Superintendencia de Notariado y Registro

GRUPO No. 3 REGIONAL CENTRO
ANEXO CONDICIONES TECNICAS ESENCIALES-FCTE PARA EL SERVICIO DE VIGILANCIA CON MEDIOS NO REGULADOS.

OBJETO: ***PRESTAR, A TRAVÉS DE MEDIO HUMANO CON ARMAS, SIN ARMAS, CON APOYO DE MEDIOS TECNOLÓGICOS: CCTV, ALARMA MONITOREADA, SISTEMAS DE COMUNICACIÓN, CENTRAL DE MONITOREO, RECEPCIÓN Y CONTROL DE ACCESO, SCANNER DE RAYOS X, DETECTORES DE METAL Y BIOMETRICOS,, EL SERVICIO DE VIGILANCIA Y SEGURIDAD PRIVADA PARA LA PROTECCIÓN DE LOS MUEBLES E INMUEBLES DE CARÁCTER PROPIO, EN COMODATO Y/O EN ARRENDAMIENTO, A CARGO DE LA SNR, NIVEL CENTRAL, DELEGADA DE TIERRAS, ALMACÉN, BODEGA DE FUNZA, EDIFICIO SAN MARTÍN Y LAS 195 OFICINAS DE REGISTRO DE INSTRUMENTOS PÚBLICOS A NIVEL NACIONAL, ASÍ COMO PARA LOS FUNCIONARIOS, CONTRATISTAS, USUARIOS Y DEMÁS PERSONAS QUE PERMANEZCAN EN LAS INSTALACIONES DE LA ENTIDAD***

1.1. ALCANCE DEL OBJETO

En el marco del contrato se prestarán los servicios para la regional Centro, de acuerdo con la siguiente distribución:

DEPARTAMENTO	NOMBRE DE LA ORIP O SEDE DE LA SNR	DIRECCIÓN SEDE	AREA M²
BOGOTÁ, D.C.	BOGOTÁ ZONA NORTE Y DIRECCIÓN REGIONAL CENTRO	Calle 74 No. 13 - 40/42/44	3954,19
BOGOTÁ, D.C.	BOGOTÁ ZONA SUR	CALLE 45ª SUR # 52C – 71 BARRIO VENECIA - DIAGONALl 45 SUR No. 50-78	2152,64
BOGOTÁ, D.C.	BOGOTÁ ZONA CENTRO	Calle 26 No. 13 - 49 Local 102 Oficina	2512,68
BOYACÁ	CHIQUINQUIRÁ	CARRERA 48 24-30 LOCAL 1	358
BOYACÁ	EL COCUY	Calle 7 No. 3 - 47 / 49	270
BOYACÁ	GUATEQUE	Calle 9 No. 7 - 46	314
BOYACÁ	MONIQUIRÁ	Calle 8 No. 4 - 93	335,44
BOYACÁ	PUERTO BOYACÁ	Carrera 2 No. 8 - 50/52/56	300
BOYACÁ	RAMIRIQUÍ	Calle 5 No. 6 - 21	316,35
BOYACÁ	SANTA ROSA DE VITERBO	Calle 7 No. 3 - 14	472,4

BOYACÁ	SOATÁ	Calle 10 No. 3 - 21/41	464,3
BOYACÁ	SOCHA	Carrera 3 No. 8 - 40	134,86
BOYACÁ	TUNJA	Carrera 2 #40-10	739
BOYACÁ	DUITAMA	Carrera 19 No. 16-33-37 EDIFICIO LAS MERCEDES local 101	428
BOYACÁ	GARAGOA	CARRERA 10 No. 11-64/66/68	580,5
BOYACÁ	MIRAFLORES	CLUB SOCIAL MIRAFLORES	539
BOYACÁ	SOGAMOSO	CARRERA 12 No. 10-14	625,65
CUNDINAMARCA	AGUA DE DIOS	Calle 13 No. 10 - 31	201
CUNDINAMARCA	CHOCONTÁ	Calle 6 No. 5 - 26	246
CUNDINAMARCA	FACATATIVÁ	Carrera 2 No. 6 - 59 Bancolombia Piso 2 Oficina 201 y Piso 3 Oficina 301	563,68
CUNDINAMARCA	FUSAGASUGÁ	Calle 18B No. 19 - 31 Barrio Piedragrande	626
CUNDINAMARCA	GACHETÁ	Calle 4 No. 4 - 51	256
CUNDINAMARCA	GIRARDOT	Calle 18 -No. 9 - 95	415,1
CUNDINAMARCA	GUADUAS	Carrera 4 No. 2 - 58	220
CUNDINAMARCA	LA MESA	Carrera 21A No. 8 - 96	353,99
CUNDINAMARCA	LA PALMA	Calle 5 No. 5 - 56-62	199,55
CUNDINAMARCA	PACHO	Carrera 15 No. 7 - 31/37/39	265,82
CUNDINAMARCA	UBATÉ	Calle 8 No. 8 - 22 - CALLE 8 No.8- 24	297,62
CUNDINAMARCA	ZIPAQUIRÁ	Carrera 10 No. 1 A - 11/13	811,95
CUNDINAMARCA	CÁQUEZA	Carrera 1 No.2-64 PLAZA DE MERCADO "HOY LA TRIADA"	200
CUNDINAMARCA	SOACHA	CALLE 14 N° 7-56	1.163,00
HUILA	GARZÓN	Calle 5 No. 8 - 55/57	476,00
HUILA	LA PLATA	Calle 5 No. 4 - 38 Palacio de Justicia - Cra. 5No. 5-40	97,57
HUILA	NEIVA	Calle 6 No. 3 - 63/66 Local 2 y mezzanine, Local 3, Local 4 y mezzanine, Local 5 y mezzanine, Garaje 23, Garaje 24	724,00
HUILA	PITALITO	CARRERA 2 Y 3 Y CALLE 15 Y 17 OFICINA 201 F, 201 G, 201 H, 201 I, 201 J, 201 K, 201 L, ESPACIO 66 V - SALON, 201W	313,38
N. SANTANDER	CHINÁCOTA	Calle 4 No. 3 - 60	295,00
N. SANTANDER	CONVENCIÓN	Calle 5 No. 7 - 23/27	246,81
N. SANTANDER	CUCUTA	Avenida 0 No. 9 - 30	1.336,00

N. SANTANDER	OCAÑA	Calle 12 No. 11 - 63	419,84
N. SANTANDER	PAMPLONA	Calle 6 No. 5 - 78 Local 2, Local 3, Piso 2	255,44
N. SANTANDER	SALAZAR DE LAS PALMAS	Calle 2 No. 5 - 28 Barrio Centro	101,00
N. SANTANDER	CACHIRA	Calle 6 No. 5-21	130,00
SANTANDER	BARICHARA	Calle 6 No. 7 - 82	155,00
SANTANDER	BUCARAMANGA	Carrera 20 Calle 34 - 01	2.363,62
SANTANDER	CHARALÁ	Carrera 17 No. 24 - 91/95	798,00
SANTANDER	CONCEPCIÓN	Carrera 4 No. 5 - 73/75	287,85
SANTANDER	CONTRATACIÓN	Carrera 4 No. 3 - 49	147,00
SANTANDER	PIEDECUESTA	Carrera 6 No. 8 - 82 Local 101, 102 Y 103 - CARRERA 15 No. 3A N 10 LOCAL 315 A	506,36
SANTANDER	PUENTE NACIONAL	Carrera 6 No. 7 - 29	509,66
SANTANDER	SAN ANDRÉS	Carrera 4 No. 16 -18 -20 - B	275,09
SANTANDER	SAN GÍL	Calle 14 No. 9 - 55 Unidad 4	201,41
SANTANDER	SAN VICENTE DE CHUCURÍ	Carrera 9 No. 10 - 41	132,86
SANTANDER	SOCORRO	Carrera 14 No. 13 - 12	664,89
SANTANDER	VÉLEZ	Calle 9 No. 2 - 57 y 2 - 51	491,25
SANTANDER	BARRANCABERMEJA	CALLE 48 No. 1-01 / CARRERA 1 #48-08	216,17
SANTANDER	MÁLAGA	Calle 11 #11-93	505,00
SANTANDER	ZAPATOCA	CALLE 23 #8-50	350,50
TOLIMA	AMBALEMA	Carrera 1A No. 9A - 60	160,00
TOLIMA	CAJAMARCA	Calle 6 No. 8 - 32/34/36	158,34
TOLIMA	CHAPARRAL	Carrera 10 No. 9 - 31	303,28
TOLIMA	EL ESPINAL	Calle 9 No. 5 - 59 Edificio Escobar Rivera Local 4, Oficina 107 y108	61,21
TOLIMA	FRESNO	Calle 5 No. 6 - 42 / 50	226,00
TOLIMA	GUAMO	Carrera 9 No. 6 - 42	219,00
TOLIMA	HONDA	Calle 11 No. 13A - 71 Paseo Bolivar	295,17
TOLIMA	IBAGUÉ	Avenida del Ferrocarril No. 42 - 97 / No. 42 - 111	2.391,36
TOLIMA	LÍBANO	Carrera 9 No. 3 - 27	215,12
TOLIMA	MELGAR	Calle 6 No. 26 - 52/54	305,07
TOLIMA	PURIFICACIÓN	Carrera 4 No. 7 - 20 / 24 /28	243,96
TOLIMA	ARMERO	Calle 6 No. 6-45	299,89

CUNDINAMARCA	FUNZA - GALICIA	Bodega 5 Manzana B Parque Industrial Galicia	2.441,33
CUNDINAMARCA	FUNZA - CELTA	AUTOPISTA MEDELLIN KM 7 BG 148	3.900,00
BOGOTA	TORRE SAN MARTÍN	CARRERA 7 No. 32 12 - Pisos 11-28-33-34-35	2500,6
BOGOTA	ALMACÉN GENERAL	Calle 22 C # 31-35	721
BOGOTA	CASA DE TIERRAS	Carrera 17 No. 38 - 16 Barrio La Magdalena	439,7
BOGOTA	SEDE NIVEL CENTRAL	CALLE 26 No. 13-49 interior 201	4.500,00

Nota: La Superintendencia de Notariado y Registro, podrá solicitar la adición del servicio objeto del contrato para nuevas sedes, debiendo el contratista mantener el valor del servicio para las unidades adicionales. Así mismo la SNR podrá realizar sin costo adicional el cambio en la dirección de la prestación del servicio para lo cual deberá informar con mínimo 30 días de antelación.

