procesos de seguridad física, recepción y control de acceso en todas sus sedes.

La solución deberá incorporar funcionalidades para el registro automatizado de visitantes mediante lectura de documentos de identificación, captura fotográfica, verificación biométrica, asignación de credenciales, programación de visitas y generación de reportes, garantizando la trazabilidad completa de los movimientos de las personas dentro de las instalaciones.

La plataforma deberá operar de forma autónoma o integrada con el sistema de control de acceso físico implementado por la Institución, permitiendo el intercambio automático de información entre ambas soluciones.

La herramienta deberá fortalecer la gestión de seguridad en porterías y recepciones, especialmente en entornos con altos volúmenes de visitantes, contratistas y personal externo, mediante procesos ágiles, confiables, auditables y alineados con estándares modernos de seguridad y tecnología.

La solución deberá permitir su integración, como mínimo, con sistemas de control de acceso físico y plataformas de analítica de video.

Asimismo, deberá soportar implementaciones bajo esquemas multisede, con bases de datos centralizadas, distribuidas o híbridas, garantizando la sincronización de la información entre todas las sedes de la Institución.

6.2. Características Generales de la Solución

La solución deberá cumplir, como mínimo, con las siguientes características:

- Registro y control de visitantes, contratistas, proveedores, periodistas y demás usuarios externos autorizados.
- Programación anticipada de visitas individuales, masivas o recurrentes.

- Automatización de procesos de portería, incluyendo gestión de visitantes, equipos, correspondencia, llaves y novedades operativas.
- Operación mediante porterías fijas, porterías móviles y/o esquemas combinados.
- Gestión de credenciales temporales mediante tarjetas de proximidad, códigos QR, biometría u otros mecanismos autorizados por la Institución.
- Administración de alertas, restricciones y listas de control definidas por la Institución.
- Trazabilidad histórica de visitantes, destinos visitados, tiempos de permanencia y eventos asociados.
- Generación de indicadores, estadísticas y reportes exportables.
- Administración de perfiles especializados para áreas de seguridad, salud y administración.
- Operación en ambientes de alta disponibilidad.
- Configuración de cierre automático de visitas.
- Registro de visitas con múltiples destinos.
- Compatibilidad con esquemas de autenticación biométrica y credenciales físicas.
- Gestión centralizada de la información para una o múltiples sedes.

La solución podrá incluir módulos de contingencia sanitaria, permitiendo la aplicación de encuestas médicas, administración de restricciones temporales y generación de alertas institucionales cuando la operación así lo requiera.

6.2.1. Módulos y Funcionalidades Requeridas

La solución deberá incluir como mínimo los siguientes módulos:

6.2.2. Módulo de Control de Visitantes

Gestión integral del registro, seguimiento, control de ingreso y salida de visitantes.

6.2.3. Módulo de Control de Contratistas

Administración de contratistas, validación documental, seguimiento de órdenes de servicio y control de vigencia de aportes al Sistema de Seguridad Social.

6.2.4. Módulo de Minuta Digital

Registro en tiempo real de novedades, eventos, incidencias operativas y cambios de turno.

6.2.5. Módulo de Verificación Biométrica

Validación de identidad mediante huella dactilar u otros mecanismos biométricos compatibles.

6.2.6. Módulo de Lectura de Documentos de Identidad

Captura automática de información contenida en cédulas de ciudadanía colombianas, tanto en formatos antiguos como vigentes.

6.2.7. Módulo de Lectura de Pasaportes

Lectura automatizada de información contenida en pasaportes nacionales y extranjeros.

6.2.8. Módulo de Registro y Control de Equipos

Control del ingreso y salida de equipos, herramientas y elementos mediante lectura de códigos de barras u otras tecnologías compatibles.

6.2.9. Panel de Control Centralizado

Interfaz de administración para la visualización consolidada de eventos, visitas activas, alertas e información operacional.

6.2.10. Módulo de Reportes

Generación y exportación de informes en formatos PDF y Excel.

6.2.11. Módulo de Consultas

Generación de consultas personalizadas sobre la información almacenada.

6.2.12. Módulo de Programación de Visitantes

Gestión de preagendamiento, reservas, autorizaciones y seguimiento de visitas.

6.2.13. Módulo de Habeas Data

Captura de firma digital para autorización del tratamiento de datos personales de conformidad con la normatividad vigente.

6.2.14. Módulo de Órdenes de Servicio

Creación, administración y seguimiento de órdenes de servicio asociadas a contratistas.

6.2.15. Módulo de Gestión Extendida

Funcionalidades avanzadas para integración con centros de costo, dependencias y bases de datos de empleados.

6.2.16. Módulo de Control de Llaves

Administración, préstamo, devolución y trazabilidad de llaves institucionales.

6.2.17. Módulo de Impresión de Escarapelas

Generación e impresión de credenciales y escarapelas en impresoras térmicas.

6.3. Requerimientos de Infraestructura

6.3.1. Servidor

La solución deberá permitir su instalación en un único servidor o en un servidor independiente de las estaciones de registro ubicadas en porterías o recepciones, garantizando condiciones adecuadas de seguridad, disponibilidad y desempeño.

6.3.2. Base de Datos

La aplicación deberá ser compatible con motores de bases de datos PostgreSQL y SQL Server, soportando altos volúmenes de información y transacciones. La Institución podrá seleccionar cualquiera de estas plataformas sin requerir desarrollos adicionales o personalizaciones específicas.

6.3.3. Arquitectura

La solución deberá soportar arquitecturas cliente-servidor e implementaciones multisede bajo esquemas centralizados, distribuidos o híbridos, garantizando la sincronización permanente de la información entre todas las sedes.

6.4. Integración con el Sistema de Control de Acceso Físico

La solución deberá integrarse de forma nativa con el sistema de control de acceso físico implementado por la Institución.

Como mínimo deberá permitir:

- Sincronización permanente de empleados, funcionarios, visitantes, niveles de acceso y grupos de acceso.
- Asignación de credenciales temporales a visitantes.
- Asociación de visitantes con tarjetas de proximidad y/o credenciales biométricas.
- Registro automático en el sistema de control de acceso de los datos del visitante.
- Trazabilidad completa de los movimientos realizados durante la visita.
- Visualización de eventos de acceso en los registros de ambos sistemas.
- Apertura de puertas, torniquetes o molinetes según los permisos asignados.
- Control de acceso únicamente a las áreas autorizadas.

- Cierre automático de visitas al momento de la salida física del visitante.
- Liberación automática de credenciales para futuras asignaciones.
- Inhabilitación automática de tarjetas al finalizar la visita.
- Control Antipassback para evitar el uso indebido o transferencia de credenciales.
- Administración de fechas de expiración de credenciales temporales.
- Sincronización de niveles de acceso especiales para visitantes.

