ANEXO TECNICO DE REQUISITOS Y REQUERIMIENTOS PARA LA HOMOLOGACIÓN DE LOS PROVEEDORES DE SISTEMA INTEGRADO DE SEGURIDAD

1. OBJETO DEL ANEXO TECNICO

El presente documento define los requisitos y requerimientos técnicos y tecnológicos que deben cumplir aquellos aspirantes a proveedores del Sistema Integrado de Seguridad de que trata el Decreto 026 de 2017 y que se divide en técnicos, administrativos, financieros y jurídicos, así como los procesos de evaluación que deben cumplir las empresas solicitantes.

2. PROTOCOLOS DE OPERACIÓN DEL SISTEMA INTEGRADO DE SEGURIDAD.

El Sistema Integrado de Seguridad es una infraestructura tecnológica operada por cualquier compañía del sector de las Tecnologías de la Información y que las Instituciones Especializadas contraten, que será previamente homologado por la Superintendencia de Vigilancia y Seguridad Privada o por quien esta delegue, para asegurar el cumplimiento de los requerimientos establecidos en el presente anexo conforme al artículo 2.6.1.1.10.1.2. del Decreto 26 de 2017 , y que deberá aplicar los siguientes protocolos de seguridad integrados:

- Garantizar el registro del pago a través de un PIN de la evaluación y del certificado de aptitud psicofísica para el porte y tenencia de armas para los particulares y para usuarios vinculados a los servicios de vigilancia y seguridad privada asumidos por las ARL.
- Registro y Asignación de citas obligatorio en agenda integrada en línea para los usuarios e Instituciones Especializadas.
- Registrar, autenticar y validar a los usuarios aspirantes su identidad a través de su huella dactilar contra la Base de Datos de la Registraduría Nacional del Estado Civil, y brindando adicionalmente la facilidad para mejorar la gestión y el control de los procesos que el sistema integrado de seguridad va a llevar, por medio de un sistema multibiométrico (multidactilar, rostro y/o de voz).
- Validar a través de la huella y/o el rostro y/o la voz a los aspirantes y a los médicos especialistas al principio y al final de cada evaluación de los exámenes de aptitud psicofísica.
- Validar que la cedula de ciudadanía no es falsa y extraer los datos de esta para la validación de los participantes en cada proceso.
- Todos los actores que interactúan con el sistema firmarán digitalmente todas las acciones y a través de la huella dactilar y/o multidactilar y/o el rostro y/o la voz.

- Registrar y validar la posición geográfica de cada sede acreditada de las Instituciones Especializadas autorizadas, cada uno de los equipos de cómputo con sus principales componentes que interviene en el registro, evaluación y certificación.
- Contar con un Software de Gestión para los procesos de: asignación de citas, registro o enrolamiento, evaluación, certificación, administración de Instituciones.
- Contar con un Sistema de Gestión de Calidad estandarizando criterios, tablas de equivalencia, técnicas de evaluación y calificación integrada en el Software de Gestión.

Permitir la integración e interoperabilidad en línea y en tiempo real entre el Sistema del Comando General de las Fuerzas Militares a través de la Dirección General de Comercio, Control de Armas y el Sistema Integrado de Seguridad, para que validen previamente antes de expedir los permisos el cumplimiento del examen de aptitud psicofísica.

3. ALCANCE DEL DOCUMENTO ANEXO TÉCNICO.

El alcance de este documento incluye la definición de los requisitos a nivel jurídico, administrativo, financiero y de los requerimientos a nivel técnico y tecnológico que deben cumplir las compañías interesadas en operar el Sistema Integrado de Seguridad para las Instituciones Especializadas en todos los exámenes de aptitud psicofísica.

Los requerimientos administrativos permitirán validar la trayectoria y experiencia de las compañías y entidades interesadas en proyectos similares de tecnología, experiencia del equipo de trabajo, entre otros.

Los Requerimientos Financieros permiten verificar que las compañías interesadas realmente cuenten con el respaldo económico suficiente para que inicie el funcionamiento del Sistema Integrado de Seguridad y que una vez puesta en marcha la operación tenga sostenibilidad, garantizando a la Superintendencia de Vigilancia y Seguridad Privada que la compañía que opere dicho sistema disponga de los recursos necesarios sostenibles en el tiempo.

Los Requerimientos Jurídicos permiten verificar la legalidad de las compañías o entidades a homologarse, de sus representantes, y que no está incursa en inhabilidades o incompatibilidades que impidan el ejercicio de las actividades involucradas en el proceso.

Los Requerimientos Técnicos y Tecnológicos permiten garantizar la idoneidad en la prestación del servicio, buscando que se utilice la

tecnología adecuada y actualizada a las necesidades de seguridad, disponibilidad y calidad del servicio.

4. REQUISITOS DOCUMENTALES.

A continuación, se establecen los requerimientos que deberán cumplir las compañías o entidades interesadas en la homologación para recibir la valoración documental; Estos se deberán suministrar con el fin de que sean corroboradas sus condiciones jurídicas, administrativas, financieras y técnicas:

4.1. DOCUMENTO DE MANIFESTACIÓN DE INTERÉS.

Las compañías o entidades que deseen aspirar a homologarse como operador del Sistema Integrado de Seguridad, deberán enviar un oficio manifestando su interés en participar en el proceso de evaluación y homologación según lo dispuesto en el presente acto administrativo de Anexo Técnico, relacionar y adjuntar los documentos exigidos en los requisitos jurídicos, administrativos, financieros y técnicos definidos en este anexo.

El oficio de manifestación de interés deberá ir firmado por el representante legal de la compañía o entidad interesada.

4.2. DOCUMENTACIÓN DE REQUISITOS.

La documentación de los requisitos aportados deberá ir foliada en orden consecutivo y clasificado por cada tipo de requisito en su orden:

A. En la primera página deberá una portada con el nombre y NIT de la compañía interesada y en el asunto “PRESENTACIÓN DE REQUISITOS DOCUMENTALES SEGÚN LA RESOLUCIÓN DEL ANEXO TECNICO DEL SISTEMA INTEGRADO DE SEGURIDAD”.

B. En la segunda página el índice general relacionando el contenido de los documentos aportados relacionando el folio donde se encuentra cada documento o soporte

C. Desde la página tres (3) en adelante se deberán adjuntar los documentos exigidos en lo Jurídico, Administrativo, Financiero y Técnico.

4.3. REQUISITOS JURÍDICOS.

Las entidades o compañías interesadas en proveer El Sistema Integrado de Seguridad para las Instituciones Especializadas en los exámenes de aptitud psicofísica requiere para su operación actividades tales como desarrollo de software, seguridad de la información y suministro e

implementación de hardware y software, para la cual las personas naturales o jurídicas deberán garantizar su legalidad y capacidad jurídica aportando los documentos o soportes de tipo jurídico para su verificación que a continuación se describen:

I. *Certificado de existencia y representación*. Expedido por la Cámara de Comercio. Expedición no mayor a 30 días calendario a la fecha de radicación en la Superintendencia de Vigilancia y Seguridad Privada.

II. *Registro Único de Proponentes.* Expedido por la Cámara de Comercio. Expedición no mayor a 30 días calendario a la fecha de radicación en la Superintendencia de Vigilancia y Seguridad Privada, en ella debe contener la experiencia certificada a aportar y registrados en al menos ocho (08) de los siguientes códigos de bienes y servicios:

- 432215 Software funcional especifico de la empresa
- 432316 Software de planificación de recursos empresariales (ERP)
- 432323 Software de Consultas y Gestión de Datos
- 432324 Programas de Desarrollo
- 432332 Software de Seguridad y Protección
- 432334 Software de Controladores de dispositivos y utilidades
- 811027 Servicios de Diseño e ingeniería de sistema e instrumentados de control.
- 811115 Ingeniería de Software o Hardware
- 811118 Servicios de sistemas y administración de componentes de sistemas.
- 811120 Servicios de datos
- 811121 Servicios de internet
- 811122 Mantenimiento y soporte de software

III. *Registro Único Tributario RUT.*

IV. *Copia de documento de identidad del representante legal.* Ampliada al 150%, está deberá ir firmada, con huella y con el siguiente mensaje impreso en la parte inferior de la copia: *"VÁLIDA ÚNICAMENTE COMO REQUISITO DOCUMENTAL PARA PROCESO DE EVALUACIÓN SUPERVIGILANCIA"*

V. *Certificado del pago de aportes parafiscales.* Certificado emitido por revisor fiscal o representante legal según corresponda, su expedición debe ser igual o inferior a 30 días calendario al de la fecha de

radicación. En caso de ser un revisor fiscal el obligado a emitir el certificado deberá anexar fotocopia de la cédula de ciudadanía, fotocopia de la tarjeta profesional y antecedentes disciplinarios de la Junta Nacional de Contadores.

VI. *Certificación de composición de socios o accionistas.* Cuando esta información no conste en el certificado de existencia o representación expedido por la Cámara de Comercio, deberá aportar la certificación de composición de socios o accionistas. Esta debe tener corte de la información en un término no superior a treinta (30) días de la fecha de presentación y radicación de la propuesta. Si dentro de la composición accionaria de la empresa se encuentra una persona jurídica cuya participación sea igual o superior al 5% del capital, esta debe aportar la composición de participación accionaria, proceso que debe repetirse hasta que los accionistas sean personas naturales. El certificado de composición de socios o accionistas deberá ser emitido por el Revisor Fiscal de la empresa o consorcio. En caso de Unión Temporal se deberá presentar un certificado de composición de socios o accionistas de cada una de las empresas que conforman la Unión Temporal. En caso de no presentar la composición accionaria por su naturaleza jurídica, el Representante Legal del aspirante a proveedor deberá presentar una declaración juramentada, autenticada con reconocimiento de texto, firma y huella en Notaría, de que no participará en más de una propuesta para el presente proceso. Debe incluir: Nombre o razón social, identificación y porcentaje de participación, siempre y cuando esta sea igual o superior al 5%. Deberá certificar el 100% de las acciones de la compañía.