2.COMPONENTES DEL SERVICIO A CONTRATAR

2.1. MEDIOS TECNOLÓGICOS

Los medios tecnológicos de apoyo que se requieren para la prestación del servicio de vigilancia y seguridad privada se clasifican en las siguientes categorías. Todos los equipos ofrecidos deberán ser NUEVOS, de primer uso, vigentes en el mercado al momento de la entrega, tecnológicamente actuales y debidamente certificados con sus respectivas fichas técnicas:

- Cámaras
- NVR 8 canales (Incluye HDD)
- NVR 16 canales (Incluye HDD)
- Discos Duros 8 TB
- Alarmas monitoreadas (alarma de seguridad inteligente)
- Biométrico (Controladora – lector)
- Cámara PTZ
- Scanner Rayos X
- Arcos detectores de metales
- Torniquetes de acceso
- Sistema de control de acceso – Molinetes
- Lectoras biométricas control de acceso (Con licencia y software si aplica)
- Cámara para control de acceso (Con licencia y software si aplica)
- Enrolador Dactilar para registro (Con licencia y software si aplica)
- Equipos de cómputo recepción
- Lectores de código de barras para cédula (Con licencia y software si aplica)

Para el centro de monitoreo se requieren los siguientes medios tecnológicos:

- Computadores centrales de monitoreo
- Televisores centrales de monitoreo
- UPS central de monitoreo
- Licencias para vigilancia central de monitoreo, sistema de alarma y biométrico

- Software control de asistencia

Relación y descripción de medios tecnológicos:

Cámara de Red Fijas con Analítica Inteligente	
	Cámara de red tipo domo o bala con capacidad de imagen a color en condiciones de baja iluminación y detección inteligente mediante algoritmos de aprendizaje profundo. Debe incorporar funciones de analítica de video avanzada y protocolos de ciberseguridad integrados.
Característica	**Especificación Mínima**
Resolución	Mínimo 8 MP (4K UHD 3840 × 2160) a 20/25/30 fps; se aceptarán resoluciones superiores.
Inteligencia Artificial	Analítica en el borde (edge AI) para detección, clasificación y seguimiento de personas/vehículos, con metadatos de eventos.
Lente	Varifocal motorizada o fija, según estudio de seguridad; selección que garantice el campo de visión y DORI requerido.
Compresión de video	H.265/H.265+ y H.264; soporte de transmisión eficiente y, cuando esté disponible, AV1.
Rango Dinámico Amplio (WDR)	Mínimo 120 dB o tecnología equivalente de amplio rango dinámico.
Iluminación	Color: ≤0,01 lux o mejor; IR adaptativo o tecnología equivalente para baja iluminación.
Distancia Identificación (DORI)	Mínimo 6 m, ajustable al escenario mediante lente/campo de visión; deberá justificarse con el estudio de seguridad.
Rango de iluminación IR	Mínimo 30 m, con IR adaptativo cuando aplique.
Almacenamiento Local	Ranura microSD, mínimo 256 GB, con soporte de almacenamiento local para contingencia cuando el modelo lo permita.
Alimentación	PoE IEEE 802.3af/at o superior; alimentación auxiliar según fabricante.
Protección	IP67 para ambientes exteriores y protección IK10 cuando el riesgo de impacto lo requiera.
Funciones adicionales	Ciberseguridad del dispositivo, HTTPS/TLS, gestión de credenciales, actualización segura de firmware, audio bidireccional cuando aplique, analítica de video y conformidad ONVIF Profile T.

Cámara PTZ

	Cámara de red tipo domo PTZ con alta sensibilidad para baja iluminación y funciones de análitica e inteligencia artificial.

Característica	Especificación Mínima
Resolución	Mínimo 8 MP (4K UHD) a 25/30 fps; se aceptarán resoluciones superiores.
Zoom Óptico	Mínimo 30x; preferiblemente 31x o superior, según disponibilidad del mercado.
Zoom Digital	Mínimo 12x, con procesamiento digital del fabricante.
Compresión de video	H.265/H.265+ y H.264; soporte de transmisión eficiente y, cuando esté disponible, AV1.
Rango Dinámico Amplio (WDR)	Mínimo 120 dB o tecnología equivalente.
Iluminación	Color: ≤0,005 lux o mejor, o tecnología equivalente para baja iluminación.
Distancia Identificación (DORI)	Mínimo 200 m, de acuerdo con lente y escena; deberá acreditarse mediante ficha técnica.
Rango de iluminación IR	Mínimo 150 m, preferiblemente con IR adaptativo.
Almacenamiento Local	Ranura microSD mínimo 512 GB.
Alimentación	PoE+ / PoE++ o alimentación DC conforme a ficha del fabricante.
Protección	Mínimo IP66 e IK10 cuando el escenario requiera resistencia a impacto.
Funciones adicionales	Ciberseguridad, HTTPS/TLS, actualización segura de firmware, audio bidireccional, analítica AI en el borde, seguimiento automático y ONVIF Profile T.

NVR 16 Canales con Inteligencia Artificial	
	
Característica	**Especificación Mínima**
Canales	16 canales IP, con posibilidad de ampliación o integración mediante VMS cuando aplique.
Resolución máxima de entrada	Mínimo 32 MP por canal/entrada conforme a arquitectura del fabricante.
Capacidad de Decodificación	Mínimo 4K (8 MP) a 30 fps en múltiples canales, de acuerdo con capacidad real de decodificación.
Salidas de video	Mínimo HDMI 4K UHD y VGA; soportar salida simultánea cuando aplique.
Bahías de disco	Mínimo 2 bahías SATA para permitir configuración de almacenamiento redundante o ampliada.
Interfaz de Red	Mínimo 1 × RJ-45 Gigabit Ethernet; preferible 2 × Gigabit para separación de redes/gestión cuando aplique.
Compresión de Video	H.265/H.265+ y H.264; AV1 cuando sea soportado por el fabricante.

Ancho de banda	Mínimo 384 Mbps de entrada, o superior según número de cámaras y resolución requerida.
Puertos de Conexión	Mínimo USB 3.0 y puertos suficientes para periféricos de operación.
Interoperabilidad	ONVIF Profile T y soporte de perfiles compatibles con las cámaras suministradas.
Almacenamiento	Mínimo 8 TB, discos de grado vigilancia/empresarial, dimensionados para cumplir el periodo de retención exigido por la SNR.
Funciones Adicionales	Analítica AI, búsqueda inteligente, ciberseguridad, gestión de usuarios, auditoría de eventos, HTTPS/TLS y actualización segura de firmware.

NVR 8 Canales con Inteligencia Artificial	
	
Característica	**Especificación Mínima**
Canales	8 canales IP.
Resolución máxima de entrada	Mínimo 32 MP por entrada/arquitectura del fabricante.
Capacidad de Decodificación	Mínimo 8 MP (4K UHD) a 30 fps en los canales definidos por el fabricante.
Salidas de video	Mínimo HDMI 4K UHD y VGA.
Bahías de disco	Mínimo 2 bahías SATA, cuando el chasis lo permita; en todo caso deberá soportar el almacenamiento requerido.
Interfaz de Red	Mínimo RJ-45 Gigabit Ethernet.
Compresión de Video	H.265/H.265+ y H.264; AV1 cuando sea soportado.
Ancho de banda	Mínimo 160 Mbps, o superior según cámaras conectadas.
Puertos de Conexión	Mínimo USB 3.0.
Interoperabilidad	ONVIF Profile T.
Almacenamiento	Mínimo 8 TB, con discos específicos para videovigilancia, dimensionados al periodo de retención exigido.
Funciones Adicionales	Analítica AI, ciberseguridad, gestión de usuarios, auditoría y actualización segura de firmware.

ALARMA MONITOREADA



Descripción

- 1 Panel
- 1 Fuente de panel
- -1 Teclado
- 10 Sensores de movimiento
- 4 Contacto magnético
- 1 Sirena 30 w
- 1 Batería 12 v 7 AMP.
- 1 Botón de Pánico
- 1 Botón de pánico inalámbrico
- 1 Caja metálica.
- 1Expansor de 8 zonas

Los sitios y cantidades de los circuitos cerrados de televisión y alarmas monitoreadas serán en todas las oficinas a nivel nacional que se encuentran incluidas en la tabla de distribución.

En algunos sitios se podrá requerir únicamente el servicio de sistemas de alarma monitoreada; dicho servicio debe incluir el suministro, instalación, funcionamiento, mantenimiento y capacitación del personal designado por el contratista y por la SNR en el uso del sistema.

La ubicación de las alarmas obedecerá al resultado de los estudios de seguridad propios y aquellos solicitados al contratista.

BIOMÉTRICO (CONTROLADORA + LECTOR)	
	- Pantalla 2.8 Pulgadas TFT - Comunicación TCP/IP, USB-Host, Wi-Fi(Opcional) - Funciones Estándar SMS, Horario de Verano, Timbre Programado, Búsqueda Self-Service, Cambio Automático de Estado, Entrada T9, Foto ID, Cámara, Multi-verificación, Salida 12V, Impresión por RS232 (Cable Opcional) - Funciones Opcionales Tarjetas ID / MIFARE, Código de Trabajo, ADMS - Interfaz de Control de Acceso Cerradura Eléctrica, Botón de Salida, Alarma - Fuente de Alimentación DC 12V 1.5A - Velocidad de Velicación ≤ 1 seg **1.1. Especificaciones Técnicas Sistema Control de Asistencia (209)**  - Capacidad de Rostros 1.500 - Capacidad de Huellas 2.000 - Capacidad de Tarjetas 2.000(Opcional) - Capacidad de Eventos 100.000

ESCANER RAYOS R

	Equipo de inspección de paquetes y equipaje con tecnología de reconocimiento inteligente
Característica	**Especificación Mínima**
Tamaño del túnel	60 cm (ancho) × 40 cm (alto), como mínimo.
Carga en Transportador	Mínimo 180 kg.
Velocidad de banda	Mínimo 0,20 m/s, regulable según fabricante.
Penetración de acero	Mínimo 35 mm.
Resolución de cable	Mínimo 38 AWG o superior según certificación del fabricante.
Monitor	Mínimo 21” LED, resolución Full HD o superior.
Computador	Procesador de generación vigente, mínimo 16 GB RAM, SSD mínimo 512 GB, sistema operativo soportado por el fabricante y software de inspección con almacenamiento de imágenes/eventos.

ARCOS DETECTORES DE METALES	
	Solución avanzada de control de accesos diseñada para la prevención proactiva de riesgos y la mitigación de amenazas en puntos de alta concurrencia. Su implementación optimiza la seguridad física perimetral, garantizando un entorno corporativo protegido y un control riguroso, sin comprometer la fluidez ni la eficiencia de los procesos operativos cotidianos.
Característica	**Especificación Mínima**
Zonas de detección	Mínimo 24 zonas independientes.
Capacidad de detección	Mínimo 60 personas/minuto.
Pantalla	LCD/LED táctil de mínimo 7”, con menú de configuración y visualización de eventos.
Contadores	Contador de personas y contador de alarmas, con registro de eventos.
Indicadores de alarma	Indicadores LED por zona y alarma sonora ajustable.
Otras Funciones	Autodiagnóstico, configuración por perfiles, registro de eventos, protección contra manipulación y medidas de ciberseguridad cuando el equipo disponga de conectividad.

TORNIQUETES DE ACCESO	
	El proveedor suministrará como parte de la prestación del servicio torniquetes tipo molinete bidireccional con capacidad de integración biométrica y lector de código de barras para cédula, para las Oficinas de Registro de Instrumentos Públicos principales.
Característica	**Especificación Mínima**
Tipo	Torniquete bidireccional tipo aleta retráctil, con operación de emergencia y modo de evacuación.

Material	Acero inoxidable de uso intensivo.
MTBF	Mínimo 3.000.000 ciclos o valor certificado equivalente.
Velocidad de paso	Mínimo 20 personas/minuto.
Protección	Mínimo IPX4; protección IK según evaluación de riesgo del sitio.

SISTEMA DE PASILLO MOTORIZADO PARA CONTROL DE ACCESO	
	Solución de seguridad integrada diseñada para la automatización, fiscalización y optimización de flujos peatonales en puntos de transición críticos. El sistema articula pasillos motorizados de aleta basculante interconectados nativamente con terminales de autenticación avanzada y procesamiento centralizado.
Característica	**Especificación Mínima**
Tipo	Pasillo motorizado bidireccional de aleta abatible/retráctil, apto para control de acceso institucional.
Material	Acero inoxidable y acrílico/policarbonato de seguridad, según fabricante.
MTBF	Mínimo 3.000.000 ciclos o equivalente certificado.
Velocidad de paso	Mínimo 20 personas/minuto.
Capacidad	Mínimo 100.000 credenciales/usuarios en la solución de control, o integración equivalente con servidor/VMS.
Protección	Mínimo IPX4 y protección IK según evaluación de riesgo.
Controlador de acceso IP, mínimo 4 puertas, soporte de TCP/IP y RS-485, almacenamiento de eventos, entradas/salidas configurables y enlace con alarma de incendio.	
Lectores biométricos/tarjeta/código de barras según requerimiento, con comunicación segura y compatibilidad con la plataforma.	
Aletas motorizadas de seguridad con detección de obstáculos y desbloqueo de emergencia.	
Pantalla táctil mínima 5”, cámara cuando aplique, TCP/IP y/o Wi-Fi según diseño de red.	
12 VDC o conforme al fabricante, con protección eléctrica y respaldo mediante UPS donde aplique.	
Entradas de puerta/sensor/tamper y salidas de relé para alarma y control.	
HTTPS/TLS, gestión de usuarios/roles, registro de auditoría y compatibilidad con estándares de interoperabilidad.	