6.5. Registro y Gestión de Visitantes

La solución deberá permitir:

- Lectura automática de cédulas colombianas mediante lectores 2D.
- Registro manual cuando no sea posible realizar captura automatizada.
- Captura fotográfica obligatoria mediante cámara web.
- Registro de nombres, apellidos, identificación, dirección, teléfono, empresa y demás información requerida.
- Registro y verificación biométrica mediante huella dactilar.
- Almacenamiento histórico de datos de visitantes frecuentes.
- Recuperación automática de la última visita registrada.
- Validación biométrica en visitas recurrentes para evitar suplantaciones.
- Captura opcional de firma digital para aceptación del tratamiento de datos personales.
- Registro de visitantes especiales.
- Registro de alertas, observaciones y restricciones.
- Conteo automático de visitas realizadas por una persona.
- Monitoreo en tiempo real de visitantes activos dentro de las instalaciones.

6.6. Programación y Preagendamiento de Visitas

La solución deberá permitir:

- Programación previa de visitantes.
- Programación recurrente hasta por treinta (30) días.
- Preagendamiento desde navegador web, estaciones administrativas o porterías.
- Agendamiento masivo mediante carga de archivos.
- Descarga de plantillas para cargues masivos.
- Envío automático de notificaciones y códigos QR.
- Control de visitas programadas, activas, retrasadas, cumplidas y canceladas.
- Autorización previa de visitas por funcionarios designados por la Institución.
- Restricción de ingreso a visitantes no autorizados cuando así se configure.
- Registro de observaciones e instrucciones especiales asociadas a la visita.
- Programación de visitas individuales o grupales.

6.7. Gestión de Destinos y Trazabilidad

El sistema deberá permitir:

- Definir áreas, dependencias, centros de costo y sitios de reunión.
- Asociar uno o múltiples destinos a una misma visita.
- Registrar funcionarios responsables de la atención del visitante.
- Definir límites de ocupación por área.
- Controlar tiempos máximos de permanencia.
- Generar consulta histórica de ubicaciones visitadas.
- Identificar funcionarios, dependencias y áreas más visitadas.
- Realizar trazabilidad completa de visitantes dentro de las instalaciones.

6.8. Gestión de Contratistas

La solución deberá permitir:

- Registro y control de ingreso y salida de contratistas.
- Administración de órdenes de servicio.
- Validación de documentación requerida.
- Control de vigencia de aportes a seguridad social.
- Administración de horarios autorizados.
- Configuración de restricciones específicas.
- Control de herramientas y equipos asociados a labores contratadas.
- Generación de indicadores de permanencia y frecuencia de ingreso.

6.9. Gestión de Equipos, Correspondencia y Llaves

6.10. Equipos

La solución deberá permitir:

- Registro de ingreso y salida de equipos.
- Lectura mediante códigos de barras.
- Asociación de equipos a visitantes o contratistas.
- Clasificación por tipos de equipos.
- Generación de reportes de movimientos.

6.11. Correspondencia

La solución deberá permitir:

- Registro de ingreso y salida de correspondencia.
- Seguimiento por número de guía.
- Control de transportadoras, remitentes y destinatarios.

- Consulta por sede, fecha, dependencia y estado de entrega.

6.12. Llaves

La solución deberá permitir:

- Préstamo y devolución de llaves.
- Registro de responsables.
- Control de autorizaciones.
- Consulta histórica de movimientos.

6.13. Minuta Digital

La solución deberá incluir una minuta digital que permita:

- Registro automático de eventos del sistema.
- Registro manual de novedades.
- Control de cambios de turno.
- Consulta histórica de eventos.
- Generación de informes por usuario, sede, fecha o portería.
- Seguimiento de incidentes y observaciones operativas.

6.14. Administración y Seguridad

La solución deberá incorporar:

- Administración de usuarios.
- Gestión de roles y perfiles.
- Configuración de permisos por funcionalidad.
- Habilitación o deshabilitación de módulos.
- Auditoría y trazabilidad de acciones realizadas.
- Políticas de contraseñas robustas con mínimo ocho (8) caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.
- Administración de listas de bloqueo y alertas.
- Actualización permanente de componentes del sistema.
- Cumplimiento de políticas institucionales de seguridad informática.

6.15. Operación Multisede

La solución deberá soportar:

- Operación centralizada o distribuida.
- Sincronización bidireccional de visitantes, empleados y centros de costo.
- Operación autónoma en caso de fallas de comunicación.

- Recuperación automática de información una vez restablecida la conectividad.
- Administración independiente de porterías por sede.
- Combinación de porterías fijas, móviles y kioscos.
- Consultas y reportes consolidados para toda la organización.
- Control y filtrado de información por sede.

6.16. Reportes e Indicadores

La solución deberá generar, como mínimo, los siguientes informes:

- Ingresos y salidas de visitantes y contratistas.
- Visitantes activos dentro de las instalaciones.
- Ingresos por área, dependencia, centro de costo y sede.
- Trazabilidad de visitantes y contratistas.
- Estadísticas diarias, semanales, mensuales y anuales.
- Funcionarios más visitados.
- Visitantes más frecuentes.
- Áreas y sitios más visitados.
- Horas pico de visitas.
- Visitas programadas, cumplidas, retrasadas y canceladas.
- Registros realizados por operadores o vigilantes.
- Equipos ingresados y retirados.
- Correspondencia gestionada.
- Llaves entregadas y pendientes de devolución.
- Permanencia promedio de visitantes y contratistas.
- Credenciales no devueltas.
- Alertas y bloqueos generados.
- Actividad por punto de acceso.
- Reportes de visitas por empleado, dependencia o centro de costo.
- Estadísticas de utilización de porterías.
- Control de aforos y ocupación de espacios.

Todos los informes deberán poder exportarse, como mínimo, a formatos PDF y Excel.

6.17. Licenciamiento y Compatibilidad

La solución deberá:

- Incluir todos los licenciamientos necesarios para su operación.
- Permitir el preagendamiento mediante navegador web sin requerir licencias adicionales.
- Integrarse con lectores biométricos, lectores de cédulas, lectores de códigos de barras, cámaras web, impresoras térmicas, tarjetas de proximidad, torniquetes y molinetes.

- Operar sobre la infraestructura tecnológica definida por la Institución.
- Permitir futuras ampliaciones y crecimiento funcional sin afectar la operación existente.

6.18. Documentación y Certificaciones

El oferente deberá presentar certificación emitida por el fabricante de la solución donde conste que conoce, acepta y cumple la totalidad de las especificaciones técnicas definidas por la Institución.