Si la propuesta es presentada en Unión Temporal o en Consorcio, se debe aportar por cada una de las personas naturales y/o jurídicas que lo(a) conformen, los documentos o soportes exigidos anteriormente.

4.4. REQUISITOS ADMINISTRATIVOS.

A continuación, se describen los requisitos que permiten verificar la idoneidad a través de la trayectoria y experiencia en proyectos similares en tecnologías, de su personal, del aseguramiento y estandarización de sus procesos y procedimientos, capacidad organizacional, entre otros aspectos:

I. *Experiencia de la Compañía*. Las entidades o compañías interesadas deben acreditar la experiencia compuesta de actividades que garanticen el cubrimiento de todos los aspectos que conforman el Sistema Integrado de Seguridad.

A. Cuantía total experiencia solicitada. La cuantía de la experiencia debe ser igual o superior a (Seis mil) SMMLV (Salarios Mínimos Mensuales Legales Vigentes). Cuando las certificaciones expresen su valor en dólares, se tendrá en cuenta la TRM a la fecha en que se celebró el contrato certificado. En caso de presentar certificaciones globales. Deberán desglosar el monto o porcentaje y objeto para el cual aplica dicha certificación.

B. Número máximo de contratos a certificar. Los interesados deberán acreditar experiencia mediante certificación firmada por los contratantes o entes gubernamentales en máximo cinco (5) certificaciones.

C. Antigüedad. Las certificaciones de experiencia ejecutada deberán tener una antigüedad máxima de siete (7) años a la fecha de radicación de la manifestación de interés y de los requisitos documentales.

D. Acreditación de la experiencia. Los aspirantes interesados deberán Acreditar experiencia mediante certificación firmada por los clientes en por lo menos un proyecto en sistemas que incluyan alguna de las siguientes funcionalidades:

i. Seguridad Informática y/o Seguridad de la Información: Manejo de Riesgo, Protección de Datos, Cifrado de Información, Auditoría de Bases de Datos, Centro de Operaciones de Seguridad (SOC), Correlación de Eventos.

ii. Software: Desarrollo y/o implantación de software.

E. Cumplimiento en contratos. Las certificaciones de experiencia que califiquen el cumplimiento del contrato como “malo”, “regular”, o expresiones similares que demuestren el cumplimiento no satisfactorio del mismo o que indiquen que durante su ejecución fueron sujetas a multas o sanciones debidamente impuestas por la administración o que a las mismas se les haya hecho efectiva la cláusula penal estipuladas en los contratos, no se aceptarán por el ente evaluador. Cada aspirante interesado acreditará la experiencia requerida para este proceso de evaluación a través de la presentación de certificaciones expedidas por quien otorga la misma. En caso de que el comité evaluador requiera información adicional, se solicitaran copias de los contratos y los documentos

que se consideren pertinentes y necesarios para la aclaración y verificación.

F. Certificaciones exigibles a las compañías interesadas. El aspirante interesado a del Sistema Integrado de Seguridad deberá contar con las siguientes certificaciones vigentes:

a) Sistema de Gestión de la Calidad.
b) Acreditación en la prestación de los servicios de certificación digital de personas jurídicas y naturales, además de archivo y conservación de documentos electrónicos transferibles, conforme a lo dispuesto en el Decreto 019 del 2012 artículo 161 numerales 1 y 8.

En caso de presentarse en Unión Temporal o Consorcio al menos una de las compañías deberá cumplir con todos los anteriores requisitos administrativos.

Las compañías interesadas deberán presentar las certificaciones y acreditaciones expedidas por quienes las otorgan en Colombia.

I. Equipo de trabajo exigible a las compañías interesadas. Deberán aportar las hojas de vida del personal idóneo con sus respectivas certificaciones y actas de grado de acuerdo a cada perfil exigido.

G. Dirección.

i. *Un Gerente de Proyectos.* Profesional en Ingeniería de Sistemas, Electrónica, Telecomunicaciones o carreras afines. Posgrado en Gerencia de Proyectos o con certificación de PMP o Maestría en Ingeniería de Sistemas. Certificaciones de Experiencia en Dirección de Proyectos en los últimos tres (3) años. Adjuntar: Copia título profesional, matrícula profesional, certificaciones y contrato con la compañía o entidad aspirante a proveedor.

H. Seguridad Informática.

i. *Un Director o Gerente Centro de Operaciones de Seguridad (SOC).* Profesional en Ingeniería de Sistemas, Electrónica, Telecomunicaciones o carreras afines. Posgrado en Seguridad Informática o certificación como Auditor Interno de ISO 27001. Certificaciones de experiencia como Gerente de SOC en los últimos tres (3) años. Adjuntar: Copia título profesional, matrícula profesional, certificaciones y contrato con la compañía o entidad aspirante a proveedor.

ii. *Un Oficial de Seguridad.* Profesional en Ingeniería de Sistemas, Electrónica, Telecomunicaciones o carreras afines. Posgrado en Seguridad Informática o certificado como CISSP o CISM. Certificaciones de experiencia como Seguridad Informática un (1) año mínimo en los últimos cinco (5) años. Adjuntar: Copia título profesional, matrícula profesional, certificaciones y contrato con la compañía o entidad aspirante a proveedor.

iii. *Un Especialista DBA*. Profesional en Ingeniería de Sistemas, Electrónica, Telecomunicaciones o carreras afines. Deberá aportar certificación técnica o experiencia certificada como DBA en la Base de Datos presentada con la aplicación construida en los últimos dos (2) años. Adjuntar: Copia título profesional, matrícula profesional, certificaciones y contrato con la compañía o entidad aspirante a proveedor.

iv. *Un Especialista en Ethical Hacking.* Profesional en Ingeniería de Sistemas, Electrónica, Telecomunicaciones o carreras afines. Deberá aportar certificado vigente como CISSP (Profesional en aseguramiento de la información) o CEH (Hacker Ethical Certificado), o contrato con una compañía para la prestación de Servicios de Ethical Hacking que tenga personal certificado como CISSP o CEH. Adjuntar: Copia de título profesional, matrícula profesional, certificaciones y contrato con la compañía aspirante a proveedor o con la compañía contratada para la prestación de servicios de Ethical Hacking.

I. Desarrollo.

i. *Un Gerente de Desarrollo.* Profesional en ingeniería de sistemas, electrónica o afines. Posgrado en arquitectura, construcción o ingeniería de software. Con experiencia laboral certificada como líder, coordinador o gerente de desarrollo en los últimos dos (2) años. Adjuntar: Copia título profesional, matrícula profesional, certificaciones y contrato con la compañía o entidad aspirante a proveedor.

ii. *Dos Ingenieros o Tecnólogos de Desarrollo.* Profesionales en Ingeniería de Sistemas o Tecnólogos en Sistemas o afines con certificación en los lenguajes de programación de la aplicación construida presentada o certificaciones de experiencia laboral en los últimos dos (2) años. Adjuntar: Copia título profesional, matrícula profesional, certificaciones y contrato con la compañía o entidad aspirante a proveedor.

iii. *Un Gerente de Operaciones.* Profesional en ingeniería de sistemas, industrial, electrónica, de redes o afines. Posgrado o certificación en ITIL o COBIT, con experiencia laboral como gerente, líder o

coordinador en los últimos dos (2) años. Adjuntar: Copia título profesional, matrícula profesional, certificaciones y contrato con la compañía o entidad aspirante a proveedor.

En caso que el desarrollo sea de una fábrica de software deberá tener un contrato con dicha fábrica y las licencias de uso.

J. Soporte.

i. *Un Coordinador de Soporte*. Profesional en ingeniería de sistemas, electrónica, telecomunicaciones o carreras afines. Posgrado o certificación en ITIL al momento de presentarse al proceso de evaluación de homologación. Experiencia como líder de soporte mínimo dos (2) años en los últimos cinco (5) años. Adjuntar: Copia título profesional, matrícula profesional, certificaciones y contrato con la compañía o entidad aspirante a proveedor.

ii. *Personal de soporte*. Dos (2) profesionales de soporte. Profesionales en ingeniería de sistemas, electrónica, telecomunicaciones o afines. Cuatro (4) técnicos de soporte. Técnicos, tecnólogos o ingenieros de sistemas, electrónica, redes, telecomunicaciones o afines. Adjuntar: Copia título profesional, matrícula profesional, certificaciones y contrato con la compañía o entidad aspirante a proveedor.

iii. *Mesa de ayuda*. La compañía aspirante debe entregar el esquema de atención de la mesa de ayuda firmado por un ingeniero con certificación ITIL versión 3 intermedio o superior, quien avale los procesos de mesa de ayuda diseñados basados en las mejores prácticas de ITIL. Conforme a lo reglamentado en el artículo 2.6.1.1.10.1.3., numeral 3 del Decreto 26 de 2017.

4.5. REQUISITOS FINANCIEROS.

A continuación, se describen los requisitos que permiten verificar la capacidad financiera para los aspirantes a proveedores para la continuidad de este proyecto.