LECTORAS BIOMÉTRICAS DE CONTROL DE ACCESO (CON LICENCIA Y SOFTWARE SI APLICA9	
	Fingerprint Access Control Terminal Estructura de información de la persona: basada en la identificación del empleado • Admite el estado de asistencia 6, que incluye check in, check out, break in, break out, tiempo extra, time out out • Soporta múltiples idiomas: inglés, vietnamita, portugués brasileño, español, francés, italiano, árabe y tailandés • Accede a la red pública a través del protocolo EHome 4.0 o 5.0, y establece los parámetros de EHome en el cliente o dispositivo • Gestión integrada del control de acceso y la asistencia • Pantalla LCD de 2.4 pulgadas para mostrar la hora, la fecha y resultados de la lectura de PIN, tarjeta / huella • Teclado alfanumérico • Registra remotamente las huellas dactilares del terminal al software • Máx. 3000 usuarios, Max. 3000 huellas dactilares y max. 100,000 registros de eventos

CAMARA CONTROL DE ACCESO

	Cámara para registro fotográfico de control de acceso, mínimo 2 MP, USB 2.0/3.x o IP según arquitectura, con compatibilidad certificada con el software biométrico y capacidad de captura de rostro/documento.

ENROLADOR DACTILAR	
	Enrolador dactilar USB, sensor óptico/capacitivo de calidad institucional, resolución mínima 500 dpi, compatible con el estándar y software biométrico suministrado; incluir licencia/controlador cuando aplique.

EQUIPO DE CÓMPUTO RECEPCIÓN	
	Equipo empresarial nuevo: procesador de generación vigente con al menos 6 núcleos, 16 GB RAM, SSD NVMe 512 GB, pantalla FHD de 21,5” o superior, Gigabit Ethernet, Wi-Fi 6/6E o superior, mínimo 2 puertos USB-A y 1 USB-C, TPM 2.0, UEFI Secure Boot y Windows 11 Pro 64 bits licenciado. Incluir teclado, mouse y garantía empresarial.

LECTOR CÓDIGO DE BARRAS PARA CÉDULA (CON LICENCIA Y SOFTWARE SI APLICA)	
	Lector 2D de uso institucional, con lectura PDF417, QR y Data Matrix, conexión USB y compatibilidad con el sistema de control de acceso. Debe permitir lectura confiable de documentos de identidad colombianos y entregar licencia/software cuando aplique.

Superintendencia de Notariado y Registro

Para la verificación de este requisito, se exigirá la presentación de la ficha técnica oficial del fabricante que contenga las especificaciones técnicas de cada uno de ellos. No se requerirá la entrega de fichas técnicas para accesorios menores, conectores, consumibles o materiales complementarios destinados a la instalación, cableado, programación y/o puesta en marcha.

Nota: Estos equipos serán entregados a la Superintendencia de Notariado y Registro en calidad de comodato. En consecuencia, la totalidad de los costos y gastos relacionados con el cableado, insumos de instalación, configuración, funcionamiento, mantenimiento (preventivo y correctivo) y el reemplazo definitivo de los elementos en caso de falla o avería, correrán por cuenta y riesgo exclusivo del contratista. La distribución del numero de equipos por sede se encuentra en el ANEXO. NECESIDADES PROCESO DE VIGILANCIA Y SEGURIDAD PRIVADA SNR GRUPO 1 REGIONAL ANDINA.

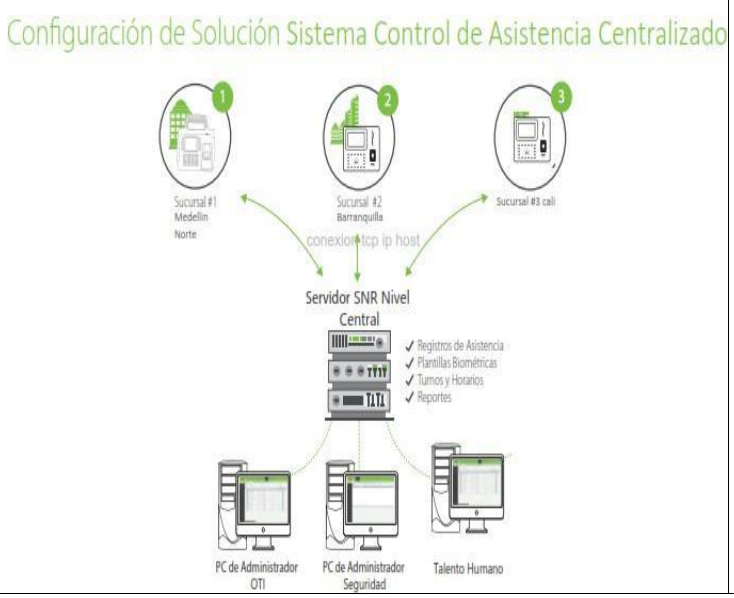
EQUIPOS CENTRAL DE MONITOREO (Especificaciones Mínimas)

EQUIPO DE COMPUTA CENTRAL DE MONITOREO	
	Estación de trabajo empresarial para operación 24/7: procesador de generación vigente con mínimo 8 núcleos y aceleración de IA/NPU cuando esté disponible, 32 GB RAM, SSD NVMe 1 TB, GPU dedicada o integrada apta para decodificación simultánea de video 4K según número de cámaras, doble salida de video 4K, Gigabit Ethernet, Wi-Fi 6E/7 cuando aplique, TPM 2.0, UEFI Secure Boot, Windows 11 Pro 64 bits licenciado y garantía empresarial. La capacidad deberá dimensionarse al VMS y al número de flujos simultáneos.

MONITOR CENTRAL DE MONITOREO	
	Monitor profesional para operación 24/7; tamaño mínimo 43”; panel LED/LCD profesional; resolución 3840×2160 (4K UHD) o superior; 60 Hz o superior; brillo y contraste adecuados para sala de monitoreo; entradas HDMI y/o DisplayPort; altavoces integrados o salida de audio; montaje VESA y soporte de pared.

UPS CENTRAL DE MONITOREO	
	UPS en línea de doble conversión, dimensionada a la carga real de la central de monitoreo, con capacidad suficiente para equipos críticos, bypass, regulación de voltaje, protección contra sobretensiones, monitoreo de estado y comunicación USB/SNMP o equivalente. Autonomía mínima recomendada: 15 minutos a carga crítica, salvo que el estudio eléctrico determine otra capacidad. Debe permitir integración con planta eléctrica cuando exista.

Superintendencia de Notariado y Registro

LICENCIA PARA VIGILANCIA CENTRAL DE MONITOREO, SISTEMA DE ALARMA Y BIOMETRICO	
	Se requiere que permitan operar la central de monitoreo, el sistema de alarma y sistema biométrico para la prestación del servicio de seguridad de la SNR.

SOFTWARE CONTROL DE ASISTENCIA

Disponer de los mecanismos y recursos de un servidor para la instalación del Sistema Control de Asistencia centralizado, con el fin de mantener la información a disposición del usuario final, este servicio de control de asistencia quedará en el nivel central (OTI).

Especificaciones y Licencias

Sistema/Arquitectura	Servidor / Web (Nube Privada)
Dispositivos Compatibles	**Dispositivos Compatibles con el software y la marca que se adquiera en calidad de comodato**
Capacidad de Dispositivos	300 en un servidor. Ilimitado en multi-servidor.
Base de Datos Compatible	PostgreSQL (Default), MS SQL Server 2005/2008/2012/2014/2016/2019, MySQL5.0.54 / Oracle10g/11g/12c
Sistema Operativo Compatible	Windows 64-bit (Windows 8/8.1/10 / Windows Server 2008/2008 R2/2012/2012 R2/2014/2016)
Tipo de Servidor	Físico / Virtual / Nube (Amazon AWS)
Navegadores Recomendados	Chrome, Firefox, IE

Requisitos de Hardware (Servidor OTI)

Dispositivos		Hasta 200	Hasta 300
Procesador		Intel, 6 núcleos @ 3.4GHz	Intel, 8 núcleos @ 3.6GHz
RAM requerida			
RAM		8-16GB DDR4	16-32GB DDR4
Almacenamiento	Mínimo 1000 GB de espacio libre. Partición NTFS. SSD recomendado.		

Superintendencia de
Notariado y Registro

Debe contar con una plataforma web para la gestión de todo el escenario operativo, administrativo y estratégico de la empresa de monitoreo de alarmas. Esto significa que el proponente debe suministrar un centro de monitoreo en las instalaciones de su empresa y suministrar un espejo en las instalaciones de la SNR.

Debe reunir todas las informaciones de monitoreo asociadas a los reportes técnicos, operativos administrativos, gerenciales y estratégicos. El sistema de monitoreo debe tener integrado el sistema de video y alarmas.

La plataforma de monitoreo tiene que permitir la operación “espejo” a la SNR a nivel nacional sin costo adicional de licencias. La tecnología de monitoreo tiene que estar integrada con los más diversos sistemas de monitoreo de imágenes de mercado.

La plataforma de monitoreo tiene que estar integrada a sistemas de monitoreo de imágenes (modelos de dispositivos de video actualmente disponibles en el mercado). Debe permitir a través de una interfaz única el monitoreo de alarmas y video, permitiendo la grabación de imágenes de forma automática, asociadas a eventos de alarmas.

Características:

- Permitir ver las imágenes en vivo de las cámaras asociadas a las áreas de las oficinas en donde se genere el evento.
- Realizar la grabación automática en la central de monitoreo cuando se produzca el evento.
- El software deberá permitir la visualización de imágenes grabadas.
- Permitir ver las diferentes disposiciones de grupos de cámaras en “n” pantallas distintas de acuerdo con la configuración apropiada para un seguimiento integral del evento en el cliente.
- Permitir la generación de eventos de “ronda virtual”, recogiendo todas las cámaras de las Oficinas de Registro de Instrumentos Públicos y sedes de la Superintendencia de Notariado y Registro, de acuerdo con el programa establecido “SERVICIO 24 HORAS”.

Nota 1: Los sitios y cantidades de los circuitos cerrados de televisión y alarmas monitoreadas y control de asistencia serán en todas las oficinas a nivel nacional que se encuentran incluidas en la tabla de distribución.

Nota 2: En algunos sitios se podrá requerir únicamente el servicio de sistemas de alarma monitoreada; dicho servicio debe incluir el suministro, instalación, funcionamiento, mantenimiento y capacitación del personal designado por el contratista y por la SNR en el uso del sistema. La ubicación de las alarmas obedecerá al resultado de los estudios de seguridad propios y aquellos solicitados al contratista.

2.2. PERSONAL DE VIGILANCIA Y SEGURIDAD PRIVADA

Con el fin de garantizar la protección integral de las personas, bienes muebles e inmuebles, infraestructura física e información en las sedes de la Superintendencia

de Notariado y Registro a nivel nacional, se determinó la estructura del componente de personal requerida. La distribución detallada del servicio se consolida en el ANEXO. NECESIDADES PROCESO DE VIGILANCIA Y SEGURIDAD PRIVADA SNR GRUPO 1 REGIONAL ANDINA, la cual especifica la cantidad de servicios requeridos por la Entidad, la modalidad operativa (con o sin arma y modalidad horaria) y el número exacto de personas requeridas por puesto de trabajo para el correcto cumplimiento del objeto contractual. La Superintendencia de Notariado y Registro, podrá solicitar la adición del servicio objeto del contrato para nuevas sedes. El contratista deberá mantener el valor del servicio para las unidades adicionales.