Asimismo, deberá suministrar la documentación técnica, manuales de usuario, procedimientos de administración y demás información necesaria para la correcta operación de la solución.

7. CONTROL PEATONAL MEDIANTE PASILLOS MOTORIZADOS

El contratista deberá suministrar, instalar, configurar, integrar y poner en funcionamiento los pasillos motorizados requeridos para el control de ingreso peatonal.

Los pasillos motorizados deberán cumplir, como mínimo, con las siguientes condiciones:

- Permitir control de flujo peatonal de ingreso y salida.
- Contar con pictogramas, señalización o indicadores de paso, según especificación técnica.
- Integrarse con los mecanismos de autorización definidos por el IDEA.
- Permitir pruebas de apertura, cierre, bloqueo y liberación.
- Contar con condiciones de operación segura.
- Permitir integración con lectoras, tarjetas, biometría o mecanismos equivalentes.
- Incluir instalación, configuración, pruebas funcionales y capacitación básica de operación.

El estudio de mercado 2026 contempla pasillos laterales y pasillo central, asociados al fortalecimiento del control peatonal y la trazabilidad de ingreso.

ESPECIFICACIONES TÉCNICAS MÍNIMAS EXIGIDAS PASILLO MOTORIZADO ULTRADELGADO DE ALTA SEGURIDAD PARA CONTROL DE ACCESO PEATONAL

ITEM	CARACTERÍSTICA	ESPECIFICACIÓN TÉCNICA EXIGIDA
1	Tipo de equipo	Pasillo motorizado tipo Speed Gate de alta seguridad, operación bidireccional inteligente, de diseño ultradelgado y arquitectura modular.

2	Aplicación	Diseñado para edificios corporativos, aeropuertos, entidades gubernamentales, banca, centros empresariales y ambientes de alto tráfico.
3	Diseño del gabinete	Gabinete ultradelgado con espesor de 150 mm por lateral en su contorno. No se aceptan equipos con dimensiones superiores.
4	Longitud del equipo	Máximo 1350 mm.
5	Altura del gabinete	Máximo 1000 mm.
6	Material estructural	Acero inoxidable AISI 304 de línea arquitectónica. Opcional AISI 316L para ambientes corrosivos.
7	Acabados	Pintura electrostática personalizada bajo estándar RAL y posibilidad de personalización estética según proyecto arquitectónico.
8	Tipo de barreras	Barreras motorizadas retráctiles en vidrio templado o acrílico de alta resistencia.
9	Espesor de barreras	Entre 8 mm y 10 mm mínimo.
10	Altura de barreras	Configurable entre 850 mm y 1800 mm.
11	Ancho de paso	Configurable entre 600 mm y 900 mm, incluyendo versión PMR para movilidad reducida.
12	Tecnología motriz	Servo motor Brushless Drive de operación continua industrial. No se aceptan motores DC ni brushless convencionales.
13	Control de movimiento	Control electrónico de aceleración y desaceleración progresiva con gestión inteligente de torque.
14	Tiempo de apertura/cierre	Configurable entre 0.5 y 5 segundos.
15	Capacidad de tráfico	Mínimo 40 personas por minuto por carril.
16	Vida útil mecánica	MCBF mínimo de 12.000.000 de ciclos certificados.
17	Nivel de ruido	Inferior a 55 dB durante operación normal.
18	Alimentación eléctrica	110 – 240 VAC autosensing.
19	Consumo energético	Máximo 280W incluyendo sistema motriz.
20	Comunicación nativa	TCP/IP, RS485, RS232, contactos secos y Modbus IP integrados de fábrica.
21	Gestión remota	Configuración y monitoreo remoto vía WEB y APP desarrollada en ios y Android nativa del fabricante. Configuración de paso unidireccional, bidireccional, pánico

		monitoreo , conteo de personas, aforo , estadísticas y señales integrables al control de acceso con un dashboard inteligente de configuración remota.
22	Arquitectura de integración	Integración IP directa con plataformas de control de acceso.
23	Gestión inteligente	Parametrización remota de modos de operación, sentidos de paso y alarmas vía red IP.
24	Capacidad de almacenamiento	Mínimo 100.000 eventos en memoria local del controlador.
25	Indicadores visuales	Pictogramas LED RGB integrados.
26	Seguridad anti atrapamiento	Sistema electrónico inteligente de detección de obstrucción con reversión automática.
27	Sistema antipánico	Liberación automática del paso ante emergencia o falla eléctrica.
28	Lógica de bloqueo	Bloqueo automático para usuarios no autorizados.
29	Modos de operación	Bidireccional, unidireccional, libre, bloqueado y emergencia.
30	Protección ambiental	Protección mínima IP43 certificable. Opcional IP56.
31	Puertas batientes en acrílico de alto impacto.	Resistentes a golpes con objetos cortopunzantes y antivandálicas.
32	Representación y soporte técnico en Colombia	Stock certificado de todos los repuestos del pasillo motorizado en Colombia y partes en stock por 10 años con carta emitida directamente por el fabricante.
33	Certificaciones mínimas	CE , certificación Retie en Colombia de todos los equipos de potencia.

REQUISITOS FUNCIONALES OBLIGATORIOS

ITEM	REQUISITO FUNCIONAL	EXIGENCIA
RF-01	Gestión remota IP	Administración remota total vía red TCP/IP.
RF-02	Configuración WEB	Parametrización desde interfaz WEB sin software local.
RF-03	Gestión APP	Monitoreo y operación desde APP móvil del fabricante.
RF-04	Integración inteligente	Integración vía Modbus IP para automatización y analítica.

RF-05	Monitoreo en tiempo real	Visualización de estados y alarmas en tiempo real.
RF-06	Operación silenciosa	Ruido inferior a 55 dB.
RF-07	Bajo consumo	Modo de reposo energético automático.
RF-08	Configuración dinámica	Cambio remoto de sentidos de paso.
RF-09	Alta disponibilidad	Operación intensiva 24/7.
RF-10	Fail Safe	Apertura automática ante pérdida de energía.
RF-11	Control de acceso universal	Compatibilidad con QR, RFID y biometría.
RF-12	Gestión de tráfico	Generación de estadísticas de uso.
RF-13	Diagnóstico remoto	Detección de fallas vía plataforma IP.
RF-14	Seguridad operacional	Protección anti tailgating y anti intrusión.

CONDICIÓN DE CUMPLIMIENTO

El oferente deberá presentar matriz de cumplimiento indicando expresamente el cumplimiento de cada característica solicitada.

No se aceptarán características similares, cumplimiento parcial, integraciones mediante hardware externo, desarrollos futuros, funcionalidades en etapa beta ni adaptaciones de terceros.