A. Presentar los Estados Financieros certificados y dictaminados de la Sociedad: Balance General, Estado de Resultados y las Notas a los Estados Financieros, con corte al 31 de diciembre del año inmediatamente anterior a la presentación de la propuesta ante la Superintendencia de Vigilancia y Seguridad Privada, debidamente certificados y dictaminados a quien corresponda. Deberán detallar Clases, Grupos y Cuentas en los diferentes estados a presentar.

B. Fotocopia de la tarjeta profesional del contador, revisor fiscal o contador independiente, según corresponda;

C. Certificación expedida por la Junta Central de Contadores, la cual no será anterior a tres (3) meses de la fecha de presentación de la oferta, del contador, revisor fiscal o contador independiente, según corresponda.
D. En caso de que el aspirante a proveedor sea evaluado antes del 31 de marzo de la vigencia en que se presente, y no cuente con los estados financieros a corte de 31 de diciembre de la vigencia inmediatamente anterior, podrá presentar los estados financieros del subsiguiente año fiscal.
E. Como requisito habilitante deberá cumplir con los siguientes indicadores financieros:

INDICADORES	CONCEPTO	REQUISITO
LIQUIDEZ	ACTIVO CORRIENTE / PASIVO CORRIENTE	>= 1,0
NIVEL DE ENDEUDAMIENTO	PASIVO TOTAL/ACTIVO TOTAL	<= al 60%
CAPITAL DE TRABAJO	ACTIVO CORRIENTE PASIVO CORRIENTE	>$2.000.000.000
DE RIESGO	ACTIVO FIJO / PATRIMONIO NETO	< 0,8

En caso de participar en Unión Temporal o Consorcio, se deberá cumplir con los indicadores financieros conforme a los parámetros que se definen a continuación:

Los Indicadores de Valor absoluto como son el Capital Real y el Capital de Trabajo se aplica la siguiente fórmula para este caso que de Unión Temporal:

La siguiente es la fórmula aplicable para los indicadores que son valores absolutos, como el capital de trabajo:

$$(i)\ Indicador\ en\ valor\ absoluto = \sum_{i=1}^{n} Indicador_i$$

Donde es el número de integrantes del oferente plural (unión temporal, consorcio).

Se interpreta como la sumatoria del resultado obtenido de cada compañía participante con respecto a los indicadores de valor absoluto.

Para los indicadores que provienen de la división de cuentas de los estados financieros, se analizarán bajo el método de ponderación de los componentes de los indicadores:

En este método cada uno de los integrantes del oferente aporta al valor total de cada componente del indicador de acuerdo con su participación en la figura del oferente plural (unión temporal, consorcio o promesa de sociedad futura).

La siguiente es la fórmula aplicable para los indicadores que son índices en la opción 1:

$$(ii)\ Indicador = \frac{\left(\sum_{i=1}^{n} Componente\ 1\ del\ indicador_i \times porcentaje\ de\ participación_i\right)}{\left(\sum_{i=1}^{n} Componente\ 2\ del\ indicador_i \times porcentaje\ de\ participación_i\right)}$$

Donde n es el número de integrantes del proponente plural (unión temporal, consorcio).Esta opción incentiva que el integrante del proponente plural con los mejores indicadores tenga una mayor participación en dicho proponente plural.

4.6. REQUERIMIENTOS TÉCNICOS.

A continuación se describen los requerimientos técnicos que deberá cumplir el Sistema Integrado General con todos los elementos que deberá tener la plataforma tecnológica (hardware, software, comunicaciones, bases de datos, etc.), necesaria para el control, seguimiento y auditoría por parte de la Supervigilancia de las evaluaciones de aptitud psicofísica, que deberá ser provista, desplegada y en operación por el Proveedor Homologado. Conforme al protocolo de seguridad reglamentado en el artículo 2.6.1.1.10.1.2. del Decreto 26 de 2017, el Sistema Integrado de Seguridad para su operación deberá contar como mínimo con los siguientes elementos estructurales:

- Un dispositivo computacional central de control y manejo de información con capacidad de múltiple procesamiento, almacenamiento y comunicaciones seguras, capaz de identificar sitios remotos;
- Múltiples lectores de información biométrica;

- Captores de huellas dactilares, con la funcionalidad de detectar dedos vivos,
- Cámara digital de alta definición,
- Escáneres o lectores de información de documentos de identificación con capacidad de leer códigos bidimensionales;
- Digitalizadores de firmas, para realizar el registro de firmas manuscritas y que vincule firmas electrónicas;
- Infraestructura de computo central para el registro, gestión y control de la información, con , multiprocesamiento de varios núcleos, memoria aleatoria RAM, memoria FLASH, almacenamiento escalable, componentes de entradas y salidas, controladores lógicos programables, comunicaciones seguras, que identifique y monitoree las sedes de evaluación a través su posición geográfica, que tenga un componente de control de tiempos mínimos y máximos que se deban cumplir en el proceso de evaluación, un componente de generación de certificados, interoperabilidad con diferentes bases de datos de carácter público a través de VPN o Redes Privadas virtuales.
- Componente de comunicaciones con módulos Ethernet TCP/IP, GPRS, serial, USB, GPS con antena.
- Comunicaciones seguras a través de redes virtuales de seguridad privada (VPN) y que permita el acceso seguro a múltiples bases de datos.

Adicionalmente el Sistema deberá contar con los siguientes componentes:

- Centro de Procesamiento de Datos (CPD). Infraestructura donde se alojará la solución tecnológica bajo las mejores prácticas.
- Centro de Operaciones de Seguridad (SOC). Monitoreo y Control de todo el Sistema.
- Software de Gestión. Cada uno de los proveedores del sistema de seguridad, deberán proveer, a través de esta aplicación (Software), a las Instituciones Especializadas donde deberán realizar la evaluación y certificación con los procesos de: registro o enrolamiento de centros, representantes legales, administradores, recepcionistas, médicos y especialistas; validación del pago; asignación de citas; registro o enrolamiento del solicitante; autenticación y validación multibiométrica de los solicitantes y de los médicos o especialistas y dactilar de los mismos contra la base de datos de la RNEC; registro de la evaluación médica y sus cuatro

etapas (psicomotriz, optometría, auditiva y médica); registro de la historia clínica. Esta aplicación estará alojada en el CPD e integrada con el SOC, el Aliado de Recaudo y el Operador de Validación Biométrica de la RNEC. Este software de gestión deberá ser aprobado por la Superintendencia de Vigilancia Privada, que lo evaluará integralmente.

- Sistema de Gestión de Calidad. El Software de Gestión, deberá tener una herramienta como instrumento de registro, verificación y control de los actores y sus procesos que se regulan es este acto.
- Mesa de Ayuda (Help Desk). Para brindar soporte a los usuarios en línea.
- Red de Comunicaciones. Para interconectar a todos los actores involucrados.
- Deberá contar con un modelo de seguridad que garantice las acciones realizadas por el personal, teniendo en cuenta los siguientes criterios:
    - Autenticidad: Atributo que garantiza que una persona natural o jurídica que intervenga en el proceso es realmente quien dice ser, y que tiene capacidad de suscribir o firmar documentos e identificarse.
    - Integridad: Condición que garantiza que la información consignada en un mensaje de datos ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.
- Deberá contar con que los servicios sean prestados por una entidad de certificación digital abierta, acreditada por el Organismo de Acreditación de Colombia - ONAC para:
    - Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.
    - Ofrecer o facilitar los servicios de generación de los datos de creación de las firmas digitales certificadas.
- Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.
    *<u>que permita garantizar el momento exacto en el cual se realizó la transacción.</u>
- Infraestructura distribuida en las Instituciones especializadas:
    - Comunicaciones:
        - Canal Dedicado de Internet o de Datos como mínimo de 3 Mbps.
        - Switch de Comunicaciones PoE de ocho (8) puertos capa 3, administrable.

- ➢ Cableado estructurado categoría 6 certificado entre las cámaras y el switch.
- ➢ Gabinete de Pared de 5U
- ➢ UPS ONLINE 750VA
- o Dispositivos de Seguridad Informática:
- ➢ Firewall de Siguiente generación NGFW deberá contar como mínimo con las siguientes especificaciones:
- ✓ Hardware: Cinco (5) puertos LAN RJ45, Dos (2) Puertos WAN, Un (1) Puerto USB, Un (1) Puerto de Consola (RJ45).
- ✓ Firewall Throughput 2,5 Gbps, 180 paquetes por segundo, Throughput NGFW 200 Mbps,
- ✓ Concurrencia en sesiones TCP un millón quinientos (1.500.000), nuevas sesiones por segundo 20.000 (veinte mil).
- ✓ Políticas de Firewall 5.000.
- ✓ IPSec VPN Throughput (paquetes 512 byte) 200 Mbps, 200 Túneles IPsec VPN Gateway-to-gateway-.
- ✓ Configuraciones de alta disponibilidad: Activo/Activo, Activo/Pasivo, Clustering.

La Administración y Gestión de la solución de Firewall es Centralizada

- o Elementos de Seguridad Física:

- ➢ Cámaras de Seguridad para la entrada, recepción y sala de espera (Tres unidades) que deberán tener como mínimo las siguientes especificaciones:

- ✓ Digital Resolución de 1.3 Megapíxeles y 720P, función día/noche, sensor CMOS e infrarrojo, PTZ 0°-360°/10°-90°/0°-360°.
- ✓ Funciones de detección de Movimiento y Antimasking,
- ✓ Compresión de video H.264, MJPEG, dual-stream encoding.
- ✓ 25/30 fps (1280x960)
- ✓ Interoperabilidad ONVIF (Open Network Video Interface Forum), PSIA y CGI.
- ✓ Protocolos de comunicaciones Ethernet RJ45 (10/100), PoE, HTTP, HTTPs, TCP, SMTP, multicast, IPv4, IPv6, FTP, UDP, DHCP.
- ✓ Software de administración.