2.2.1. DOTACIÓN MÍNIMA DE LOS PUESTOS DE SERVICIO DE LA SNR

Para el servicio de vigilancia y seguridad privada se requiere que cada uno de los guardas de seguridad y equipo de apoyo cuenten con una dotación mínima por cada uno de los servicios requeridos:

- Lockers individuales, uno por puesto.
- Directorio telefónico de acuerdo con las necesidades y modalidad del servicio.
- Puntos de control electrónico de rondas de acuerdo con el requerimiento de la Entidad, para verificar el correcto cumplimiento de las funciones de supervisión.
- Por cada entrada vehicular en el nivel central, se debe contar con un espejo cóncavo de inspección de acuerdo con los requerimientos de la entidad.
- Cajillas de seguridad de armamento en la ubicación, cantidades y calidad exigidas por la entidad.
- Tubo de descargue de armas en la ubicación, cantidades y calidad exigidas por la entidad.
- Pito metálico, por cada vigilante.
- Linternas especiales de vigilancia: Con alcance mínimo de 10 metros, con batería de repuestos, para cada uno de los puestos de vigilancia requeridos por la Entidad.
- Lámparas de emergencia
- Alarma de pánico
- Ronderos

Nota: La Superintendencia de Notariado y Registro, podrá solicitar la adición del servicio objeto del contrato para nuevas sedes. El contratista deberá mantener el valor del servicio para las unidades adicionales.

Aspectos, los cuales son de obligatorio cumplimiento por parte de los proponentes:

1. Deberán contar con una sala y/o central de monitoreo ubicada en la ciudad de Bogotá, en donde pueda comprobarse que existen los medios técnicos para prestar el servicio de alarma monitoreada, la cual deberá ser operada por personal del proponente, previa verificación de que la ubicación de esta sala y/o central de monitoreo visitada se encuentre en una sede de propiedad del proponente o de cualquiera de los integrantes del oferente plural. Se debe instalar un espejo de la central de monitoreo en la Superintendencia de Notariado y Registro para la verificación de eventos una vez iniciado el

contrato.

2. En la sala y/o central de monitoreo, los proponentes deberán demostrar que el operador de medios tecnológicos, deberá ser un concentrador industrial capaz de recibir señales telefónicas, comunicación vía internet /canal dedicado, entre otros. Los funcionarios verificarán el envió y recibo de estas señales de alarma y video.

3. Los equipos deberán ser de alta tecnología y permitir la integración de dispositivos de última generación demostrado con fichas técnicas al momento de la visita. El centro de monitoreo debe contar con las especificaciones óptimas de respaldo y seguridad como son:

- Centro de monitoreo aislado (seguridad locativa necesaria para la protección de datos, del software informático y las redes)
- Protocolo de acceso de personas externas al centro de monitoreo
- Centro de monitoreo con ventilación
- Equipos de respaldo en espacio seguro (control de acceso)
- Protocolos de respaldo correctamente definidos
- Sistema de fuentes de respaldo de la información de objeto de monitoreo
- Sistema de seguridad (software e interfaz)
- Sistema de alimentación ininterrumpida UPS o planta eléctrica.

El comité responsable de llevar a cabo la verificación técnica en dicha visita analizará en cada caso la procedencia de solicitar aclaraciones a los proponentes.

Nota 1: ESPEJO DE INFORMACIÓN EN TIEMPO REAL

Cada empresa de vigilancia y seguridad privada deberá garantizar la implementación y operación de un mecanismo tecnológico que permita realizar un espejo en tiempo real de la información generada por los sistemas de seguridad y monitoreo instalados en los inmuebles objeto del contrato, hacia la Central General de Monitoreo ubicada en la Regional Centro.

La información deberá ser transmitida de manera continua, simultánea, segura y en tiempo real, permitiendo a la Central General de Monitoreo realizar el seguimiento, supervisión y verificación de los eventos de seguridad que se presenten en las instalaciones vigiladas.

El sistema deberá permitir, como mínimo, la visualización y/o recepción en tiempo real de la información asociada a los sistemas de videovigilancia, alarmas, controles de acceso y demás dispositivos tecnológicos de seguridad que hagan parte del servicio contratado, de acuerdo con las condiciones y requerimientos técnicos definidos por la Entidad.

Cada empresa será responsable de garantizar la disponibilidad, conectividad, integridad y continuidad de la transmisión de la información, así como de contar con los equipos, licencias, software, infraestructura y demás elementos tecnológicos necesarios para asegurar el correcto funcionamiento del espejo de información durante toda la vigencia del contrato.

En caso de presentarse fallas, interrupciones o pérdida de comunicación con la Central General de Monitoreo, el contratista deberá contar con mecanismos de contingencia que permitan restablecer el servicio en el menor tiempo posible e informar oportunamente a la supervisión del contrato sobre la novedad presentada y las acciones implementadas para su solución.

2.3 CAPACITACIÓN DE POLÍGONO Y TIRO:

El contratista deberá garantizar que todo el personal de vigilancia y seguridad privada asignado a la ejecución del contrato que, de acuerdo con las condiciones del servicio, tenga a su cargo el manejo y porte de armas de fuego, se encuentre debidamente capacitado, entrenado y certificado para el desarrollo de dicha actividad, de conformidad con la normativa vigente y los requisitos establecidos por la Superintendencia de Vigilancia y Seguridad Privada.

Para tal efecto, el contratista deberá presentar, cuando sea requerido por la Entidad o por el supervisor del contrato, las certificaciones expedidas por las academias o escuelas de capacitación debidamente autorizadas por la autoridad competente, en las cuales se acredite la capacitación correspondiente. Dichas certificaciones deberán contener, como mínimo, la identificación del trabajador, el curso realizado, la fecha de realización, la intensidad horaria y el puntaje o resultado obtenido, cuando corresponda.

Durante la ejecución del contrato, el contratista deberá garantizar la capacitación y el entrenamiento permanente del personal de vigilantes y coordinadores asignados al servicio, especialmente en materia de seguridad en el manejo de armas de fuego, procedimientos operativos y prácticas de tiro, de acuerdo con la normatividad vigente.

Para tal efecto, deberá garantizar, como mínimo, las siguientes actividades:

a) Capacitación operacional:

Realizar, como mínimo una (1) vez al año, actividades de capacitación y refuerzo sobre las normas de seguridad para el manejo, porte, almacenamiento y utilización de las armas de fuego, así como sobre los procedimientos operativos aplicables al servicio.

b) Ejercicios de tiro y polígono:

Garantizar, como mínimo una (1) vez al año, la realización de ejercicios prácticos de tiro y polígono para el personal autorizado para el porte y manejo de armas de fuego, de conformidad con las disposiciones legales y reglamentarias vigentes.

El contratista deberá conservar y presentar a la supervisión del contrato los soportes que acrediten la realización de las actividades de capacitación y entrenamiento, incluyendo, según corresponda, certificados, registros de asistencia, contenidos impartidos, fechas de realización, resultados obtenidos y demás documentos que permitan verificar el cumplimiento de esta obligación.

2.4. ESPECIFICACIONES TÉCNICAS DEL SERVICIO

1. Objeto

Contratar la prestación del servicio de suministro, instalación, configuración, integración,

operación, soporte técnico y mantenimiento preventivo y correctivo de los medios tecnológicos de seguridad electrónica requeridos en las Oficinas de Registro de Instrumentos Públicos (ORIP) de la Superintendencia de Notariado y Registro (SNR), de acuerdo con las necesidades de cada regional y las condiciones particulares de las sedes incluidas en el contrato.

El servicio comprenderá los sistemas de alarma, circuito cerrado de televisión (CCTV), cámaras, sensores, paneles de control, equipos de grabación, elementos de conectividad interna, software, licencias, accesorios y demás componentes necesarios para su correcto funcionamiento. Asimismo, deberá garantizar la transmisión de eventos y la visualización en tiempo real de los sistemas desde la Central General de Monitoreo ubicada en el Nivel Central de la SNR, sin perjuicio de la organización contractual por regionales.

2. Alcance

El contratista deberá garantizar la disponibilidad, funcionamiento, continuidad, interoperabilidad y mantenimiento de los medios tecnológicos de seguridad electrónica instalados o suministrados en las ORIP objeto del contrato.

El servicio incluirá, como mínimo:

a. Suministro de equipos nuevos, instalación, configuración y puesta en funcionamiento.

b. Implementación y mantenimiento de los sistemas de alarma y CCTV.

c. Instalación del cableado estructurado y los elementos necesarios para la interconexión de los equipos, de acuerdo con las condiciones técnicas y de seguridad informática definidas por la SNR.

d. Integración de los sistemas de las ORIP con la Central General de Monitoreo del Nivel Central.

e. Grabación, almacenamiento, consulta, descarga y entrega de registros de video y de eventos.

f. Monitoreo de eventos, recepción de alarmas, notificaciones y atención de incidentes.

g. Acceso web y funcionalidades de consulta desde dispositivos móviles, conforme a los permisos y perfiles autorizados.

h. Mantenimiento preventivo y correctivo, soporte técnico y reposición de equipos cuando resulte necesaria para restablecer el servicio.

i. Entrega de informes, registros, inventarios, manuales, evidencias de mantenimiento y demás documentación relacionada con la ejecución.

j. Continuidad del servicio durante la vigencia contractual y durante el periodo de transición previsto en esta ficha.

Las cantidades, ubicaciones y características particulares de los equipos se determinarán de acuerdo con el inventario y las necesidades de cada ORIP, así como con los anexos técnicos del proceso.

3. Requisitos generales de los equipos

3.1. Los equipos suministrados por el contratista deberán tener un uso no superior a 2 años, certificando siempre que cuente con tecnología vigente, adecuados para el uso previsto y compatibles con la infraestructura tecnológica de la SNR.

3.2. El contratista deberá suministrar e instalar todos los equipos, accesorios, elementos de conexión, fuentes de alimentación, soportes, licencias y componentes requeridos para el funcionamiento integral del servicio.

3.3. Los equipos de CCTV podrán comprender cámaras, monitores, grabadores de video en red (NVR), grabadores híbridos o equivalentes (NVDR, XVR u otros compatibles con la solución implementada), discos duros y los demás elementos necesarios, de acuerdo con la tecnología instalada y las necesidades de cada sede.

3.4. Las cámaras instaladas deberán tener una resolución superior a cuatro (4) megapíxeles y permitir una visualización adecuada de las áreas objeto de vigilancia, de acuerdo con las condiciones físicas y las necesidades de seguridad de cada ORIP.

3.5. Los equipos de seguridad electrónica deberán conectarse a la red eléctrica regulada o a los sistemas de protección eléctrica disponibles y técnicamente definidos para la sede, con el propósito de reducir los riesgos derivados de variaciones de voltaje y proteger la integridad de los equipos.

3.6. El contratista deberá suministrar e instalar los racks, gabinetes, soportes y demás elementos necesarios para alojar y organizar los equipos de CCTV y sus componentes asociados, cuando se requieran.

3.7. En el piso o lugar donde se encuentre el cuarto de cableado de comunicaciones deberá organizarse y concentrarse la conectividad de los equipos de CCTV, de acuerdo con las condiciones técnicas de cada inmueble y las instrucciones de la SNR.

3.8. Los equipos deberán contar con las garantías, documentación técnica y elementos necesarios para su adecuada operación y mantenimiento durante la ejecución contractual.

4. Sistema de alarma

El sistema de alarma deberá operar de manera continua, durante las veinticuatro (24) horas del día, los siete (7) días de la semana, durante la vigencia del contrato.