La entidad podrá solicitar pruebas funcionales y validación técnica sobre integración IP, Modbus, configuración WEB y operación del sistema antes de la adjudicación.

8. SISTEMA DE VIDEOVIGILANCIA — CCTV —

El contratista deberá ejecutar actividades de suministro, instalación, configuración, mantenimiento, soporte técnico y complementación puntual del sistema de videovigilancia —CCTV— del IDEA.

Este frente podrá incluir:

- Cámaras tipo domo.
- Cámaras tipo bala.
- Licencias de grabación o gestión de video.
- Controladores, teclados o periféricos de operación.
- Monitores industriales o elementos de visualización.
- Configuración de flujos de video.
- Pruebas de transmisión, grabación y reproducción.
- Validación de alertas por pérdida de video.
- Verificación de calidad de imagen.

- Limpieza técnica.
- Revisión de almacenamiento y retención.
- Soporte sobre software o plataforma de gestión de video.

Las actividades sobre CCTV deberán preservar la compatibilidad con la infraestructura de videovigilancia instalada y/o actualizada durante la vigencia 2025, incluyendo cámaras Hanwha, licenciamiento WAVE y demás componentes asociados.

Especificaciones Técnicas Cámara Bala Exterior

CARACTERÍSTICAS DE VIDEO	
Tipo de Sensor de Imagen	CMOS o CCD
Tamaño del Sensor	Entre 1/2,8" y 2/3" o superior
Tipo de Escaneo	Progresivo
Megapíxeles en Sensor	5 Megapíxeles o superior
Iluminación mínima a Color	0.07 Lux o mejor
Iluminación mínima a Blanco y Negro	0.007 Lux ó 0 Lux con IR encendido
CARACTERÍSTICAS DEL LENTE	
Lente	Incluido
Tipo de Lente	DC auto iris
Tipo de Foco	Lente Varifocal Motorizado
Control de Foco	Enfoque Simple
Distancia Focal	3.2~10.2mm
Zoom Óptico	3.2x o Superior
CONDICIONES DE OPERACIÓN	
Dia / Noche	Filtro de Corte Infrarojo Automatico (ICR)
Leds Infrarojos	Embebidos en la cámara
Alcance de Infrarrojos	30 Mts o superior
Wide Dynamic Range	120dB Reales o Superior, No se aceptaran WDR Digitales
Filtro digital de reducción de ruido	Incluido 2D y 3D o Superior
Vista Modo Pasillo	Incluido
Corrección de Distorción de Lente	Incluido

Analíticas Incluidas	Debe permitir correr Mínimo siete analíticas de manera concurrente sin presentar bloqueo alguno o cancelación entre las mismas. Tipo de objeto clasificado: Persona / Vehículo, Atributos: Vehículo (Tipo: coche / autobús / camión / moto / bicicleta), Eventos de análisis basados en motor de IA: Detección de movimiento, Detección de objetos, Línea virtual (Cruce / Dirección), Área virtual (Merodear / Intrusión / Entrar / Salir), Eventos de análisis, Detección de desenfoque, manipulación, área virtual (aparecer / desaparecer), Inteligencia de Negocios basada en motor de IA: Recuento de personas, Recuento de vehículos, Gestión de colas, Mapa de calor
Transferencia de alarma/evento	Generado en la cámara a otras cámaras en la misma red para realizar un preset de forma automática, sin interacción de software o NVR externo
Balance de Blancos	ATW/ AWC / Exterior / Interior / Manual
Máscaras de Privacidad	Mínimo 24 Cuadrantes
Detección de Movimiento	Mínimo 8 Poligonales
Entradas de Alarma	Mínimo 1
Salidas de Alarma	Mínimo 1
Memoria	2GB RAM, 1GB Flash
CARACTERÍSTICAS DE RED	
Ethernet	RJ-45 (10/100 Base-T)
Resolución de Video	2592x1944
Compresión de Video	H.264 / H.265
Control de Bitrate	Variable (VBR) ó Constante (CBR)
Imágenes por segundo (FPS)	25fps o Superior en ambos codec de compresión
Usuarios conectados simultáneamente en unicast	20 o superior
Capacidad de Streaming de Video	Debe soportar Múltiples streaming como Mínimo 5 perfiles

Seguridad	Arranque seguro, Firmware firmado, Cifrado de firmware, Autenticación 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, Cifrado de información de autenticación de protección de datos, cifrado de compresión ZIP, Auditar el acceso de usuarios / sistema / gestión de registros de eventos, Certificado de dispositivo ID de dispositivo, Cifrado de partición de tarjeta SD de almacenamiento seguro Certificado de seguridad Seguro por defecto
ONVIF Conformance	ONVIF profile S/G/T/M y API. Se deben Incluir certificado de la pagina www.onvif.org . La certificación de Onvif debe haberse hecho con la herramienta de prueba versión 23 o superior (favor adjuntar certificación).
IP	IPv4, IPv6
Slot de Memoria	SD/SDHC/SDXC
Almacenamiento SD	Minimo 256 GB o Superior
Audio	Bidireccional
Protocolos de Audio	G.711, G.726, AAC-LC
Protocolos de Red soportados	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, CDP, SRTP (TCP, UDP Unicast)
CARACTERISTICAS DE AMBIENTE	
Temperatura máxima de operación	55°C o Superior
Protección de Ingreso	IP66 o Superior
Resistencia a Golpes	IK10 o Superior
Voltaje de Alimentación	PoE
PoE	IEEE802.3af, Class3
Consumo de potencia	PoE: máx. 12,95 W, típico 5,3 W
RESPALDOS	
Garantía	5 Años o Superior
MTBF	Mayor a 80.000 horas certificado por el fabricante
Certificados de Calidad	FCC, CE, UL, RoSH
Centro de Servicio	En Colombia, incluir certificación expedida por el fabricante

Certificación	Carta de Fabricante certificando al integrador en capacidad para instalar, configurar y realizar mantenimiento a los equipos
Restricciones de Comercialización	Las marcas ofertadas no deben presentar veto o restricciones de venta en otros países.
Certificaciones estándares y	EMC FCC 47 CFR 15 Subpart B Class A, ICES-3(A)/NMB-3(A), CE/UKCA, EN 55032 Class A, EN 50130-4, EN 61000-3-2, EN 61000-3-3 VCCI CISPR 32 Class A, RCM AS/NZS CISPR 32 Class A. Safety UL 62368-1, CAN/CSA C22.2 NO. 62368-1, IEC/EN 62471. Environment IEC/EN 63000, IEC/EN 60529 IP66, IEC/EN 62262 IK10