- ➢ DVR de cuatro (4) canales, que deberán tener como mínimo las siguientes especificaciones:

- ✓ Procesador embebido, Interface HDMI y VGA. 2 puertos USB 2.0, Control de PTZ.
- ✓ Disco Duro 6 TB.
- ✓ Compresión H.264, grabación 1080N, 720P, 960H.
- ✓ Detección y Alarma de Video, Eventos de activación: Grabación, PTZ, Tour, Salida de alarma, Push de vídeo, Correo electrónico, FTP, Instantánea, Buzzer y Pantalla.
- ✓ Detección de movimiento, MD Zones: 396 (22 × 18), pérdida de video y manipulación.
- ✓ Función de Reproducción y Backup: Reproducción, Pausa, Detener, Rebobinar, Reproducción rápida, Reproducción lenta, Archivo siguiente, Archivo anterior, Cámara siguiente, Cámara anterior, Pantalla completa, Repetir, Aleatorio, Selección de copia de seguridad, Zoom digital.
- ✓ Función OSD (Reproducción en Pantalla): Título de la cámara, Tiempo, Pérdida de vídeo, Bloqueo de la cámara, Detección de movimiento, Grabación. En caso de que la grabación falle por veinticuatro (24) horas el sistema integrado de seguridad bloqueará la emisión de certificados.

-DOCUMENTACIÓN TÉCNICA REQUERIDA.

Las compañías interesadas deberán aportar con la manifestación de interés la siguiente documentación técnica:

a. Certificado de registro de soporte lógico de la Dirección Nacional de Derechos de Autor del software desarrollado propio o a través de un tercero con su respectiva autorización o licencia de uso para este proyecto.
b. Copia de la resolución expedida por la Superintendencia de Industria y Comercio donde se conceda la patente de invención o modelo de utilidad a la compañía aspirante interesada o una autorización por parte del propietario de la patente, en donde contenga en su alcance y/o en sus reivindicaciones los elementos estructurales del Sistema Integrado de Seguridad definidos en los requerimientos técnicos, respetando los derechos de propiedad industrial reconocidos mediante patente de invención o patente modelo de utilidad por la Superintendencia de Industria y Comercio, cumpliendo con todas las características, los elementos y los requisitos aquí establecidos y con las condiciones y especificaciones técnicas

complementarias. Con base en lo establecido en el artículo 2.6.1.1.10.1.5. del Decreto 26 de 2017.

c. Copia de contrato del Centro de Procesamiento de Datos, en caso de que el CPD se encuentre subcontratado. Los contratos deberán tener una duración mínima de dos (2) años.
d. Relación de equipos de SOC y Datacenter. El Hardware dispositivos de seguridad, servidores, appliance, las licencias respectivas de las aplicaciones, bases de datos y de los sistemas operativos, entre otros. En el Hardware utilizado se debe relacionar la marca, modelo, el datasheet y soporte de Gartner o Forester Wave de las soluciones de servidores, IPS, Firewall, Herramienta DAM, Herramienta SIEM, SAN, Escáner de Vulnerabilidades, Application Delivery Controller. En el caso en el que el Centro de operaciones SOC se encuentre subcontratado, la relación presentada deberá ser del proveedor contratado.

4.6.2. REQUISITOS OPERADORES DE RECAUDO.

Las compañías interesadas en ser proveedores del Sistema Integrado de Seguridad deberán contar con uno o más operadores de recaudo en alianza que deberán cumplir con los siguientes requisitos:

I. Miembro del Sistema Financiero Colombiano calificado como de bajo riesgo o un operador postal de pago autorizado en Colombia y que deberá tener un convenio para este proyecto con por lo menos con una entidad financiera vigilada por la Superintendencia Financiera de Colombia.
II. Acreditar experiencia mediante certificación firmada por los clientes en por lo menos un proyecto donde se haya efectuado integración con los sistemas transaccionales de cualquier sector productivo en los últimos tres (3) años.
III. El aliado de recaudo deberá generar un número de identificación único de pago (PIN) a través de un proceso seguro, que se realiza a través de un algoritmo que concatena diferentes campos de información de una transacción, que finalmente se construye con un consecutivo secuencial, único e irrepetible de forma segura y deberá cumplir además con los siguientes criterios:

i. Encriptación de los datos que viajan a través de la red.
ii. Actualización en línea de lo recaudado.

iii. Despliegue en operación un esquema de replicación en línea de los datos.
iv. Deberá emitir o generar comprobantes de recaudo, con posibilidades de emitir las copias necesarias.
v. Redundancia de un datacenter principal y un datacenter alterno, garantizando continuidad del servicio.
vi. Contar con dispositivos de seguridad perimetral en la red.
vii. Disponer de un canal de atención inmediata para usuarios y clientes (P.Q.R).
viii. Restricción en la manipulación técnica de la plataforma de recaudo y de los equipos de cómputo o terminales en los puntos de recaudo.
ix. Debe obtener datos del recaudo tales como fecha, hora, remitente, Tipo ID del que compra, Número de ID del que compra, asegurando dichos datos donde solo la plataforma de recaudo pueda utilizarlos.
x. Debe controlar, validar y llevar trazabilidad de los datos del recaudo como son: Número único de identificación de pago o recaudo, el valor del pago, el estado (pago o utilizado), fecha del uso del servicio, hora del uso del servicio, número único de uso, entre otros.
xi. Presentar procedimiento que evite que traten de falsificar comprobantes de recaudo.
xii. A través de él o los aliados de recaudo, la compañía interesada como proveedor del Sistema Integrado de Seguridad, debe garantizar puntos de atención en todos los municipios del país donde se ubiquen las Instituciones Especializadas y manifestar que está en la disposición de habilitar nuevos puntos de atención conforme a los requerimientos y demandas concertados con la Supervigilancia.
xiii. Cada Operador de Recaudo deberá generar una póliza de cumplimiento a favor de cada Institución Especializada y del proveedor homologado del Sistema Integrado de Seguridad por el buen manejo del dinero recaudado. El o los aliados de recaudo, deberán brindar diferentes medios de pago como pueden ser: pagos a través de Internet, datafonos, dispositivos satélites ubicados en las Instituciones Especializadas, entre otros.
xiv. Cada Operador de recaudo deberán suscribir un documento de compromiso mediante el cual se obligan a cumplir con niveles de servicios del 99%, en los periodos de atención de las Instituciones Especializadas.

xv. El aliado de recaudo deberá contar con certificación de calidad.

IV. Compromisos Posteriores.

A. El Operador de Recaudo deberá generar y entregar un oficio a la Superintendencia de Vigilancia y Seguridad Privada comprometiéndose generar una póliza de cumplimiento a favor de cada Institución Especializada y del proveedor homologado por el buen manejo del dinero recaudado y niveles de servicios del 99% en los periodos de atención de las Instituciones Especializadas.

B. El operador del recaudo deberá estar integrado con el Sistema de Control y Vigilancia para la consulta, validación y consumo de los Pines y la publicación para la Superintendencia de Vigilancia Privada de:

i. Pines consumidos por las distintas Instituciones Especializadas identificando el número de único de identificación de pago o el PIN, valor del pago, Institución donde fue consumido el PIN, datos del usuario, fecha y hora.

ii. Pines devueltos y/o Pines no consumidos en un periodo superior a siete (7) días calendario.

iii. En cualquier momento, el aspirante a proveedor o el proveedor autorizado Sistema Integrado de Seguridad podrá solicitar la ampliación del número de operadores de recaudo, cumpliendo con los requisitos antes señalados.
Lo anterior con base en lo reglamentado en el artículo 2.6.1.1.10.2.4. del Decreto 026 de 2017 para los proveedores de recaudo que interactúen con el Sistema Integrado de Seguridad

4.6.3. REQUISITOS DEL OPERADOR TECNOLÓGICO DEL SERVICIO PARA LA AUTENTICACIÓN BIOMÉTRICA DE LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL (RNEC).

Las compañías interesadas deberán contar con un operador del servicio para autenticación biométrica de las huellas dactilares que cumpla con todos los requerimientos y evaluaciones exigidos por la Registraduría Nacional del Estado Civil (RNEC) y habilitado por esta. El operador debe cumplir con los siguientes requerimientos:

I. Acreditar cumplimiento de Requerimientos con la RNEC.

II. Deberá tener Infraestructura Tecnológica aprobada, desplegada, auditada por la RNEC y en producción realizando consultas permanentes para por lo menos una entidad pública o con funciones públicas del servicio de Validación de Identidad contra las bases de datos de identificación ciudadana (Biometría), manejando el estándar ISO 197942, conforme a lo dispuesto en la Resolución 3341 del 2013 de la RNEC, su anexo y la normatividad vigente.
III. La validación de identidad biométrica deberá tener características de firma electrónica con validez jurídica y probatoria según el Decreto 2364 de 2012, asegurando la autenticidad, integridad y no repudio de la transacción usando los mecanismos previstos por la ley 527 de 1999.
IV. El operador del servicio que cumpla con los anteriores requerimientos deberá establecer un convenio con la Superintendencia de Vigilancia Privada para presentarse como Operador Biométrico Homologado.