Como mínimo, deberá permitir:

a. Recibir, procesar y transmitir las señales generadas por los sensores y dispositivos instalados en cada sede hacia el centro de monitoreo y la Central General de Monitoreo del Nivel Central.

b. Identificar la sede, zona, sensor o dispositivo que origine cada evento.

c. Registrar los eventos de armado y desarmado del sistema, tanto por parte del usuario autorizado como por las operaciones remotas permitidas.

d. Permitir el armado y desarmado remoto por parte de la central de monitoreo, previa autorización del usuario facultado y conforme a los protocolos de seguridad establecidos por la SNR.

e. Detectar y registrar la activación y desactivación de alarmas, identificando los sensores y zonas involucradas.

f. Permitir el bloqueo de sensores que presenten fallas técnicas desde la central de monitoreo, únicamente bajo los procedimientos autorizados, dejando el registro correspondiente y sin comprometer injustificadamente la seguridad de la sede.

g. Registrar la activación y restauración de señales de pánico.

h. Detectar y reportar aperturas, cierres, cortes de energía, batería baja, desconexión de equipos, pérdida de conectividad, pérdida de datos y activación de dispositivos antisabotaje (tamper), cuando el sistema instalado disponga de tales funcionalidades.

i. Ser compatible con la sonorización y los dispositivos de alerta que integren la solución de alarma.

j. Contar con un panel de control principal que reciba y transmita las señales generadas en las instalaciones y permita la comunicación con el centro de monitoreo.

k. Realizar pruebas de comunicación entre los dispositivos y la central, con el fin de verificar la disponibilidad del sistema y reportar oportunamente las interrupciones.

l. Mantener un historial de los eventos generados por cada sede, con identificación del tipo de evento, fecha, hora, estado y acciones realizadas.

5. Sistema de circuito cerrado de televisión (CCTV)

El sistema de CCTV deberá permitir la supervisión visual de las áreas definidas por la SNR y la consulta de imágenes en tiempo real, tanto desde la plataforma de monitoreo autorizada como desde la Central General de Monitoreo del Nivel Central.

Como mínimo, deberá cumplir las siguientes condiciones:

a. Instalar cámaras con resolución superior a cuatro (4) megapíxeles.

b. Disponer de equipos de grabación compatibles con la tecnología implementada, incluyendo NVR, NVDR, XVR u otros dispositivos equivalentes, según las características de la solución.

c. Garantizar la grabación local de video y, cuando corresponda a la tecnología instalada, audio, con almacenamiento en discos duros u otros medios técnicamente adecuados.

d. Disponer de capacidad de almacenamiento suficiente para conservar las grabaciones durante un periodo mínimo de cuatro (4) meses, de acuerdo con el número de cámaras, la resolución, la frecuencia de grabación, la configuración de compresión y las necesidades de cada ORIP.

e. Permitir la visualización en tiempo real de las cámaras cuando se presente un evento de alarma o cuando un usuario autorizado requiera consultar las imágenes.

f. Permitir la búsqueda, reproducción y descarga de grabaciones asociadas a un evento o a un rango de fechas.

g. Permitir la exportación de los registros de video en formatos compatibles, incluyendo H.264 y AVI cuando la solución implementada lo permita, o en otros formatos que garanticen su reproducción y consulta.

h. Registrar y reportar la pérdida de señal de video, desconexión de cámaras, fallas de grabación y demás eventos que afecten el funcionamiento del sistema, siempre que sean detectables por los equipos instalados.

i. Facilitar la identificación de la sede, cámara, fecha y hora correspondientes a las grabaciones consultadas o descargadas.

j. Contar con los elementos de instalación, conexión, protección, organización y soporte necesarios para garantizar el funcionamiento de la solución.

El contratista deberá dimensionar la capacidad de almacenamiento de cada ORIP de forma que se cumpla el periodo mínimo de retención de cuatro (4) meses. La capacidad no podrá establecerse exclusivamente con base en una cantidad fija de almacenamiento si esta resulta insuficiente para garantizar dicho periodo.

6. Almacenamiento y entrega de información

6.1. Las grabaciones deberán conservarse durante un periodo mínimo de cuatro (4) meses, con independencia de la regional a la que pertenezca la ORIP.

6.2. El contratista deberá entregar a la SNR las grabaciones del sistema cada cuatro (4) meses y cuando la Entidad las requiera, de acuerdo con los procedimientos y medios seguros que se establezcan.

6.3. La entrega de grabaciones deberá permitir identificar la sede, la cámara o dispositivo, el rango de fechas y horas y, cuando corresponda, el evento relacionado.

6.4. El contratista deberá garantizar que las grabaciones puedan consultarse, reproducirse y descargarse sin depender exclusivamente de la disponibilidad de un equipo o usuario de su propia organización.

6.5. Los registros de eventos del sistema de alarma deberán conservarse en la plataforma o servidor correspondiente. La solución deberá permitir la consulta histórica de los eventos por sede y rango de fechas. La capacidad deberá ser suficiente para conservar la información necesaria para el seguimiento y la trazabilidad del servicio.

6.6. El contratista deberá adoptar medidas para evitar la pérdida, alteración, eliminación no autorizada o acceso indebido a las grabaciones y a los registros de eventos.

6.7. La consulta, extracción y entrega de información deberá realizarse únicamente por usuarios autorizados y conforme a los procedimientos de seguridad y protección de la información de la SNR.

7. Conectividad, cableado e instalación

7.1. El contratista deberá suministrar, instalar, organizar y mantener el cableado estructurado requerido para el funcionamiento de los sistemas, de acuerdo con las cantidades y necesidades identificadas para cada sede y con las normas técnicas aplicables y las directrices de la SNR.

7.2. El cableado deberá mantenerse organizado, protegido mediante canaletas u otros elementos apropiados y dispuesto de forma que reduzca el riesgo de daños, interferencias, desconexiones o afectaciones a la infraestructura del inmueble.

7.3. El contratista deberá suministrar los elementos necesarios para conectar las cámaras, sensores, paneles de alarma, grabadores y demás componentes que formen parte de la solución.

7.4. La SNR proveerá el servicio de conectividad a internet y definirá los puntos IP, el acceso a la red y las condiciones de conectividad que correspondan, de acuerdo con su infraestructura y sus políticas de seguridad informática.

7.5. El contratista deberá realizar las configuraciones necesarias para aprovechar la conectividad que suministre la Entidad y garantizar la transmisión de señales hacia la Central General de Monitoreo del Nivel Central.

7.6. La central de monitoreo del contratista deberá disponer del canal de internet y de los recursos

de conectividad que requiera su propia operación, para realizar las actividades de visualización, recepción de alarmas y seguimiento de eventos. Este requisito no trasladará al contratista la provisión de la conectividad de las sedes que corresponda a la SNR, ni eximirá al contratista de sus obligaciones de integración.

7.7. Toda conexión a la infraestructura de la SNR deberá coordinarse previamente con la Entidad y cumplir sus lineamientos de seguridad informática. No se podrán instalar conexiones, dispositivos o accesos no autorizados.

8. Control web, movilidad y consulta remota

El sistema deberá disponer de herramientas de acceso web que permitan a los usuarios autorizados consultar información relacionada con el funcionamiento de los equipos y las actividades de soporte técnico.

Como mínimo, la solución deberá permitir:

a. Consultar el estado actualizado de los servicios técnicos ejecutados y en ejecución.

b. Consultar la información de las actividades de mantenimiento, atención de incidentes y novedades reportadas.

c. Consultar los eventos de armado y desarmado, las notificaciones de alarma y el histórico de eventos por rango de fechas.

d. Visualizar las cámaras en tiempo real, de acuerdo con los permisos de acceso asignados.

e. Consultar los registros y las novedades relacionadas con cada sede.

f. Disponer de funcionalidades de consulta desde dispositivos móviles compatibles, cuando así lo permitan la solución y los perfiles autorizados.

g. Gestionar perfiles y permisos diferenciados por usuario, de manera que cada persona acceda únicamente a las funciones e información que le hayan sido autorizadas.

h. Permitir la trazabilidad de las consultas y operaciones que la plataforma tenga capacidad de registrar.

La SNR podrá asignar los recursos tecnológicos y los accesos que correspondan dentro de las plataformas institucionales existentes, de acuerdo con sus políticas de seguridad informática. El contratista deberá prestar el apoyo técnico necesario para la configuración y operación de la solución dentro de los límites autorizados.

9. Gestión de eventos y asistencia desde la central de monitoreo

La solución deberá contar con mecanismos de seguimiento de eventos durante las veinticuatro (24) horas del día, los siete (7) días de la semana, durante la vigencia del contrato.

Deberá permitir el tratamiento de situaciones como alarmas que permanezcan sin armar, desarmes fuera de horario, activación de pánico, pérdida de comunicación y demás eventos definidos por la SNR.

Cuando se requiera realizar verificaciones telefónicas, el sistema deberá permitir:

a. Integración con la plataforma telefónica utilizada para el seguimiento de eventos.

b. Contacto con los números registrados y autorizados para cada sede.

c. Verificación de identidad mediante los mecanismos de autenticación establecidos.

d. Uso de mecanismos de contraseña de coacción cuando estén disponibles y hayan sido definidos en el protocolo de operación.

e. Registro de los intentos de comunicación, las respuestas obtenidas, las novedades y el cierre del evento.

f. Identificación de situaciones como teléfono ocupado, ausencia de respuesta, contraseña inválida o inconsistencia con los horarios autorizados, cuando estas funcionalidades estén habilitadas.

Los procedimientos de atención deberán ajustarse a los protocolos definidos con la SNR y no podrán limitarse al registro automático del evento: deberán contemplar las acciones de verificación, comunicación, escalamiento y seguimiento que correspondan.

10. Integración obligatoria con la Central General de Monitoreo del Nivel Central

10.1. Integración de todas las sedes

Sin perjuicio de que la contratación se estructure por regionales, el contratista deberá garantizar que los sistemas de alarma, CCTV y demás medios tecnológicos instalados en las ORIP incluidas en su contrato se integren y transmitan la información correspondiente a la Central General de Monitoreo ubicada en el Nivel Central de la SNR.

La integración deberá permitir que la Entidad cuente con una visión centralizada de los sistemas tecnológicos de seguridad electrónica de las sedes cubiertas por los contratos regionales.

10.2. Información que deberá transmitirse

La integración deberá permitir, como mínimo, la recepción y consulta de:

a. Señales de activación, desactivación, armado y desarmado de los sistemas de alarma.

b. Activación y restauración de señales de pánico.

c. Alertas generadas por sensores y dispositivos instalados.

d. Eventos de apertura y cierre, cuando se encuentren asociados a los sistemas implementados.

e. Pérdida de video, desconexión de cámaras y fallas de grabación detectables.

f. Cortes de energía, batería baja, desconexión de equipos y activación de dispositivos antisabotaje, cuando el sistema cuente con estas funcionalidades.

g. Pérdida de comunicación, interrupciones de conectividad y fallas que afecten la transmisión de señales.

h. Imágenes en tiempo real y grabaciones históricas, de acuerdo con los permisos autorizados.

i. Historial de eventos, reportes de novedades y acciones ejecutadas frente a las alertas.

10.3. Acceso y disponibilidad de la información

El contratista deberá habilitar los mecanismos técnicos necesarios para que los usuarios autorizados por la SNR puedan visualizar las cámaras en tiempo real, recibir y consultar eventos, acceder a los registros históricos y solicitar o descargar las grabaciones correspondientes.

La disponibilidad de esta información no podrá depender exclusivamente de la plataforma interna del contratista ni de la intervención de un operador suyo para cada consulta ordinaria. La SNR deberá contar con accesos y permisos acordes con sus funciones y con sus políticas de seguridad informática.

10.4. Compatibilidad e implementación

El contratista deberá verificar las condiciones técnicas necesarias para la integración con la infraestructura y las plataformas autorizadas por la SNR. Deberá suministrar, configurar y mantener los equipos, programas, licencias, interfaces y demás componentes que sean de su responsabilidad y resulten necesarios para cumplir la integración contratada.

Las actividades de conexión a la red institucional deberán coordinarse con la SNR y sujetarse a sus lineamientos de seguridad informática.

10.5. Pruebas y aceptación

Antes de dar por recibida la instalación o la integración de una sede, el contratista deberá realizar pruebas documentadas que permitan verificar, como mínimo:

a. Transmisión de señales desde la ORIP hacia la Central General de Monitoreo del Nivel Central.

b. Recepción e identificación de eventos.

c. Visualización en tiempo real de las cámaras habilitadas.

d. Consulta de grabaciones y de registros históricos.

e. Funcionamiento de las notificaciones y de los mecanismos de comunicación.

f. Operación de los perfiles y permisos de usuario.

g. Disponibilidad de las funcionalidades que correspondan a la solución instalada.