Especificaciones Técnicas Cámara Mini Domo Exterior

CARACTERÍSTICAS DE VIDEO	
Tipo de Sensor de Imagen	CMOS o CCD
Tamaño del Sensor	Entre 1/2,8" y 1/3" o superior
Tipo de Escaneo	Progresivo
Megapíxeles en Sensor	5 Megapíxeles o superior
Iluminación mínima a Color	0.07 Lux o mejor
Iluminación mínima a Blanco y Negro	0.007 Lux ó 0 Lux con IR encendido
CARACTERÍSTICAS DEL LENTE	
Lente	Incluido
Tipo de Lente	DC auto iris
Tipo de Foco	Lente Varifocal Motorizado
Control de Foco	Enfoque Simple
Distancia Focal	3.2~10.2mm
Zoom Óptico	3.2x o Superior
CONDICIONES DE OPERACIÓN	
Día / Noche	Filtro de Corte Infrarojo Automático (ICR)
Leds Infrarrojos	Embebidos en la cámara
Alcance de Infrarrojos	30 Mts o superior
Wide Dynamic Range	120dB Reales o Superior, No se aceptaran WDR Digitales

Filtro digital de reducción de ruido	Incluido 2D y 3D o Superior
Vista Modo Pasillo	Incluido
Corrección de Distorción de Lente	Incluido
Analíticas Incluidas	Debe permitir correr Mínimo siete analíticas de manera concurrente sin presentar bloqueo alguno o cancelación entre las mismas Tipo de objeto clasificado: Persona / Vehículo, Atributos: Vehículo (Tipo: coche / autobús / camión / moto / bicicleta), Eventos de análisis basados en motor de IA Detección de movimiento, Detección de objetos, Línea virtual (Cruce / Dirección), Área virtual (Merodear / Intrusión / Entrar / Salir), Eventos de análisis, Detección de desenfoque, manipulación, área virtual (aparecer / desaparecer), Inteligencia de Negocios basada en motor de IA: Recuento de personas, Recuento de vehículos, Gestión de colas, Mapa de calor
Transferencia de alarma/evento	Generado en la cámara a otras cámaras en la misma red para realizar un preset de forma automática, sin interacción de software o NVR externo
Balance de Blancos	ATW/ AWC / Exterior / Interior / Manual
Máscaras de Privacidad	Mínimo 24 Cuadrantes
Detección de Movimiento	Mínimo 8 Poligonales
Memoria	2GB RAM, 1GB Flash
CARACTERÍSTICAS DE RED	
Ethernet	RJ-45 (10/100 Base-T)
Resolución de Video	2592x1944
Compresión de Video	H.264 / H.265
Control de Bitrate	Variable (VBR) ó Constante (CBR)
Imágenes por segundo (FPS)	25fps o Superior en ambos codec de compresión
Usuarios conectados simultáneamente en unicast	20 o superior
Capacidad de Streaming de Video	Debe soportar Múltiples streaming como Mínimo 5 perfiles

Seguridad	Arranque seguro, Firmware firmado, Cifrado de firmware, Autenticación 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, Cifrado de información de autenticación de protección de datos, cifrado de compresión ZIP, Auditar el acceso de usuarios / sistema / gestión de registros de eventos, Certificado de dispositivo ID de dispositivo, Cifrado de partición de tarjeta SD de almacenamiento seguro Certificado de seguridad Seguro por defecto
ONVIF Conformance	ONVIF profile S/G/T/M y API. Se deben Incluir certificado de la pagina www.onvif.org . La certificación de Onvif debe haberse hecho con la herramienta de prueba versión 23 o superior (favor adjuntar certificación).
IP	IPv4, IPv6
Slot de Memoria	SD/SDHC/SDXC
Almacenamiento SD	Minimo 256 GB o Superior
Audio	Bidireccional
Protocolos de Audio	G.711, G.726, AAC-LC
Protocolos de Red soportados	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, CDP, SRTP(TCP, UDP Unicast), MQTT
CARACTERISTICAS DE AMBIENTE	
Temperatura máxima de operación	55°C o Superior
Protección de Ingreso	IP66, NEMA4X o Superior
Resistencia a Golpes	IK10 o Superior
CARACTERÍSTICAS ELÉCTRICAS	
Voltaje de Alimentación	PoE
PoE	IEEE802.3af, Class3
Consumo de Energia	PoE: máx. 12,95 W, típico 5,3 W
RESPALDOS	
Garantía	5 Años o Superior
MTBF	Mayor a 80.000 horas certificado por el fabricante
Certificados de Calidad	FCC, CE, UL, RoSH, EAC, NDAA
Centro de Servicio	En Colombia, incluir certificación expedida por el fabricante

Certificación	Carta de Fabricante certificando al integrador en capacidad para instalar, configurar y realizar mantenimiento a los equipos
Restricciones de Comercialización	Las marcas ofertadas no deben presentar veto o restricciones de venta en otros países.
Certificaciones estándares y	EMC FCC 47 CFR 15 Subpart B Class A, ICES-3(A)/NMB-3(A), CE/UKCA, EN 55032 Class A, EN 50130-4, EN 61000-3-2, EN 61000-3-3 VCCI CISPR 32 Class A, RCM AS/NZS CISPR 32 Class A. Safety UL 62368-1, CAN/CSA C22.2 NO. 62368-1, IEC/EN 62471. Environment IEC/EN 63000, IEC/EN 60529 IP66, IEC/EN 62262 IK10, NEMA 250 type 4X

IP/Analog Hybrid Keyboard Controller – HANWHA - SPC-7000

CARACTERÍSTICAS OPERACIONALES	DETALLE / ESPECIFICACIÓN TÉCNICA
Pantalla LCD	Pantalla de 5" TFT touch LCD
Joystick	Joystick de 3 ejes con giro para control de zoom (3 Axis twist zoom) , desmontable para uso universal (mano derecha o izquierda)
Jog Shuttle	Control de reproducción para SSM / DVR integrado
Control de Cámaras	Soporte para funciones Pan/Tilt/Zoom, Foco, Auto foco, Preset, Grupo, Tour, Swing, Trace, Auto tracking, Alarma on/off, Congelado (Freeze)
Gestión de Video Wall	Mapeo rápido de cámara-mosaico (canal) y cambio de diseño de división de pantalla (Layout)
Gestión de Grabadores	Control de grabación/reproducción, apagado de alarmas y menú
Gestión de Dispositivos	Registro y modificación de dispositivos integrados directamente en la pantalla LCD
Gestión de Usuarios	Soporta 1 Administrador + 9 Operadores
Importación / Exportación	Importación y exportación de archivos de configuración del sistema