4.6.4. ASPECTOS TÉCNICOS GENERALES

La Plataforma Tecnológica que soporta el proceso del Sistema Integrado de Seguridad en la realización de la evaluación y certificación de aptitud psicofísica por parte de las Instituciones Especializadas, estará a cargo de los proveedores homologados. Sus instalaciones y las del sistema de respaldo (sistema espejo), deberán estar ubicadas en la República de Colombia, en un sitio seguro, con controles de acceso y vigilancia, que permita procesos de auditoría sobre la información. Lo compone además de los elementos de hardware requeridos, un conjunto de programas (software) que garantizan la adecuada operación. A su vez, el Sistema Integrado de Seguridad es el encargado del envío de la información solicitada por la Supervigilancia en tiempo real.

Los servidores centrales del Sistema Integrado de Seguridad deben tener la capacidad necesaria para garantizar el procesamiento de las operaciones realizadas en las Instituciones Especializadas, con la concurrencia que el mercado demande. Estos servidores deben tener la capacidad de ser expandidos a medida que aumenten y/o cambien las necesidades. El Sistema Integrado de Seguridad debe estar desplegado sobre una infraestructura en alta disponibilidad y contar con un CPD de respaldo para garantizar la continuidad de servicio conforme el futuro contrato con las Instituciones Especializadas.

El Sistema Integrado de Seguridad deberá tener una infraestructura tecnológica estable que garantice la disponibilidad de la información almacenada en una las bases de datos: información de control, resultados de los eventos, información de los registros o transacciones generadas. Debe tener como mínimo:

- Un arreglo de servidores redundantes, comunicaciones redundantes, un sistema de red de comunicación de datos y una base de datos relacional. El servidor o servidores deberán cumplir con los requerimientos de conectividad y seguridad (se utilizan como guía los estándares IEEE 802 y 27001).
- Registrar todas las transacciones y operaciones realizadas desde los computadores y equipos ubicados en las Instituciones Especializadas e interconectados al Sistema Integrado de Seguridad: Transacciones, eventos, datos de control, así como eventos de funcionamiento del Sistema Integrado de Seguridad. Toda transacción debe ser replicada al sistema redundante de respaldo. Se debe de garantizar que el 100 % de las transacciones se encuentran replicadas al momento de requerirse la entrada en operación del sistema de respaldo.
- Registro de todo el proceso de evaluación y certificación en el Software de Gestión.
- Garantizar el correcto funcionamiento de las actividades del Sistema Integrado de Seguridad en la Institución Especializada.
- Generar los mecanismos de seguridad de la información en línea, a través de alarmas y alertas.
- Con la manifestación de interés presentada ante la Superintendencia de Vigilancia y Seguridad Privada, se entiende que la compañía aspirante a proveedor conoce que está obligado a generar todos los reportes y cruces de información que sean solicitados por la Superintendencia.

  Lo anterior con base en las características y componentes del sistema integrado de seguridad según lo reglamentado en el artículo 2.6.1.1.10.1.3 del Decreto 26 de 2017.

4.6.5. COMPONENTES DEL SISTEMA INTEGRADO DE SEGURIDAD Y SUS REQUERIMIENTOS TÉCNICOS.

El sistema técnico y en general el conjunto de sistemas e instrumentos técnicos o telemáticos, que posibiliten el registro, control e inspección; deberá disponer de los mecanismos de autenticación suficientes para garantizar, entre otros, la confidencialidad e integridad en las

comunicaciones, validación, autenticidad y cómputo, el control de su correcto funcionamiento y el acceso a los componentes del sistema informático.

Los proveedores deben disponer del material de software, equipos, sistemas, terminales e instrumentos en general, necesarios para el desarrollo de las actividades de inspección, vigilancia y control; debidamente homologados bajo los requerimientos técnicos y el establecimiento de las especificaciones necesarias para su funcionamiento.

El proceso conforme a lo dispuesto en el Decreto 026 de 2017, deberá disponer de los componentes y características que se describen a continuación:

I. Centro de Operaciones de Seguridad SOC. El cual estará conformado por un grupo de personas, procesos, infraestructura y tecnología dedicados a gestionar, tanto de forma reactiva como proactiva, amenazas, vulnerabilidades y en general incidentes de seguridad de la información, con el objetivo de minimizar y controlar el impacto en la organización. Para este proceso se necesitará proveer de sistemas Hardware, software, comunicaciones, dispositivos de seguridad, servicios de integración y gestión de proyecto. A continuación, se detallan los elementos Hardware y Software necesarios.

- Seguridad Física y Ambiental. Deberá prever amenazas como desastres naturales, incendios accidentales, amenazas ocasionadas por el hombre, sabotajes internos y externos deliberados.
- Control de acceso. Deberá contar con un control de acceso biométrico a través de huella dactilar, o de reconocimiento facial, o de verificación de patrones oculares. Se validará que cumplan con los estándares actuales para el acceso biométrico seleccionado.
- Protección electrónica. El SOC deberá contar con un sistema de circuito cerrado de televisión, que permita monitorear y registrar las actividades de ingreso y las que se realizan al interior del SOC y el control sobre los elementos activos y pasivos dentro del mismo.
- Condiciones Ambientales. El SOC debe contar con elementos de detección y extinción de fuego, en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.

- El SOC debe contar con un esquema de evacuación, y su personal debidamente capacitado ante desastres.
- Seguridad del Equipamiento. Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos solo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados. Para protegerlos se debe tener en cuenta que: La temperatura no debe sobrepasar los 23°C, deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores). Sistema de Aire Acondicionado. Se debe proveer un sistema de ventilación y aire acondicionado. Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de inundaciones, en caso de utilizar sistemas de enfriamiento por agua se verificará que estén instaladas redes de protección en todo el sistema de cañería al interior y al exterior.
- El SOC deberá contar con un esquema seguridad contra desastres naturales como sismos, terremotos e inundaciones, deberá contar con un esquema de evacuación ante terremoto.
- Sistema de Alimentación Ininterrumpida (SAI). EL SOC deberá contar con un sistema de corriente regulada en línea y de contingencia que garantice la operatividad en ausencia del sistema de suministro de energía principal por un tiempo mínimo de 4 horas continuas. Se verificará en la visita.
- Seguridad Lógica. Control de acceso a través Identificación y Autenticación, políticas de protección de acceso de acceso a la información en todos los equipos. Todos y cada uno de los equipos que se encuentren en el SOC deberán contar con sistemas que permitan definir políticas de protección de acceso a la información, como lo son usuarios y contraseñas.
- Deberá contar con los siguientes elementos de seguridad informática:

  - SIEM: Solución basada en hardware o software para la correlación de eventos de seguridad generados por el equipamiento y aplicaciones de la red de la plataforma tecnológica del Sistema Integrado de Seguridad.

    La solución utilizada deberá encontrarse en el cuadrante de Leaders o Visionaries del Magic Quadrant Security Information and Event Management de Gartner.

- FIREWALL PERIMETRAL UTM: Solución basada en hardware o software que deberá tener los servicios activos de Firewall, IPS (Intrusion Prevention System), Escáner de Vulnerabilidades de Red, firewall de aplicaciones web y antivirus de Red. Debe tener como mínimo 1 Gbps de throughput y fuente redundante o alta disponibilidad. Leaders, Visionaries o Challengers del Magic Quadrant for Unified Threat Management (UTM).

  La solución utilizada deberá encontrarse en el cuadrante de Leaders, Visionaries o Challengers del Magic Quadrant for Unified Threat Management (UTM).

- ENDPOINT: Software para protección antimalware de los servidores de sistemas operativos, bases de datos y de aplicaciones que se utilicen en el Sistema Integrado de Seguridad.

II. Centro de Procesamiento de Datos (CPD). El Centro de Procesamiento de Datos es aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información del Sistema Integrado de seguridad y deberá cumplir con todas las condiciones técnicas de un Datacenter TIER III y los estándares de la ISO 27001.

III. Sistema Multibiométrico.

El proponente deberá proveer una plataforma que incluya un motor multibiométrico, cuyo fin será permitir identificar de múltiples maneras los usuarios utilizando las diferentes posibilidades de reconocimiento biométrico (multidáctilar, rostro, huella, voz).

El proponente deberá garantizar que la entidad será propietaria de toda la información biométrica recolectada y que en caso de que el futuro se cambie el proveedor deberá entregar la base de datos con todos registros existentes en ella en formato que permita ser utilizado por cualquier sistema.

Con el fin de crear dicha base de datos el proponente deberá proveer los equipos o mecanismo a través los cuales se realizara el enrolamiento de los usuarios del sistema mediante capturara las huellas y el rostro y la voz y de esta manera empezar a poblar la base de datos; el sistema deberá garantizar que se podrá hacer búsquedas 1 a N (con la toma de

la huella, o el rostro, o la voz, el sistema deberá estar en capacidad de poder hacer una búsqueda en toda la base de datos e identificar el usuario o actor del sistema con toda su información, con el fin de validar la identidad de un usuario registrado en el sistema de seguridad.

Todo el proceso de inscripción biométrica se deberá llevar a cabo con todos los actores que intervienen en el proceso y los solicitantes, los cuales deberán leer del código de la cedula y cargar los datos demográficos, esta misma funcionalidad se deberá poder tener en una aplicación para smartphones. Los datos mínimos que se deben capturar en la base de datos se dividen en dos partes:

1. Datos demográficos
   a. Nombre
   b. Apellidos
   c. Fecha de nacimiento
   d. Número de identificación
   e. Género
   f. Foto del documento de identificación
2. Datos biométricos
   a. 2 huellas dactilares (índice derecho e izquierdo)
   b. 1 Imagen multidactilar
   c. 1 imagen facial
   d. 1 registro de la voz

Este proceso no debe demorar más de 90 segundos en total.