Los resultados deberán quedar registrados en un informe o acta de pruebas. Las fallas que impidan el cumplimiento de los requisitos deberán corregirse antes de la aceptación de la instalación o de la integración correspondiente.

11. Atención inmediata de eventos críticos y continuidad de la seguridad

11.1. Clasificación de eventos

Para efectos de la prestación del servicio, los eventos deberán clasificarse según su impacto en la seguridad de las personas, los bienes, las instalaciones y la continuidad de los sistemas tecnológicos.

Eventos críticos: aquellos que representen o puedan representar un riesgo para las personas, los bienes o las instalaciones, o que afecten de manera significativa el funcionamiento de los sistemas de alarma, CCTV, transmisión de señales o monitoreo, comprometiendo la detección oportuna de riesgos.

Podrán considerarse críticos, según las circunstancias, la activación de señales de pánico, la

pérdida generalizada de comunicación con una sede, la falla del sistema de alarma, la interrupción sustancial de la videovigilancia, la pérdida de grabación relevante o la desconexión de componentes esenciales.

Eventos no críticos: aquellos que no generen un riesgo inmediato ni comprometan de manera significativa la capacidad de detección y respuesta, y que puedan atenderse dentro del plazo ordinario establecido sin afectar sustancialmente la seguridad de la sede.

La clasificación deberá considerar la naturaleza del evento, el alcance de la falla y el riesgo que represente, evitando calificar como no crítico un incidente que comprometa la operación efectiva del sistema.

11.2. Atención de eventos críticos

Los eventos críticos deberán recibir atención inmediata desde el momento en que sean detectados o reportados, sin esperar el vencimiento de un plazo ordinario de mantenimiento.

La atención comprenderá, según corresponda:

a. Registrar el evento con fecha y hora de detección o reporte.

b. Informar de inmediato a la Central General de Monitoreo del Nivel Central y a los responsables definidos por la SNR.

c. Iniciar las acciones de verificación y diagnóstico remoto que sean técnicamente posibles.

d. Activar los protocolos de contingencia y escalamiento correspondientes.

e. Coordinar el desplazamiento de personal técnico cuando la situación no pueda resolverse remotamente o requiera intervención presencial.

f. Informar al supervisor del contrato o a los responsables designados sobre la naturaleza del evento, las acciones realizadas y las medidas adoptadas para reducir el riesgo.

g. Mantener el seguimiento hasta el restablecimiento del servicio o la implementación de una medida de contingencia aceptada por la SNR.

h. Documentar las causas identificadas, las actividades ejecutadas, los tiempos de respuesta y la fecha y hora de restablecimiento.

La atención inmediata implica iniciar sin demora las acciones de respuesta, diagnóstico, comunicación y mitigación. La solución definitiva deberá ejecutarse con la mayor celeridad técnicamente posible, de acuerdo con la naturaleza del incidente, sin perjuicio de los protocolos de seguridad de la Entidad.

11.3. Atención de eventos no críticos

Los eventos clasificados como no críticos deberán solucionarse en un plazo máximo de cinco (5) días hábiles, contados a partir de su reporte formal al contratista.

El contratista deberá registrar el reporte, asignar responsable, realizar las actividades de diagnóstico y reparación, y documentar la solución aplicada.

Si durante la atención se identifica que el evento afecta la seguridad o la operación esencial de los sistemas, deberá reclasificarse y atenderse como crítico.

11.4. Registro y seguimiento de incidentes

El contratista deberá mantener un registro actualizado de los incidentes y solicitudes de soporte, que incluya como mínimo:

a. Identificación de la sede y del sistema afectado.

b. Fecha y hora del reporte o detección.

c. Descripción y clasificación del evento.

d. Fecha y hora de inicio de la atención.

e. Acciones de diagnóstico, mitigación y reparación.

f. Personal responsable de la atención.

g. Comunicaciones y escalamiento efectuados.

h. Medidas de contingencia implementadas.

i. Fecha y hora de restablecimiento del servicio.

j. Evidencias de la solución y cierre del caso.

La información deberá estar disponible para consulta de la SNR y del supervisor del contrato.

11.5. Continuidad y costos de atención

El contratista deberá disponer de los recursos humanos, técnicos y logísticos necesarios para atender los eventos incluidos en el alcance contractual.

La atención de incidentes críticos, el diagnóstico, las medidas de contingencia y las actividades de reparación que correspondan a las obligaciones contratadas no podrán condicionarse al reconocimiento de costos adicionales por parte de la SNR.

12. Suministro, instalación y puesta en funcionamiento

El contratista deberá:

12.1. Suministrar los equipos nuevos y los componentes requeridos para la ejecución del servicio, de acuerdo con las cantidades y necesidades definidas para cada ORIP.

12.2. Asumir las actividades de transporte, cargue, descargue, entrega, traslado, instalación, configuración, puesta en funcionamiento y, cuando corresponda, desinstalación de los equipos.

12.3. Instalar el cableado estructurado, las canaletas, los racks, los soportes y los demás elementos requeridos para garantizar la correcta conexión y organización de los sistemas.

12.4. Desplazar el personal técnico idóneo que resulte necesario para ejecutar las instalaciones, mantenimientos y demás actividades contratadas.

12.5. Presentar al supervisor del contrato un cronograma de instalación de los equipos y medios tecnológicos, con identificación de las sedes, actividades y tiempos previstos.

12.6. Ejecutar la entrega e instalación de los medios tecnológicos durante el periodo de empalme,

sin exceder el tercer (3.er) mes de ejecución del contrato, de acuerdo con el cronograma aprobado y las condiciones de cada sede.

12.7. Brindar asesoría y formular recomendaciones técnicas sobre la ubicación de las cámaras, sensores y demás elementos, atendiendo las condiciones físicas de los inmuebles y las necesidades de seguridad identificadas.

12.8. Realizar las pruebas de funcionamiento y documentar los resultados antes de la entrega de cada instalación.

13. Integración y transmisión de información

El contratista deberá:

13.1. Garantizar la transmisión de las señales desde las ORIP incluidas en el contrato hasta la Central General de Monitoreo ubicada en el Nivel Central de la SNR.

13.2. Informar por escrito al supervisor del contrato las características de la solución de monitoreo, los mecanismos de transmisión, el lugar de recepción de las señales y los datos de los responsables de recepción y comunicación del contratista.

13.3. Configurar los sistemas para que los eventos, las alertas y las imágenes puedan ser consultados por los usuarios autorizados de la SNR, conforme a los permisos establecidos.

13.4. Coordinar con la Entidad las actividades que requieran conexión a su infraestructura de comunicaciones, acceso a la red o intervención sobre plataformas institucionales.

13.5. Mantener la compatibilidad de los sistemas con la infraestructura autorizada y realizar los ajustes técnicos que sean necesarios para cumplir las condiciones de integración incluidas en el contrato.

13.6. Ejecutar pruebas de comunicación y de integración, documentar los resultados y corregir las fallas atribuibles a la solución suministrada o instalada.

13.7. Mantener actualizada la información de los equipos, sedes y componentes integrados, de forma que la SNR pueda identificar la ubicación y el estado de los sistemas.

14. Operación y disponibilidad del servicio

El contratista deberá:

14.1. Garantizar la operación de los sistemas de alarma y CCTV durante las veinticuatro (24) horas del día, los siete (7) días de la semana, durante la vigencia contractual.

14.2. Mantener operativos los paneles de control, sensores, cámaras, grabadores y demás componentes suministrados o puestos a disposición en desarrollo del contrato.

14.3. Verificar el funcionamiento de los mecanismos de transmisión de señales y realizar pruebas periódicas que permitan identificar fallas o interrupciones.

14.4. Atender las alarmas, alertas y novedades que sean recibidas por la central de monitoreo, aplicando los procedimientos de verificación, comunicación y escalamiento correspondientes.

14.5. Mantener actualizados los registros de eventos y las actuaciones realizadas para su atención.

14.6. Informar oportunamente al supervisor sobre fallas que afecten la prestación del servicio, así como sobre las medidas de contingencia adoptadas y el tiempo estimado para el restablecimiento, cuando sea posible determinarlo.

14.7. Evitar interrupciones injustificadas de los sistemas y adoptar las medidas necesarias para reducir el impacto de las fallas.

15. Mantenimiento preventivo y correctivo

El contratista deberá:

15.1. Realizar mantenimiento preventivo de los equipos como mínimo cada tres (3) meses, dejando registro de las actividades efectuadas, los elementos revisados, los resultados y las recomendaciones técnicas.

15.2. Ejecutar las actividades de mantenimiento correctivo requeridas para restablecer el funcionamiento de los equipos y sistemas.

15.3. Atender inmediatamente los eventos críticos, de acuerdo con lo establecido en el numeral 11 de esta ficha.

15.4. Solucionar los eventos no críticos en un plazo máximo de cinco (5) días hábiles, contados a partir de su reporte formal.

15.5. Suministrar el soporte técnico necesario durante la ejecución del contrato, de acuerdo con las necesidades que se presenten.

15.6. Realizar los diagnósticos, reparaciones, ajustes y configuraciones requeridos para mantener los equipos en condiciones adecuadas de operación.

15.7. Reponer o cambiar los equipos o componentes que presenten fallas y cuya reparación no permita restablecer oportunamente el servicio, cuando corresponda conforme al alcance contractual.

15.8. Documentar las actividades de mantenimiento y entregar los informes o registros correspondientes al supervisor del contrato.

15.9. Mantener disponibles los elementos y recursos necesarios para ejecutar las labores de soporte, sin trasladar a la SNR costos diferentes de los contemplados en la propuesta económica y el contrato.

16. Grabación, almacenamiento y entrega de información

El contratista deberá:

16.1. Garantizar que la capacidad de almacenamiento de cada sede permita conservar las grabaciones durante un periodo mínimo de cuatro (4) meses.

16.2. Dimensionar los discos duros, grabadores y demás recursos de almacenamiento según la cantidad de cámaras, la resolución y la configuración de grabación, sin que ello afecte el cumplimiento del periodo mínimo exigido.

16.3. Verificar periódicamente el funcionamiento de los sistemas de grabación y alertar sobre fallas que puedan ocasionar pérdida de imágenes o reducción del periodo de retención.

16.4. Entregar a la SNR las grabaciones de todo el sistema cada cuatro (4) meses y cuando la

Entidad lo requiera, de acuerdo con las instrucciones y los mecanismos seguros definidos.

16.5. Facilitar la consulta, reproducción, búsqueda y descarga de videos relacionados con eventos o rangos de fechas solicitados por los usuarios autorizados.

16.6. Conservar los registros de eventos y permitir su consulta histórica por sede y rango de fechas.

16.7. Adoptar medidas de seguridad para proteger la integridad, confidencialidad y disponibilidad de las grabaciones y de los registros.

16.8. Atender las solicitudes de extracción o entrega de información que formule la SNR por los canales autorizados y dejar constancia de la entrega realizada.

17. Plataforma, perfiles y acceso remoto

El contratista deberá:

17.1. Disponer de una plataforma o solución tecnológica que permita la consulta de eventos, el estado de los equipos, las grabaciones y la información asociada a la prestación del servicio, de acuerdo con las características de la solución implementada.

17.2. Habilitar las funcionalidades de acceso web y consulta desde dispositivos móviles que hagan parte de la solución contratada.

17.3. Permitir la gestión de perfiles y permisos diferenciados, con el fin de que cada usuario acceda únicamente a la información y funcionalidades autorizadas.

17.4. Facilitar a la SNR los accesos y permisos necesarios para la consulta de la información correspondiente a sus sedes, respetando las políticas institucionales de seguridad informática.

17.5. Permitir la consulta del estado de las solicitudes de soporte, las actividades técnicas ejecutadas y las novedades de los equipos.

17.6. Apoyar la configuración de las plataformas institucionales existentes cuando la SNR así lo determine y dentro de los permisos autorizados.