Captura de Video (Snapshot)	Exportación de imágenes fijas (cámaras de red) mediante memoria USB
Entrada de Texto	Entrada de caracteres alfabéticos mediante teclado virtual en pantalla
Idiomas Soportados	Inglés, Español, Francés, Italiano Alemán, Turco, Polaco, Ruso, Coreano, Chino y Japonés

CARACTERÍSTICAS DE COMUNICACIÓN Y RED	DETALLE / ESPECIFICACIÓN TÉCNICA
Equipos Controlados	Cámaras de red (IP), Cámaras análogas, DVRs y software SSM
Capacidad de Unidades a Controlar	• Cámaras de red: Máx. 255 unidades
	• SSM: 1 unidad
	• Cámaras Análogas / DVR: Máx. 255 unidades
	• 1 puerto Ethernet (para cámaras de red)
Interfaces de Conexión	• 1 puerto USB para conexión a SSM
	• 1 puerto USB para actualización, importación/exportación de configuración y captura de imágenes
	• 1 puerto RS-485/422 para cámaras análogas y DVR
	• 1 puerto RS-485/422 para conexión en cascada entre controladores
	• SUNAPI (para equipos de red/IP)
Protocolo de Interfaz	• Protocolo dedicado (SSM)
	• Protocolos análogos: SRD, Pelco-D/P, Panasonic, Vicon, AD, Honeywell, Bosch, Elmo, GE, Samsung-T/E
	Configurable de 2,400 a 57,600 bps
Velocidad de Baudios (RS-485/422)	
Protocolos de Red Soportados	TCP, HTTP, DHCP, IPv4

CONDICIONES AMBIENTE	DE	DETALLE / ESPECIFICACIÓN TÉCNICA
Temperatura Operación	de	De 0°C a 40°C (+32°F ~ +104°F)
Humedad Operación	de	Del 20% al 85% de humedad relativa

CARACTERÍSTICAS ELÉCTRICAS	DETALLE / ESPECIFICACIÓN TÉCNICA
Voltaje Alimentación	de 12V DC
Consumo de Energía	Máximo 6.4W

CARACTERÍSTICAS MECÁNICAS	DETALLE / ESPECIFICACIÓN TÉCNICA
Dimensiones (Ancho x Alto x Profundo)	459.1 mm x 59.1 mm x 177.9 mm (18.07" x 2.33" x 7")
Peso	1.5 kg (3.3 lb)

RESPALDOS Y CERTIFICACIONES	DETALLE / ESPECIFICACIÓN TÉCNICA
Certificados Calidad	de EAC, UL Listed, CE, FC
Fabricante / Origen	Hanwha Vision CO., LTD. (Anteriormente conocida como Hanwha Techwin)

9. SISTEMA DE DETECCIÓN DE INCENDIOS

El contratista deberá realizar mantenimiento preventivo, predictivo y correctivo al sistema de detección de incendios existente en el Instituto.

Las actividades deberán incluir, como mínimo:

- Verificación del panel principal de incendio.
- Revisión de detectores de humo fotoeléctricos.
- Revisión de detectores térmicos.
- Verificación de pulsadores manuales.
- Revisión de parlantes, estrobos y elementos audiovisuales de notificación.
- Verificación de detectores tipo Beam.
- Pruebas de activación de módulos y sensores.

- h. Revisión de mensajes de error o falla.
- i. Verificación de zonificación.
- j. Validación de audioevacuación y alarmamiento.
- k. Capacitación al personal designado.
- l. Informe técnico con hallazgos, actividades ejecutadas y recomendaciones.

El estudio de mercado 2026 identifica actividades de mantenimiento preventivo sobre el sistema de control de incendios Notifier Honeywell, incluyendo panel NFS-320, detectores, pulsadores, parlantes estrobos y detectores tipo Beam.

10. SISTEMA DE INTRUSIÓN

El contratista deberá realizar mantenimiento preventivo, predictivo y correctivo al sistema de intrusión existente en el Instituto.

Las actividades deberán incluir, como mínimo:

- a. Verificación funcional del panel de intrusión.
- b. Revisión de expansores y módulos.
- c. Verificación de contactos magnéticos.
- d. Revisión de botones de pánico.
- e. Pruebas de sirenas y dispositivos de alarmamiento.
- f. Revisión de sensores de movimiento.
- g. Verificación de sensores de rotura de vidrio y sensores sísmicos.
- h. Revisión de teclados.
- i. Validación de conectividad con software de monitoreo.
- j. Actualización de usuarios, claves o parámetros, cuando aplique.
- k. Pruebas de alarmamiento.
- l. Capacitación al personal designado por el IDEA.
- m. Informe técnico con hallazgos y recomendaciones.

El estudio de mercado 2026 contempla mantenimiento preventivo al sistema de intrusión RISCO, incluyendo panel LIGHTSYS+, tarjetas expansoras, sensores, magnéticos, botones de pánico, sirenas, teclados y demás periféricos asociados.

11. INFRAESTRUCTURA, CABLEADO Y ADECUACIONES ASOCIADAS

El contratista deberá suministrar e instalar la infraestructura complementaria necesaria para la adecuada operación de los componentes incluidos en el contrato.

Este frente podrá comprender:

- Cableado para periféricos de accesos e intrusión.
- Cableado de comunicación para sistemas de incendio.

- Tubería EMT.
- Canalización.
- Puntos de conexión.
- Elementos de fijación.
- Soportes.
- Accesorios menores de instalación.
- Pruebas de continuidad.
- Marcación y organización del cableado.
- Evidencias de instalación.

Las intervenciones deberán ejecutarse bajo buenas prácticas técnicas, condiciones de seguridad, orden, limpieza, protección de la infraestructura existente y coordinación previa con la supervisión.

12. MANTENIMIENTO GENERAL DE SISTEMAS EXISTENTES

El contratista deberá ejecutar mantenimiento general sobre los Sistemas Electrónicos de Seguridad existentes, incluyendo como mínimo:

- a. Sistema de control de acceso Schneider Security Expert.
- b. Sistema de detección de incendios Notifier Honeywell.
- c. Sistema de intrusión RISCO.
- d. Sistema CCTV Hanwha.
- e. Plataformas, licencias, controladores, periféricos, racks, estaciones y componentes asociados.

Estas actividades deberán incluir verificación integral de funcionamiento, depuración de bases de datos, revisión de usuarios, actualización de políticas de acceso, revisión de grabaciones, validación de respaldos, identificación de tiempos de retención, parametrización de alertas, limpieza técnica, pruebas funcionales y capacitación.