El proceso de inscripción deberá está diseñado para verificar la calidad de la muestra biométrica para la huella, el multidactilar, el rostro ó la voz e inscribir con precisión al sujeto en la base de datos, el flujo general del sistema es como sigue:

1 Validación de la autenticidad del documento.

2 Lectura del código de la cedula de ciudadanía

3 Carga de los datos demográficos

4 Cargue de la foto de la cedula

5 Toma de foto usuario

6 Toma de la huella.

7 Toma de la imagen multidactilar

8 Validación del patrón o template multidactilar

9 Registro de voz

10 Cargue de datos en la base de datos de la entidad

Como se describe en los pasos anteriores, se deberá crear una evaluación de la calidad para cada muestra biométrica que se obtendrá del sujeto y se deberá hacer 3 reintentos para tomar una muestra perfecta para poder mantener una base de datos biométricos de alta calidad, los datos se deberán incluir en un paquete con los datos demográficos y actualizan la inscripción de la persona.

La plataforma deberá ser accesible para los diferentes usuarios del sistema desde diferente canales por intermedio de una página web que deberá contar con todos los esquemas de seguridad (certificado ssl, cifrado de contraseñas, esquemas redundantes, servicios en alta disponibilidad) también deberá proveer una aplicación móvil que permita hacer la validación de la identidad de la personas que se encuentran validadas dentro del sistema.

IV. Otros Requerimientos. El aspirante deberá presentar un documento técnico que permita garantizar la idoneidad del mismo. El documento técnico deberá contar con los siguientes capítulos:

a. El aspirante debe anexar el esquema de soporte para atención de los ANS (Acuerdo de Niveles de Servicio) de la solución completa.
b. El aspirante a homologación podrá tener subcontratado el servicio de Centro de Operaciones de Seguridad SOC. En este caso deberá presentar el contrato firmado con el proveedor que le preste el servicio de SOC mínimo por veinticuatro (24) meses y las hojas de vida del equipo de seguridad podrán ser funcionarios del proveedor de SOC y cumpliendo con la totalidad de Requerimientos administrativos exigidos para el equipo de trabajo. Se aclara que el único responsable ante la Superintendencia por los ANS (Acuerdo de Niveles de Servicio) es el homologado y no el SOC contratado.
c. En caso de presentar desarrollos propios, se debe adjuntar copia del certificado de registro de soporte lógico de la Dirección Nacional de Derechos de Autor. En el caso de que el aspirante utilice una licencia de software de una

solución fabricada por otra compañía, el aspirante deberá adjuntar copia de la respectiva licencia.

d. El aspirante a homologación podrá tener subcontratado el servicio de Centro de Procesamiento de Datos (CPD). En este caso deberá presentar el contrato firmado con el proveedor que le preste el servicio de CPD mínimo por veinticuatro (24) meses y cumpliendo con la totalidad de Requerimientos exigidos. Se aclara que el único responsable ante la Superintendencia por los ANS (Acuerdo de Niveles de Servicio) es el homologado y no el CPD contratado.
e. El proveedor deberá suministrar Hardware, Software, Comunicaciones y Servicios de Integración y Gestión de Proyecto.

Lo anterior con base en las características y componentes del sistema integrado de seguridad según lo reglamentado en el artículo 2.6.1.1.10.1.3 del Decreto 26 de 2017.

5. SISTEMA DE GESTIÓN DE CALIDAD

El Sistema de Gestión de Calidad tiene como objetivo estandarizar y unificar los sistemas de gestión que las Instituciones Especializadas establecen para realizar sus actividades de certificación de personas.

Asegurar que los organismos de certificación de personas que operan los esquemas de certificación de la aptitud Psicofísica, trabajen de forma coherente, comparable y confiable.

Cumplir la reglamentación y legislación legal vigente aplicable a las Instituciones Especializadas, unificar los criterios de evaluación definido por este sistema de gestión, con lo cual se busca proporcionar y mantener la confianza para todas las partes interesadas. Así mismo, se establecen las características del esquema de certificación que deberán implementar todos Las Instituciones Especializadas. El Sistema de Gestión de Calidad regulado en el presente acto, deberá ser implementado por cada Institución Especializada.

Lo anterior con base en lo reglamentado en el numeral 5 del artículo 2.6.1.1.10.1.3 del Decreto 26 de 2017.

5.1 Referencias Normativas o Marco Legal

El Sistema de Gestión de Calidad, deberá garantizar el cumplimiento de la normatividad legal vigente que regula la certificación de la aptitud psicofísica tales como:

La Ley 1119 de 2006 del Ministerio de Defensa.

Decreto Ley 019 de 2012

La Ley 1539 de 2012.

Sentencia C-850 de 2013 Corte Constitucional, de la ley 1539 de 2012.

Decreto 2525 de 2003

Decreto 2858 de 2007

Decreto 4675 de 2007

Resolución 2984 de 2007

Resolución 2056 de 2007

Decreto 0738 de 2013

Decreto 2368 de 2012

o en cualquier norma que la adicione, modifique, complemente o reglamente.

5.2 Definiciones

Gestión: Actividades coordinadas para dirigir y controlar una organización en lo referente en la calidad.

Sistema: conjunto de elementos mutuamente relacionados que interactúan entre sí.

Sistema de Gestión de Calidad: Es el Sistema de Gestión de Calidad que cumple con los Requerimientos de la Norma NTC ISO/IEC 17024:2013, o en cualquier norma que la adicione, modifique, complemente o reglamente, y que asegura que los organismos de certificación de personas que operan los esquemas de certificación de la aptitud psicofísica, trabajen de forma coherente, comparable y confiable bajo un solo criterio unificado y/o modelo técnico. Este estandariza los criterios, tablas de equivalencia, técnicas de evaluación y calificación, entre otras.

Certificado médico de aptitud psicofísica para la tenencia y el porte de armas de fuego. Es el documento expedido y suscrito por un médico que actúa en nombre y representación de una Institución Especializada, dotada con los equipos y el personal necesario e inscrita en el Ministerio

de Defensa Nacional-Dirección General de Sanidad Militar-Subdirección de Servicios de Salud, en el cual se certifica que el aspirante a obtener por primera vez la autorización y/o revalidación para la tenencia y el porte de armas de fuego, posee la capacidad de visión, capacidad auditiva, agudeza visual y campimetría, y la coordinación integral motriz adecuada a las exigencias que se requieren para dicha actividad de alto riesgo.

Esquema de Certificación: Requerimientos específicos de certificación relacionados con categorías especificadas de personas a las que se aplican las mismas normas y reglas particulares, y los mismos procedimientos. Es facultad exclusiva del Estado el diseño, desarrollo y validación del esquema de certificación.

Proceso de Certificación: Todas las actividades reguladas en el presente anexo que deben cumplir Las Instituciones Especializadas para evaluar y expedir la certificación de aptitud física, mental y de coordinación motriz.

Evaluación: Proceso regulado en el presente anexo mediante el cual se evalúa en los Solicitante/Aspirante el cumplimiento de los Requerimientos del esquema de certificación, que conduce a una decisión de certificación.

Examen: Mecanismo regulado en el presente anexo que hace parte de la evaluación, que mide la competencia de un Solicitante/Aspirante por uno o varios medios, tales como, medios científicos, orales, prácticos y por observación.

Competencia: Capacidad demostrada de aptitudes y/o habilidades y atributos personales, como se define en el esquema de certificación.

Solicitante/Aspirante: Persona que requiere al Organismo de Certificación de Personas su participación en el proceso de certificación de un esquema de certificación de acuerdo a la finalidad perseguida por el solicitante/aspirante, de la siguiente manera: civil, deportistas y coleccionistas de armas de fuego, fuerzas militares y servicios de vigilancia y seguridad privada.

Examinador: Persona con las calificaciones técnicas y personales pertinentes, que es competente para llevar a cabo y/o calificar un examen.

Calificación: Demostración de atributos personales, educación, formación y/o experiencia laboral.

Apelación: Solicitud presentada por un aspirante, candidato o persona que requiere la certificación, para reconsiderar cualquier decisión

adversa tomada por la Institución Especializada relacionada con el estado de certificación deseada.

Queja: Solicitud, en el ámbito de la evaluación de la conformidad, distinta de una apelación, presentada por una organización o persona a un OC de Certificación de Personas, de acción correctiva relacionada con las actividades de la Institución Especializada.

Agudeza Auditiva: Capacidad de discriminación de estímulos auditivos a través de una audiometría en cabina sonoamortiguada para determinar los niveles mínimos de audición que tiene la persona en cada uno de los oídos.

Agudeza Visual: Capacidad de discriminar detalles de los objetos a una distancia determinada, teniendo en cuenta factores como condiciones de luminosidad, contraste y tamaño. Se evalúa la visión cercana y la visión lejana, visión del color, deslumbramiento o saturación luminosa, córnea, retina, cristalino, órbita, parpados, motilidad extrínseca, afecciones traumáticas, fusión, estereopsis, agudeza visual cinética.

Anamnesis: Información general del candidato obtenida a partir de una entrevista inicial y que se consigna en la primera parte de la historia clínica.

Auditoría: Proceso sistemático, independiente y documentado para la obtención de evidencias de cumplimiento del Sistema de Gestión de Calidad, confrontándolo con las normas vigentes de los entes reguladores, orientadas al mejoramiento de su calidad y rendimiento.