17.7. Mantener la información actualizada y disponible durante la ejecución del contrato.

18. Personal técnico y soporte

El contratista deberá:

18.1. Disponer de personal con los conocimientos y competencias técnicas requeridos para instalar, configurar, operar, mantener y reparar los equipos objeto del contrato.

18.2. Asumir los costos de mano de obra, desplazamientos y demás recursos necesarios para cumplir las obligaciones técnicas contratadas.

18.3. Informar al supervisor del contrato los datos de contacto de los responsables de soporte, atención de incidentes y coordinación técnica.

18.4. Mantener canales de comunicación que permitan reportar fallas, hacer seguimiento a las solicitudes y escalar los eventos que requieran atención prioritaria.

18.5. Garantizar que el personal que intervenga la infraestructura tecnológica de la SNR cumpla

los procedimientos de acceso, autorización y seguridad establecidos por la Entidad.

19. Informes y documentación técnica

El contratista deberá entregar y mantener actualizada, según corresponda, la siguiente documentación:

a. Inventario de equipos instalados por sede, con identificación de tipo, ubicación y características técnicas.

b. Cronograma de instalación y evidencia de las actividades ejecutadas.

c. Informes de pruebas de funcionamiento e integración.

d. Informes de mantenimiento preventivo y correctivo.

e. Registros de incidentes, tiempos de atención, acciones ejecutadas y cierre de casos.

f. Reportes de fallas, interrupciones y medidas de contingencia.

g. Registros de entrega de grabaciones y demás información solicitada por la SNR.

h. Manuales, fichas técnicas y documentación de los equipos y componentes suministrados.

i. Información de los responsables técnicos y de los canales de atención.

j. La demás documentación necesaria para verificar el cumplimiento de las obligaciones contractuales.

Los informes deberán permitir al supervisor comprobar el cumplimiento de las especificaciones técnicas y hacer seguimiento a la continuidad y calidad del servicio.

20. Costos incluidos en la oferta económica

El proponente deberá discriminar el valor unitario del servicio de alarma y monitoreo para cada oficina, a nivel regional, incluyendo los impuestos de ley y los demás componentes económicos exigidos en el proceso.

El valor ofertado deberá contemplar los costos correspondientes a:

a. Suministro y provisión de equipos, incluidos aquellos entregados en calidad de comodato, cuando aplique.

b. Transporte, cargue, descargue, entrega y traslado.

c. Instalación, cableado, configuración, puesta en funcionamiento e integración.

d. Operación y mantenimiento preventivo y correctivo.

e. Soporte técnico, mano de obra y desplazamientos.

f. Reposición o cambio de equipos cuando corresponda conforme a las obligaciones contractuales.

g. Licencias, accesorios y componentes necesarios para la operación de la solución ofertada.

h. Desinstalación de equipos al finalizar el periodo correspondiente, conforme a la programación

acordada con el supervisor.

i. Los demás costos necesarios para cumplir integralmente las obligaciones técnicas previstas en la oferta y el contrato.

La SNR asumirá los valores correspondientes a los servicios especificados en la propuesta económica aceptada y en el contrato. No se reconocerán costos adicionales por actividades que ya estén comprendidas en las obligaciones del contratista.

21. Continuidad del servicio al finalizar el contrato

El contratista deberá garantizar la continuidad del servicio de medios tecnológicos durante un periodo mínimo de tres (3) meses posteriores a la terminación del contrato, en los términos previstos en los documentos contractuales y con el fin de evitar que el retiro de los equipos afecte la seguridad de las sedes.

La programación de la desinstalación de los medios tecnológicos deberá acordarse con el supervisor del contrato, de manera que se asegure una transición ordenada y se eviten interrupciones injustificadas del servicio.

Durante dicho periodo, el contratista deberá cumplir las condiciones de continuidad y las actividades que expresamente se hayan previsto para esa etapa, sin generar costos adicionales diferentes de los establecidos en el contrato.

El contratista deberá coordinar con la SNR la entrega de la información, las grabaciones, los registros y la documentación técnica que correspondan, así como las actividades necesarias para facilitar la transición a un nuevo proveedor o a la solución que determine la Entidad.

22. Obligaciones generales de cumplimiento técnico

El contratista deberá:

22.1. Cumplir integralmente las especificaciones técnicas, los anexos, la propuesta aceptada y las instrucciones impartidas por el supervisor dentro del marco contractual.

22.2. Garantizar que la prestación del servicio se ajuste a las necesidades particulares de las ORIP incluidas en el contrato.

22.3. Mantener la calidad, disponibilidad y funcionalidad de los equipos y sistemas suministrados o instalados.

22.4. Cumplir los protocolos de seguridad física, informática y de acceso definidos por la SNR.

22.5. Proteger la información a la que tenga acceso durante la ejecución contractual y evitar su divulgación, alteración, pérdida o utilización no autorizada.

22.6. Informar al supervisor las circunstancias que puedan afectar el funcionamiento, la integración o la continuidad de los sistemas.

22.7. Adoptar las acciones correctivas necesarias cuando se identifiquen incumplimientos o fallas atribuibles a la solución contratada.

22.8. Facilitar la supervisión del servicio y suministrar los soportes requeridos para verificar la ejecución de las actividades.

22.9. Asumir los costos que correspondan al cumplimiento de las obligaciones incluidas en su

oferta y en el contrato.

22.10. Garantizar que la organización del servicio por regionales no afecte la integración centralizada de las ORIP con la Central General de Monitoreo del Nivel Central.

23. Criterios mínimos de verificación

Para comprobar el cumplimiento de la ficha técnica, la SNR podrá verificar, entre otros, los siguientes aspectos:

ComponenteCriterio de verificación

Equipos Equipos con tecnología vigente, instalados y operativos, acordes con las especificaciones y necesidades de cada sede.

CCTV Cámaras con resolución superior a 4 megapíxeles y visualización en tiempo real.

Almacenamiento Grabaciones disponibles durante un periodo mínimo de cuatro (4) meses.

Integración Recepción de señales y visualización de las sedes en la Central General de Monitoreo del Nivel Central.

Alarmas Recepción e identificación de eventos, zonas y sensores, según la solución instalada.

Conectividad Transmisión de señales mediante la infraestructura autorizada por la SNR y cumplimiento de sus políticas de seguridad informática.

Acceso web y móvil Consulta de eventos, históricos y funcionalidades habilitadas para usuarios autorizados.

Mantenimiento preventivo Ejecución como mínimo trimestral, con evidencia documental.

Eventos críticos Inicio inmediato de las acciones de atención, diagnóstico, comunicación y mitigación.

Eventos no críticos Solución en un máximo de cinco (5) días hábiles desde el reporte formal.

Informes Entrega de inventarios, registros de eventos, soportes de mantenimiento y demás documentos exigidos.

Continuidad Cumplimiento de las condiciones contractuales de continuidad y transición al finalizar el contrato.

El supervisor podrá solicitar las pruebas, informes, registros y evidencias que resulten necesarios para comprobar el cumplimiento de las especificaciones y obligaciones técnicas.

24. Consideraciones finales

Las especificaciones de esta ficha deberán interpretarse de manera integral con los demás documentos del proceso de selección, el anexo de cantidades y necesidades por ORIP, la propuesta económica aceptada y el contrato que se suscriba.

La solución tecnológica deberá dimensionarse de acuerdo con las necesidades de cada sede, sin perjuicio de los requisitos mínimos obligatorios establecidos en este documento. En particular, el contratista deberá garantizar la retención de grabaciones por cuatro (4) meses, la integración de

todas las ORIP contratadas con la Central General de Monitoreo del Nivel Central y la atención de incidentes conforme a los plazos definidos.

La integración centralizada constituye una condición técnica transversal a los contratos regionales y deberá mantenerse durante la ejecución del servicio, de forma que la SNR pueda ejercer las funciones de consulta, monitoreo y seguimiento que le correspondan desde el Nivel Central.

3.CONTROL EXTERNO DEL SERVICIO:

El contratista debe garantizar la supervisión externa de los puestos de vigilancia donde se prestará el servicio con medio humano, sin costo adicional para la Superintendencia de Notariado y Registro, la cual debe ser realizada por personal idóneo que debe estar plenamente identificado con el emblema de la empresa, contar con su respectivo vehículo y equipo de comunicación.

- **Procedimiento para atención del servicio no conforme**:

El contratista deberá presentar dentro de los tres (5) días siguientes a la suscripción del contrato para aprobación del supervisión el procedimiento para atender los reclamos del servicio por parte de la Superintendencia de Notariado y Registro.

- **Procedimiento de investigación por pérdidas**:

El contratista velará por la custodia y cuidado de los bienes a él encomendados. En caso que ocurra daño o siniestro por hurto o pérdida de los mismos, en las dependencias donde la compañía de vigilancia presta el servicio y para efectos de determinar la omisión, negligencia, impericia o falta de vigilancia o falla en los medios tecnológicos y custodia por parte del contratista, se llevará a cabo una reunión entre los supervisores del contrato designado por la Superintendencia, el coordinador del servicio y un funcionario del área donde ocurrió el hecho; de dicha reunión se suscribirá un acta con los hechos acaecidos y la consecuente falta de vigilancia y custodia por parte del contratista, si es del caso. Corresponderá al contratista demostrar la existencia de factores imposibles de resistir o prever para exonerarse de la responsabilidad por pérdidas o daños.

Suscrita el acta anterior, y si en la misma se estableció la falta de vigilancia o falla en los medios tecnológicos y custodia de la empresa de vigilancia, ésta deberá reponer los bienes en un término no mayor a treinta (30) días calendario, contados a partir de la fecha de recibo de la comunicación expedida por el supervisor del contrato.

4. RESTITUCIÓN DE PÉRDIDAS.

En caso de establecerse la responsabilidad de la vigilancia en la pérdida o daño por parte del contratista, éste deberá reponer el bien con las características y condiciones iguales o superiores a las del bien hurtado o dañado, sin que implique para la Superintendencia pago alguno por el costo del bien objeto de reposición; los supervisores del contrato realizarán el ingreso de dicho bien a través del

almacén general y equipo de inventarios de la SNR.

El contratista deberá reponer o reparar el bien perdido o dañado dentro de un término de treinta (30) días calendario, contado a partir de la fecha de suscripción del acta en la cual quedó demostrado la responsabilidad de la empresa de vigilancia, previo a la respectiva investigación y debido proceso.

5. ESTUDIO DE SEGURIDAD DE LOS BIENES MUEBLES E INMUEBLES DE LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.

La Superintendencia de Notariado y Registro a través del estudio de seguridad requiere de un instrumento básico para determinar vulnerabilidades de las diferentes sedes con las cuales cuenta, dicho estudio se debe presentar a los sesenta (60) días hábiles después de firmado el acta de inicio, para tal fin, se requiere que el proponente para el desarrollo del estudio de seguridad cumpla con los siguientes requerimientos.

A. Seguridad Física:

1. Determinar la ubicación, tamaño y características físicas de la sede
2. Señalar los peligros locales que pueden ser causado a su alrededor y terreno donde se ubica.
3. Señalar las investigaciones de seguridad que se han realizado, incluyendo fecha y dependencia que las condujo, incluyendo las acciones correctivas que se tomaron.
4. Disposición de la sede (anexe como pruebas: Cartas, croquis y fotografías que muestren el área, tipos y ubicación de los edificios, vías de penetración hacia o desde la instalación, así como también si hay instalaciones de ferrocarriles y muelles.

B. Barreras Perimétricas:

1. Tipo de barreras, incluir la altura y si tiene o no protección superior.
2. ¿Forman parte del perímetro edificaciones altas? (Edificios o extensiones de agua), y si es así, ¿Qué medidas de protección se emplean?
3. ¿Están las instalaciones dotadas de servicios públicos? (Teléfonos, agua, luz, etc) ¿Y las ventanas y puertas exteriores, apropiadamente protegidas?).
4. ¿Se usan alarmas eléctricas, electrónicas o dispositivos, para descubrir intrusos en el perímetro? Si las hay, descríbalas.
5. ¿Se usan letreros de advertencias en el perímetro? Si los usan, especifique el tamaño y la ubicación (incluya un dibujo o fotografía a escala como prueba).