13. SOPORTE MENSUAL Y VISITAS PROGRAMADAS

El contratista deberá prestar soporte mensual durante el periodo definido por el contrato, conforme a lo establecido en el estudio de mercado y a las necesidades del IDEA.

Este soporte incluirá, como mínimo:

- a. Visitas programadas a la sede principal.
- b. Revisión funcional de componentes críticos.
- c. Actualización o ajuste de bases de datos de usuarios.
- d. Configuración y ajustes del sistema.
- e. Atención de requerimientos operativos.
- f. Soporte a novedades del sistema.

- g. Acompañamiento técnico a la supervisión.
- h. Entrega de reporte de actividades por visita.

El estudio de mercado 2026 contempla soporte mensual para el periodo julio a diciembre de 2026, con visitas mensuales para actualización de bases de datos, configuración y ajustes del sistema, según necesidad.

14. ATENCIÓN DE PREDIOS DEL IDEA

El contratista deberá atender los predios del IDEA que cuenten con infraestructura de seguridad electrónica o requieran mantenimiento preventivo o correctivo conforme al alcance contractual.

Dentro del estudio de mercado 2026 se contemplan actividades en predios como:

- Funza, Cundinamarca — Casa Blanca.
- Parque Tecnológico Manantiales — Alto de Las Palmas, Antioquia.
- Hacienda Santa Teresa — Santa Elena, Antioquia.

Las actividades podrán incluir revisión de CCTV, DVR, cámaras, monitores, cableado, fibra óptica, racks, sistemas de detección de incendios, sensores, sirenas, estaciones manuales y demás componentes instalados en cada predio.

15. PERSONAL, HERRAMIENTAS Y SEGURIDAD EN EL TRABAJO

El contratista deberá disponer del personal técnico, profesional, operativo y de apoyo necesario para la correcta ejecución del contrato.

El personal deberá contar con la formación, experiencia y certificaciones requeridas para intervenir los sistemas electrónicos de seguridad objeto del contrato. Cuando aplique, deberá acreditarse conocimiento o certificación relacionada con las plataformas y marcas instaladas en el IDEA.

El contratista deberá disponer, por su cuenta y riesgo, de:

- a. Herramientas menores y especializadas.
- b. Equipos de medición y prueba.
- c. Escaleras, elevadores, andamios o elementos de acceso seguro.
- d. Elementos de protección personal.
- e. Uniformes e identificación empresarial.
- f. Equipos necesarios para instalación, mantenimiento y soporte.
- g. Personal SISO o responsable de seguridad y salud en el trabajo, cuando aplique.

La ejecución deberá cumplir las normas de seguridad y salud en el trabajo, prevención de riesgos, uso de elementos de protección personal y demás lineamientos definidos por el IDEA.

16. PRUEBAS, PUESTA EN FUNCIONAMIENTO Y RECIBO A SATISFACCIÓN

Todo componente suministrado, instalado, configurado o intervenido deberá ser probado antes de su recibo a satisfacción por parte de la supervisión.
Las pruebas podrán incluir, según aplique:

- a. Pruebas de encendido.
- b. Pruebas de comunicación.
- c. Pruebas de integración.
- d. Pruebas de autenticación.
- e. Pruebas de alarmamiento.
- f. Pruebas de grabación y reproducción.
- g. Pruebas de apertura y cierre.
- h. Pruebas de lectura de credenciales.
- i. Pruebas de biometría.
- j. Pruebas de generación de eventos.
- k. Pruebas de consulta de registros.
- l. Pruebas de respaldo, logs o trazabilidad, cuando aplique.

El recibo a satisfacción estará condicionado a que los bienes y servicios cumplan con las especificaciones técnicas, estén operativos, integrados, documentados y aceptados por la supervisión del contrato.

17. SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE DATOS

El contratista deberá cumplir los lineamientos del IDEA en materia de seguridad de la información, ciberseguridad, privacidad, protección de datos personales y confidencialidad. En particular, deberá:

- a. Coordinar con las áreas competentes cualquier acceso a redes, servidores, bases de datos, plataformas, usuarios o credenciales.
- b. No utilizar contraseñas por defecto.
- c. Mantener la trazabilidad de las intervenciones realizadas.
- d. Proteger la información biométrica, registros de acceso, imágenes de videovigilancia, logs y eventos.
- e. Habilitar registros de auditoría cuando aplique.
- f. Respetar los roles y perfiles definidos por la Entidad.
- g. No copiar, extraer, divulgar o modificar información sin autorización.
- h. Cumplir los acuerdos de confidencialidad exigidos por el Instituto.

Las actividades deberán ejecutarse evitando la generación de vulnerabilidades, pérdida de información, indisponibilidad de servicios, afectación de integridad de datos o accesos no autorizados.

REQUISITOS DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

El Contratista como parte integral de los servicios o productos entregados deberá cumplir con lo siguiente:

- ✓ Implementar y mantener durante toda la ejecución del contrato las medidas técnicas, administrativas y organizativas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información del IDEA.
- ✓ Implementar una arquitectura de alta disponibilidad que garantice la continuidad de la solución.
- ✓ El proveedor deberá entregar un diagrama técnico detallado de la arquitectura implementada, incluyendo infraestructura, aplicaciones, componentes, integraciones, flujos de comunicación y conexiones relevantes. Así mismo, deberá identificar los controles de seguridad y ciberseguridad implementados para la protección de la plataforma, con el fin de permitir la adecuada validación, gestión y seguimiento de la arquitectura por parte del IDEA.
- ✓ El proveedor deberá entregar el inventario actualizado de los activos de información asociados a la solución implementada, incluyendo datos, archivos, bases de datos, servidores, dispositivos y demás componentes relacionados. Dicho inventario deberá contener como mínimo: dirección IP, nombre del activo, especificaciones técnicas del dispositivo (marca, referencia, versión y hoja de datos técnica, cuando aplique), ubicación, así como los controles de seguridad y ciberseguridad implementados para su protección.
- ✓ Proveer las condiciones de ciberseguridad y privacidad de la información para asegurar la protección de los datos de los usuarios, estableciendo estándares de seguridad robustos que cumplan con la ley 1581 de protección de datos personales.
- ✓ La solución debe permitir la creación de roles y perfiles, que permita la segregación de funciones.
- ✓ La solución debe permitir la integración con el Directorio Activo del IDEA.
- ✓ En caso de requerir acceso a la infraestructura del IDEA durante la implementación, el contratista debe utilizar los mecanismos definidos por la Dirección de TI y la Dirección de Ciberseguridad para que se garantice la seguridad de la información.