Auditoría Externa: Las auditorías externas incluyen las que se denominan generalmente auditorías de segunda y tercera parte. Las auditorías de segunda parte las realizan las partes que tienen interés en la organización, por ejemplo, los clientes. Las auditorías de tercera parte las realizan organizaciones auditoras externas e independientes, con autoridad para certificar o acreditar una compañía bajo una norma de gestión establecida.

Auditoría Interna: Auditoría que realiza la organización al Sistema de Gestión de Calidad implementado. La puede realizar personal interno.

Sistema Obligatorio de Garantía de Calidad de Atención en Salud del Sistema General de Seguridad Social en Salud (SOGCS): Es el conjunto de instituciones, normas, Requerimientos, mecanismos y procesos deliberados y sistemáticos que desarrolla el sector salud para generar, mantener y mejorar la calidad de los servicios de salud en el país.

Calidad de la Atención de Salud: Se entiende como la provisión de servicios de salud a los usuarios individuales y colectivos de manera accesible y equitativa, a través de un nivel profesional óptimo, teniendo en cuenta el balance entre beneficios, riesgos y costos, con el propósito de lograr la adhesión y satisfacción de dichos usuarios.

Sistema Único de Habilitación: Es el conjunto de normas, requerimientos y procedimientos mediante los cuales se establece, registra, verifica y controla el cumplimiento de las condiciones básicas de capacidad tecnológica y científica, de suficiencia patrimonial y financiera y de capacidad técnicoadministrativa, indispensables para la entrada y permanencia en el Sistema, los cuales buscan dar seguridad a los usuarios frente a los potenciales riesgos asociados a la prestación de servicios y son de obligatorio cumplimiento por parte de los Prestadores de Servicios de Salud y las EAPB.

Condiciones de Capacidad Tecnológica, Científica y de Infraestructura: Son los requerimientos básicos de estructura y de procesos que deben cumplir los Prestadores de Servicios de Salud por cada uno de los servicios que prestan y que se consideran suficientes y necesarios para reducir los principales riesgos que amenazan la vida o la salud de los usuarios en el marco de la prestación del servicio de salud.

Auditoría para el mejoramiento de la calidad de la atención de salud: Es el mecanismo sistemático y continúo de evaluación y mejoramiento de la calidad observada respecto de la calidad esperada de la atención de salud que reciben los usuarios.

Software de Gestión de Calidad: Es una herramienta tecnológica cuyo fin es centralizar, unificar y controlar todas las actividades propias del Sistema de Gestión de Calidad de las Instituciones Especializadas a nivel nacional.

Comité Técnico: Es la Instancia asesora del Ministerio de Defensa y/o de la Superintendencia de Vigilancia Privada, encargada de proponer modificaciones, revisar, actualizar y avalar el esquema de certificación, las metodologías y los documentos que lo respaldan.

Miembros del Comité Técnico: Los miembros del comité del esquema de certificación son funcionarios del Ministerio de Defensa y/o de la Superintendencia de Vigilancia Privada que demuestran competencia para desarrollar, revisar y validar el Esquema de Certificación. Esta facultad podrá ser delegada en el proveedor del Sistema.

Método de Evaluación: El método de evaluación será el regulado en el marco legal vigente. La validación de cada uno de los métodos deberá

ser suministrado por el proveedor de los equipos utilizados por La Institución Especializada.

Esquema de Certificación: Requerimientos específicos para evaluación y certificación, regulados en la norma ISO 17024:2013 o el marco legal vigente y desarrollado en el presente anexo, que deben cumplir el solicitante/aspirante que deseen obtener o renovar el permiso para el porte y tenencia de armas de fuego

Condiciones de capacidad tecnológica y científica: Son los Equipos y Medios Tecnológicos idóneos y requeridos para que cada uno de las Instituciones Especializadas pueda desempeñar sus actividades de evaluación conforme a la normatividad vigente.

Instituciones Especializadas: Son las instituciones que cuentan con la facultad para realizar la evaluación y certificación de la aptitud Psicofísica para la tenencia y porte de armas de fuego autorizadas por la entidad competente.

Sistema Integrado de Seguridad: Es una infraestructura tecnológica operada por cualquier ente público o privado previamente homologado por la Superintendencia de Vigilancia Privada, para asegurar el cumplimiento de los parámetros técnicos mínimos que le permita prestar con calidad el servicio para garantizar la expedición segura del certificado de aptitud psicofísica.

Validez: Los proveedores de los equipos e instrumentos utilizados en la evaluación suministrarán la información suficiente donde se garantiza que las pruebas miden lo requerido por el esquema de certificación.

Equidad: El esquema de certificación garantizará por sí mismo la igualdad de oportunidades de éxito a todos los solicitante/aspirantes.

Fiabilidad: La fiabilidad de las evaluaciones, sin perjuicio del evaluador o momento en que se realicen las pruebas, será garantizada por el esquema de certificación toda vez que se aplicarán las mismas formas de evaluación en todas las Instituciones Especializadas a todos solicitante/aspirantes.

Desempeño: Cada Organismo garantizará la forma como el personal cumple con lo establecido en el Esquema de Certificación, a través de la evaluación del desempeño.

Baremación: Los baremos iniciales serán suministrados por los proveedores de los diferentes equipos de evaluación y posteriormente el Software de Gestión ajustará los baremos de aprobación de conformidad con la población específica colombiana.

5.3. Requerimientos Generales
5.3.1 Temas Generales

Las Instituciones Especializadas, deberán cumplir con los siguientes documentos que los acreditan como una entidad legal, que en cualquier momento la Superintendencia los podrá solicitar:

Certificado de existencia y de representación legal de la sociedad.

Certificado de matrícula mercantil del establecimiento de comercio.

Formulario de inscripción en el registro especial de prestadores de servicios de salud.

-- El Certificado como organismo certificador de personas expedido por el ONAC - norma ISO/IEC 17024:2013

-- Resolución de inscripción en el Registro otorgada por el Ministerio de Defensa Nacional – Dirección General de Sanidad Militar – Subdirección de Salud

Certificado de suficiencia patrimonial.

Balance general suscrito por un contador con tarjeta profesional y fotocopia de la cédula de ciudadanía.

Concepto de uso de suelos.

Licencia de construcción.

Permiso de vertimientos líquidos y de emisiones atmosféricas.

Sistema de prevención y control de incendios.

Plan de emergencias y desastres.

Planes de mantenimiento de la planta física, instalaciones físicas e instalaciones fijas.

Planes de mantenimiento de los equipos.

Certificación Invima de persona idónea para el mantenimiento de equipos biomédicos.

Certificación de instalaciones eléctricas, expedida por un ingeniero eléctrico, un técnico del SENA en electricidad, donde indique que la instalación se encuentra actualizada con el Reglamento Técnico Internacional de Instalaciones Eléctricas.

Lo anterior según lo dispuesto en el artículo 2.6.1.1.10.1.4. del Decreto 26 de 2017, donde se reglamentan las entidades autorizadas que solo podrán interactuar con el Sistema Integrado de Seguridad.

5.3.2. Responsabilidad en Materia de Decisión de la Certificación
Las Instituciones Especializadas son responsables por las certificaciones que emiten para lo cual deberán contratar bajo su responsabilidad, mediante contrato laboral al personal certificador.

5.3.3 Gestión de la Imparcialidad

5.3.3.1 El organigrama de los Centros de Reconocimiento de Personas

Deberá respetar como mínimo el siguiente esquema:

ORGANIGRAMA DE LA ALTA DIRECCIÓN DE LA INSTITUCIÓN ESPECIALIZADA

Este será susceptible de ampliaciones de conformidad a las necesidades de la empresa, el mercado, etc.

Las instituciones especializadas, implementarán el procedimiento para gestionar la imparcialidad.

Cada Institución Especializada, deberá publicar la declaración por la cual establece la importancia que se da a la imparcialidad en el proceso de evaluación y certificación.

5.3.3.2 Todo el personal de la Institución Especializada, deberá estar sensibilizado en la imparcialidad del proceso, frente a sus solicitantes, candidatos y personas certificadas, por lo que en el área de inducción se deberá capacitar a los evaluadores y certificadores del procedimiento de imparcialidad.

5.3.3.3 El Sistema de Gestión de Calidad, al contar con procedimientos estandarizados obligatorios para todas las evaluaciones, permite por sí solo que el proceso de evaluación y certificación sea equitativo para todos los solicitantes, candidatos y personas certificadas, así mismo no permite establecer algún tipo de restricción para acceder a la certificación y obliga a dar cumplimiento a lo establecido en las normas técnicas y legales vigentes.

5.3.3.4 Cada Institución Especializada podrá realizar convenios, alianzas o acuerdos comerciales, pero deberá registrar en la matriz de riesgos suministrada por el Sistema de Gestión de Calidad los controles que adelanta para garantizar que los acuerdos comerciales no generan

presiones indebidas que afecten la imparcialidad de las certificaciones. Lo anterior sin perjuicio en lo dispuesto en el artículo 2.6.1.1.10.2.2. del Decreto 026 de 2017 donde se reglamentan las instituciones y condiciones que deberán cumplir para poder contratar o celebrar convenios.

5.3.3.5 Las Instituciones Especializadas deberán diligenciar la matriz de riesgo, donde se identifican y gestionan las amenazas a la imparcialidad de manera continua y sistemática.