C. Entradas:

1. Especifique el número, tipo y ubicación de portones (puertas principales en la periferia), para vehículos o peatones.
2. Horas en que están abiertos los portones.
3. Portones inactivos y ocasiones en las cuales se usan éstos.
4. Tipo de dispositivos de cierre en los portones.
5. Ubicación de las llaves para los dispositivos de cierre.
6. ¿Está en operación un sistema de control de llaves?
7. ¿Están los portones activos, apropiadamente iluminados, para que el

guardia pueda inspeccionar los pases y los ocupantes o el contenido de los vehículos que entren o salgan de la instalación.

D. Alumbrado:

1. Descripción, método, ubicación de control y las instalaciones de energía disponibles.
2. ¿Están separados, el sistema de alumbrado para protección y el sistema de alumbrado para trabajo?
3. ¿Hay una fuente auxiliar de energía para el alumbrado protector? Si lo hay, ¿de qué tipo y capacidad?
4. ¿Están las luces controladas por un sistema mecánico o son estas operadas manualmente?
5. ¿Qué alumbrado de emergencia hay disponible?

E. Áreas restringidas:

1. Número, tamaño y ubicación de las áreas restringidas.
2. Grado de restricción en cada una.
3. ¿Están las áreas restringidas separadas independientemente? Si esto es así, ¿qué tipo de separación se usa?
4. ¿Se mantiene una lista de control de acceso, para las personas autorizadas a entrar?
5. ¿Se utiliza alarma electrónica o dispositivos, para descubrir intrusos?

F. Control de Entrada:

1. Sistema de identificación para el personal asignado, empleados y obreros (incluya muestra de la tarjeta o placas, o ambas).
2. Antecedentes y clasificación del personal.
3. Control y emisión de identificaciones (describa brevemente).
4. Pérdida de la identificación (describa el sistema de control).
5. Control de los visitantes (describa el sistema de: registro, placas, escoltas).
6. Control de los vehículos de vendedores, incluyendo los conductores y ayudantes.
7. Procedimiento de registro y control, para los vehículos de propiedad privada.
8. Número de estacionamientos, dando: ubicación, si están cercados, alumbrados y vigilados.

NOTA IMPORTANTE:

El contratista será responsable de realizar la instalación y puesta en funcionamiento de los medios tecnológicos requeridos, de acuerdo con las necesidades operativas de cada sede. Para tal fin, la ubicación exacta de los equipos deberá contar con la validación previa del supervisor de la Dirección Regional o del funcionario que este designe en la respectiva sede. Asimismo, el contratista deberá atender oportunamente las solicitudes y requerimientos formulados por la supervisión, y ejecutar un plan de mantenimiento periódico que garantice el óptimo estado, funcionamiento permanente y operatividad de la totalidad de los equipos instalados, asegurando así el cumplimiento efectivo de la cobertura requerida por la Entidad y la finalidad del servicio contratado.

2. El contratista deberá contar, para la ejecución del contrato, con un (1) coordinador para la operación del servicio de vigilancia de la SNR y un (1) coordinador de medios tecnológicos,

quienes deberán tener la experticia requerida para atender la operación y dar solución oportuna y de fondo.

El coordinador de la operación del servicio será el encargado de las siguientes actividades:

- Actuar como enlace permanente entre la Administración y el Supervisor del contrato que se designe para tal fin.
- Organizar, programar, dirigir y controlar las labores del personal asignado del contrato.
- Coordinar la acción de los Supervisores.
- Efectuar visitas periódicas a los sitios donde se presta el servicio.
- Establecer las condiciones de riesgo, detectar oportunamente y corregir los problemas en la prestación del servicio.
- Programar la rotación de vigilantes y mantener disponibilidad permanente para atender los requerimientos que se hagan por parte del supervisor del contrato.

ESPECIFICACIONES DEL CENTRO DE CONTROL DE MONITOREO – REGIONAL CENTRO

1. Características generales

El contratista deberá disponer, operar y mantener un Centro de Control de Monitoreo destinado a la recepción, supervisión, gestión y seguimiento de las señales generadas por los sistemas de seguridad electrónica instalados en las Oficinas de Registro de Instrumentos Públicos (ORIP) que se encuentren bajo la cobertura del contrato de vigilancia de la Regional Centro.

El Centro de Control deberá garantizar la operación continua durante las veinticuatro (24) horas del día, los siete (7) días de la semana, incluidos domingos y festivos, durante la vigencia contractual.

2. Recepción y gestión de señales

El Centro de Control deberá contar con la infraestructura tecnológica, el software, los equipos de comunicación y los demás recursos necesarios para recibir, identificar, registrar y gestionar, como mínimo, las siguientes señales y eventos, según los sistemas instalados en cada ORIP:

a. Activación de alarmas de intrusión.

b. Activación de botones de pánico o dispositivos de emergencia.

c. Activación de sensores de movimiento y demás dispositivos de detección.

d. Fallas de comunicación entre los sistemas instalados y el Centro de Control.

e. Pérdida de alimentación eléctrica o fallas de los dispositivos, cuando el sistema permita su detección y reporte.

f. Otros eventos generados por los sistemas de seguridad electrónica instalados en las sedes objeto del contrato.

3. Atención de eventos y protocolos de actuación

El contratista deberá establecer e implementar procedimientos para la recepción, clasificación, atención, escalamiento, seguimiento y cierre de los eventos reportados por los sistemas de seguridad electrónica.

Los eventos críticos deberán recibir atención inmediata, lo cual comprende el inicio inmediato de las acciones de verificación, diagnóstico, comunicación, escalamiento y mitigación que correspondan,

de acuerdo con la naturaleza del evento y los protocolos establecidos.

Los eventos no críticos deberán ser atendidos y solucionados en un plazo máximo de cinco (5) días hábiles, contados a partir de su reporte formal, salvo que la naturaleza de la situación exija una actuación más inmediata.

Toda actuación deberá quedar registrada, con indicación de la fecha y hora de recepción, las verificaciones efectuadas, las acciones adelantadas, las personas o dependencias contactadas y el resultado de la gestión.

4. Personal y procedimientos operativos

El Centro de Control deberá contar con personal capacitado para operar la plataforma de monitoreo, interpretar las señales recibidas, aplicar los protocolos de atención y efectuar las comunicaciones y escalaciones correspondientes.

El contratista deberá mantener actualizados los procedimientos de operación, los directorios de contacto y las rutas de escalamiento para reportar oportunamente los eventos al supervisor del contrato y a los responsables que designe la Superintendencia de Notariado y Registro (SNR).

5. Infraestructura tecnológica y comunicaciones

El contratista deberá disponer de los equipos informáticos, dispositivos de visualización, plataformas de monitoreo, licencias de software, medios de comunicación, sistemas de respaldo eléctrico y demás componentes necesarios para el funcionamiento adecuado del Centro de Control.

Asimismo, deberá garantizar la conectividad y los recursos de comunicación requeridos para la recepción de señales provenientes de las ORIP objeto del contrato, así como el funcionamiento de los componentes tecnológicos bajo su responsabilidad.

La conectividad institucional disponible en las sedes será suministrada por la SNR, conforme a su infraestructura. El contratista deberá realizar las configuraciones e integraciones técnicas necesarias para el funcionamiento de los sistemas contratados.

6. Integración con la Central General de Monitoreo del Nivel Central de la SNR

El contratista deberá garantizar que los sistemas de seguridad electrónica de las ORIP cubiertas por el contrato puedan integrarse y transmitir la información correspondiente a la Central General de Monitoreo ubicada en el Nivel Central de la SNR, de acuerdo con los requerimientos técnicos definidos por la Entidad.

Para tal efecto, deberá efectuar las configuraciones, parametrizaciones, pruebas y ajustes necesarios, sin perjuicio de las obligaciones operativas propias de su Centro de Control.

7. Registro, trazabilidad e informes

El contratista deberá conservar registros verificables de los eventos recibidos y gestionados, incluyendo su clasificación, fecha y hora, actuaciones adelantadas, comunicaciones realizadas, tiempos de atención y estado de cierre.

La información deberá estar disponible para consulta de la supervisión del contrato y deberá suministrarse cuando sea requerida, en los formatos y condiciones que establezca la SNR.

8. Seguridad de la información

El contratista deberá implementar controles de acceso a las plataformas del Centro de Control, administrar los perfiles de usuario autorizados y proteger la confidencialidad, integridad y disponibilidad de la información recibida y gestionada.

No podrá permitir accesos no autorizados, divulgar información de seguridad de las sedes ni utilizar los registros o imágenes para fines distintos de los relacionados con la ejecución contractual.

9. Continuidad del servicio y soporte técnico

El contratista deberá disponer de procedimientos de contingencia para atender fallas de sus equipos, plataformas o canales de comunicación, procurando mantener la continuidad de la operación del Centro de Control.

Las fallas que afecten la recepción de señales, la gestión de alarmas o la comunicación con las ORIP deberán reportarse y gestionarse oportunamente. Cuando se requiera intervención técnica, el contratista deberá coordinarla con el responsable de la sede y con la supervisión del contrato, según corresponda.

10. Pruebas y verificación de funcionamiento

Antes de la puesta en operación de los sistemas y cuando se realicen modificaciones que puedan afectar su funcionamiento, el contratista deberá efectuar las pruebas necesarias para verificar la comunicación entre las ORIP y el Centro de Control, la recepción de señales, el registro de eventos y la transmisión de información a la Central General de Monitoreo del Nivel Central de la SNR.

Los resultados deberán documentarse y ponerse a disposición de la supervisión del contrato. Las fallas identificadas deberán corregirse antes de dar por aceptado el funcionamiento del componente afectado.

11. ESPEJO DE MONITOREO E INTEGRACIÓN DE LOS SISTEMAS DE LAS REGIONALES

El Centro de Control de Monitoreo dispuesto por el contratista de la Regional Centro deberá contar con la infraestructura tecnológica y los recursos necesarios para alojar y operar el espejo de monitoreo de la Superintendencia de Notariado y Registro (SNR), a través del cual se recibirá y visualizará, en tiempo real, la información generada por los sistemas de seguridad electrónica de las Oficinas de Registro de Instrumentos Públicos (ORIP) correspondientes a las diferentes regionales de la Entidad.

Para tal efecto, el contratista deberá garantizar la compatibilidad, integración, configuración y funcionamiento de los componentes tecnológicos necesarios para centralizar la visualización de la información de monitoreo proveniente de las regionales, de acuerdo con los requerimientos técnicos establecidos por la SNR.

El espejo de monitoreo deberá permitir, según las funcionalidades de las plataformas implementadas, la consulta y visualización centralizada de las cámaras de videovigilancia, las señales de alarma, los eventos de seguridad y los demás datos transmitidos por los sistemas integrados.

El contratista deberá disponer de los equipos, licencias, software, interfaces, capacidad de procesamiento, almacenamiento temporal cuando resulte necesario y recursos de conectividad requeridos para garantizar el funcionamiento del espejo de monitoreo, así como realizar las configuraciones, pruebas y ajustes técnicos necesarios para su puesta en operación.

La integración deberá permitir que la información de las distintas regionales sea recibida y visualizada desde el Centro de Control de Monitoreo ubicado en la Regional Centro, sin que ello sustituya las responsabilidades operativas de los contratistas encargados del monitoreo en las demás regionales.

El contratista deberá garantizar la disponibilidad del servicio, la seguridad de la información, el control de acceso de los usuarios autorizados por la SNR y la atención de las fallas que afecten la recepción o visualización de la información. Asimismo, deberá coordinar con la Entidad y con los demás

contratistas las actividades técnicas necesarias para asegurar la interoperabilidad de los sistemas.

Los costos asociados a la implementación, configuración, licenciamiento, operación, mantenimiento y soporte del espejo de monitoreo deberán estar incluidos en la oferta económica y en el valor del contrato, conforme a las obligaciones y condiciones establecidas en el proceso contractual.