- ✓ El contratista debe dejar habilitados los logs de eventos, auditoría, seguridad y acceso a la solución.
- ✓ La solución debe garantizar la Integración con el SOC (centro de operación de seguridad) a través de mecanismos como SYSLOG u otro mecanismo estándar que garantice el envío de los logs requeridos.
- ✓ En las configuración y parametrizaciones de los sistemas configurados, el CONTRATISTA deberá garantizar en el momento de la entrega que:
 - Que la información clasificada como reservada (confidencial), incluyendo datos biométricos se encuentre cifrada tanto en tránsito, como en reposo utilizando estándares internacionalmente reconocidos, como AES 256 o RSA, asegurando la protección adecuada frente a accesos no autorizados.
 - El sistema de autenticación biométrica facial que se implemente deberá utilizar tecnología basada en templates biométricos faciales (plantillas biométricas), evitando el almacenamiento de imágenes faciales originales de los usuarios en la solución, con el fin de garantizar que la información biométrica no pueda ser reconstruida, replicada o utilizada de forma no autorizada. Adicionalmente, los templates biométricos deberán almacenarse cifrados utilizando estándares criptográficos robustos y mecanismos de protección de privacidad de datos.
 - Garantizar el cifrado de la base de datos de los templates de registro facial utilizando AES de 256 bits o un estándar criptográfico equivalente o superior.
 - La solución debe utilizar protocolo de comunicación en tránsito TLS 1.2 y en reposo AES-256 o superior entre sus componentes.
 - Los dispositivos deben manejar a nivel de hardware la funcionalidad de tampering (eliminar la información en caso de que el dispositivo sea retirado o removido de la pared o molinete o sea violentado).
 - El sistema de reconocimiento facial deberá contar con detección de vida (liveness detection) para garantizar que la autenticación se realiza con una persona real y prevenir suplantaciones mediante fotos, videos u otros medios.
 - Los relojes de los sistemas involucrados deben estar sincronizados con la hora oficial suministrada por el Instituto Nacional de Metrología de Colombia.
 - Habilitar sólo los protocolos, puertos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios.
 - Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura.
 - Dejar establecido el tiempo máximo de inactividad, después del cual se debe dar por cancelada las sesiones en los sistemas, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.
 - Asegurar que ningún componente de la solución quede con las contraseñas por defecto. Es fundamental que todos los accesos estén configurados con credenciales



seguras, siguiendo buenas prácticas de seguridad como el múltiple factor de autenticación (MFA).

- ✓ Al finalizar el contrato, deberá entregar toda la información recolectada al supervisor y garantizar la eliminación segura de toda la información y datos personales tratados, mediante técnicas de borrado seguro certificables.
- ✓ Aceptar y cumplir con las cláusulas establecidas en el formato “F-SSI-SPC-001 Formato Acuerdo de Confidencialidad y Privacidad – Proveedores
- ✓ Garantizar a largo plazo el soporte, mantenimiento y actualización de versiones de la herramienta.
- ✓ Definir el Acuerdo de Nivel de Servicio (ANS) establecido entre el IDEA y el proveedor, conforme al formato F-SSI-SPC-002 Formato ANS IDEA, en el marco del contrato de prestación de servicios, así como brindar soporte y asesoría técnica para atender las solicitudes relacionadas con el funcionamiento de la plataforma, garantizando la resolución oportuna de incidentes, dudas y requerimientos, con el fin de mantener la plataforma en óptimas condiciones de operación.
- ✓ El proveedor deberá garantizar que todo el licenciamiento objeto del presente contrato sea expedido, registrado y entregado a nombre del IDEA, incluyendo las credenciales, certificados, derechos de uso y demás documentos asociados, asegurando que la entidad figure como titular legítimo de las licencias adquiridas

18. CAPACITACIÓN

El contratista deberá capacitar al personal designado por el IDEA en la operación básica, administración funcional, buenas prácticas de uso, recomendaciones de mantenimiento y manejo de los sistemas o componentes intervenidos.

Las capacitaciones deberán documentarse mediante:

- Actas.
- Listados de asistencia.
- Material de apoyo, cuando aplique.
- Certificados o constancias de capacitación, si se requieren.

19. INFORMES Y ENTREGABLES

El contratista deberá entregar a la supervisión, según corresponda, los siguientes documentos:

- a. Plan de trabajo.
- b. Cronograma de actividades.
- c. Informes técnicos de mantenimiento.
- d. Reportes de soporte.
- e. Actas de visita.
- f. Evidencias fotográficas.
- g. Registros de pruebas funcionales.
- h. Relación de equipos suministrados.
- i. Relación de seriales, licencias o credenciales, cuando aplique.
- j. Certificados de puesta en funcionamiento.
- k. Actas de capacitación.
- l. Recomendaciones técnicas.
- m. Informe de hallazgos.
- n. Informe final de ejecución.

Los informes deberán presentarse de manera clara, organizada y con evidencias suficientes para verificar la actividad ejecutada, el estado de los sistemas intervenidos y las recomendaciones técnicas correspondientes.

20. GARANTÍA Y SOPORTE

El contratista deberá garantizar la calidad de los bienes, componentes, licencias, servicios, instalaciones, configuraciones e intervenciones ejecutadas.

Cuando se suministren equipos, licencias o componentes, estos deberán contar con las garantías de fabricante o proveedor autorizado, sin perjuicio de las garantías contractuales exigidas por el IDEA.

El contratista deberá atender las novedades, defectos, inconsistencias o fallas atribuibles a la instalación, configuración, suministro o intervención realizada durante la ejecución contractual y durante el periodo de garantía aplicable.

21. CONDICIONES DE RECIBO

La supervisión del contrato verificará que los bienes y servicios ejecutados cumplan con:

- a. Las especificaciones técnicas mínimas.
- b. El estudio de mercado.
- c. El presente Anexo Técnico.
- d. Las condiciones del contrato.
- e. Las instrucciones impartidas por la supervisión.
- f. Las pruebas funcionales requeridas.
- g. La documentación y evidencias de soporte.

El IDEA podrá abstenerse de recibir bienes, servicios o actividades que no cumplan las condiciones técnicas exigidas, que presenten fallas, que no sean compatibles con la infraestructura existente o que no cuenten con los soportes requeridos.

22. RESULTADO ESPERADO

Con la ejecución de las actividades previstas en el presente Anexo Técnico, el IDEA espera mantener operativos, disponibles, confiables, interoperables y soportados sus Sistemas Electrónicos de Seguridad durante la vigencia 2026, conservando la arquitectura tecnológica intervenida durante la vigencia 2025 e incorporando únicamente los complementos puntuales requeridos para fortalecer el control de ingreso, la gestión de visitantes, la autenticación, la videovigilancia, la detección de incendios, la intrusión, el soporte técnico y la atención de predios institucionales.