5.3.3.6 Al ser mandato legal el proceso de certificación se estructuró y gestionó de manera que garantiza y salvaguarda la imparcialidad del proceso de evaluación y certificación.

5.3.3.7. Responsabilidad Legal y Financiamiento. Solamente podrán operar como organismos de certificación de personas quien demuestre tener los recursos financieros suficientes para la operación. Las Instituciones Especializadas deberán realizar un estudio de factibilidad del negocio y del costo de la implementación del mismo para, de acuerdo con los resultados, determinar si cuenta con los recursos financieros suficientes para cubrir la compra o alquiler de equipos biomédicos e informáticos, adecuación de instalaciones, contratación del personal durante por lo menos doce meses, pago de servicios de auditoría y acreditación y demás elementos requeridos para la operación.

Las Instituciones Especializadas que operan al momento de ser promulgado este documento deberán demostrar la suficiencia patrimonial y financiera requerida por las normas legales vigentes para continuar operando, por lo que el representante legal deberá reportar a la Superintendencia de Vigilancia Privada de la información financiera del costo de su operación en el mes inmediatamente anterior, el precio de venta de cada examen y el valor de otros ingresos, para demostrar que La Institución Especializada es viable económicamente. Esta información será reportada a la DIAN para lo de su competencia.

El incumplimiento durante tres meses continuos de este numeral será causal de suspensión de la acreditación y desconexión del Software de Gestión hasta tanto demuestre que se encuentra en condiciones económicas y financieras para operar.

5.3.4 REQUERIMIENTOS RELATIVOS A LA ESTRUCTURA

5.3.4.1 Dirección y Estructura de la Organización

5.3.4.1.1 La Institución Especializada, da cumplimiento a este requisito con el organigrama establecido.

5.3.4.1.2 Los individuos responsables de las siguientes actividades son:

a) Junta de socios o propietario, definen las políticas relativas a la operación La Institución Especializada, aporta el capital inicial o de trabajo;

b) El gerente o representante legal establece los procedimientos requeridos para la operación, contrata personal, realiza seguimientos al cumplimiento de las políticas establecidas por la junta de socios o dueño, gestiona recursos, firma acuerdos, contratos.

El responsable del área de calidad que puede ser el mismo gerente/representante legal, implementa el Sistema de Gestión de Calidad única nacional, protocolos, programa de capacitación, programas de mantenimiento de equipos e instalaciones;

c) El contador es el responsable de las finanzas del organismo de certificación, quien informará al gerente/representante legal de la viabilidad financiera de la operación.

d) El desarrollo y mantenimiento del esquema de certificación está a cargo de la norma legal vigente;

e) Los profesionales en área de la salud como psicología, optometría, fonoaudiología y medicina general serán los responsables de la evaluación;

f) Las decisiones relativas a la certificación estará a cargo de cualquier profesional de la salud.

5.3.4.2 Estructura del Organismo de Certificación en relación con las actividades de Formación

Este requisito no aplica ya que Las Instituciones Especializadas no realizan actividades de formación.

5.3.5 REQUERIMIENTOS RELATIVOS AL PERSONAL

5.3.5.1 Requerimientos Generales al Personal

5.3.5.1.1 Mínimo una vez al año La Institución Especializada realizará evaluación y seguimiento al desempeño del personal (Recepcionista, Psicología, Optometría, Fonoaudiología, Medicina General y certificación) que interviene en el proceso de certificación. Esta evaluación de desempeño debe ser registrada en el software único de gestión en cuanto fecha de realización, resultado de la misma y método empleado.

5.3.5.1.2 Cada Institución Especializada deberá contar al menos con el siguiente personal para realizar sus actividades de certificación.

– Un Psicólogo;

– Un Optómetra;

– Un Fonoaudiólogo;

– Un Médico general;

– Un Profesional de la salud (con función de certificador);

– Personal Técnico, administrativo y subalterno que resulte necesario. La Institución Especializada, debe asegurar que el personal evaluador y certificador cuenta con la competencia necesaria, para lo cual el Sistema de Gestión de Calidad, cuenta con el procedimiento "Gestión Humana" en el que se establece la metodología para asegurar la competencia del personal.

La Institución Especializada debe asegurar y demostrar que el personal con el que cuenta es suficiente para el volumen de atención que realiza.

5.3.5.1.3 En el Software de Gestión, se publican los perfiles de cargo en el que se establecen los deberes y responsabilidades de los evaluadores y certificadores.

5.3.5.1.4 Las Instituciones Especializadas, deben mantener actualizado en su archivo físico los registros que demuestren, calificaciones, formación, experiencia, competencias para el personal evaluador y certificador.

5.3.5.1.5 El Sistema de Gestión de Calidad cuenta con mecanismos de control que permiten garantizar la confidencialidad de la información que se genera en el proceso de evaluación y certificación de la aptitud psicofísica.

5.3.5.1.6 La Institución Especializada, debe contratar laboralmente al personal que interviene en el proceso de evaluación y certificación. Así mismo se deberán realizar las evaluaciones establecidas en la Resolución 2346 de 2007 del Ministerio de la Protección Social.

5.3.5.1.7. Cuando La Institución Especializada certifique a alguno de sus funcionarios, la evaluación deberá realizarse bajo supervisión para prevenir cualquier conflicto de interés que afecte la imparcialidad de las actividades.

5.3.5.2 Personal Que Interviene En El Proceso De Certificación

5.3.5.2.1 Generalidades

El personal que labora en La Institución Especializada debe registrar en el Software de Gestión, las personas hasta tercer grado de consanguinidad y afinidad, para que en el momento que estos soliciten certificación, se realice supervisión de las actividades de evaluación.

5.3.5.2.2 Requerimientos para examinadores.

5.3.5.2.2.1 El personal evaluador debe cumplir con los siguientes requerimientos:

– Hoja de vida

– Certificados laborales o

– Certificados de estudio o

– Diploma universitario

– Acta de grado.

– Carné y/o resolución de inscripción en la seccional de salud que realizará sus funciones.

– Tarjeta profesional para quienes aplique de acuerdo a su fecha de grado.

Posterior al proceso de contratación, se debe realizar una etapa de inducción en la que se asegure que cada evaluador conoce y es capaz de realizar las pruebas requeridas en la normatividad legal vigente para la certificación de la aptitud Psicofísica.

- ✓ Esta inducción debe cumplir con el siguiente esquema:
- ✓ Fase Inducción: Temas / Responsable / Método
- ✓ Segunda: Sensibilización: Se da a conocer Director de Presentaciones
- ✓ Tercera: Sensibilización en normatividad vigente para expedir certificados de aptitud psicofísica e instructivos de evaluación y manejo de equipos.
- ✓ Cuarta: Evaluación de la inducción
- ✓ Fase teórica: Se da a conocer la normatividad, pruebas a realizar y criterios de aprobación.

- ✓ Fase práctica: Una vez explicada la parte teórica, se procede a realizar etapa práctica y se evalúa la adherencia a los temas impartidos.

Fase	Temas	Responsable	Método
Primera	Inducción		
Segunda	Sensibilización		
Tercera	Normatividad Vigente		
Cuarta	Evaluación de la inducción		
Fase teórica			
Fase práctica			

Para evaluador y certificador solo puede ser un profesional para que se encargue de esta actividad

El responsable de la evaluación debe ser una persona diferente al que dictó la capacitación.

Documental y presencial.

La evaluación de la inducción deber ser realizada en el Software de Gestión.

5.3.5.2.2.2 Cuando se evidencie que alguno de los funcionarios involucrados en el proceso de evaluación (Recepción, evaluadores, certificador) tiene algún conflicto de interés, La Institución Especializada deberá realizar supervisión de las actividades para evitar que la confidencialidad e imparcialidad de las evaluaciones no se vea afectada. Esta supervisión deberá dejarse registrada.

5.3.5.2.3 Requerimientos relativos a otro personal

El personal administrativo que interviene en el proceso de evaluación y certificación, (calidad, recursos humanos, gerencia) no puede realizar presiones indebidas en los evaluadores y certificadores. De presentarse alguna presión indebida, el profesional deberá registrar el hecho en el espacio de observaciones del Software de Gestión.

5.3.5.2.3.1 Contratación externa

La Institución Especializada debe tener acuerdos documentados con todos los proveedores de productos y servicios relacionados directamente en el proceso de evaluación y certificación en los que se salvaguarde la confidencialidad y se eviten conflictos de interés.

La evaluación no puede ser subcontratada, esta debe ser realizada únicamente por el organismo habilitado y acreditado.

Cuando el organismo de certificación contrata externamente trabajos relacionados con la certificación debe:

a) Asumir la responsabilidad total por el trabajo contratado externamente;

b) Asegurarse de que el organismo que realiza los trabajos contratados externamente es competente y cumple las disposiciones aplicables de esta Norma internacional, para lo cual se debe utilizar el formato evaluación de proveedores suministrado por el Sistema de Gestión de Calidad;

c) Evaluar y hacer el seguimiento del desempeño de los organismos que realizan los trabajos contratados externamente de acuerdo con sus procedimientos documentados;

d) Tener registros que demuestren que los organismos que realizan los trabajos contratados externamente cumplen todos los Requerimientos pertinentes del trabajo contratado externamente;

e) Mantener una lista de los organismos que realizan trabajos contratados externamente.

5.3.5.2.3.2 Otros recursos

Las Instituciones Especializadas deben realizar las actividades de evaluación y certificación de la aptitud psicofísica utilizando instalaciones adecuadas, equipos y recursos requeridos en la normatividad legal vigente.

5.3.5.2.4 Requerimientos relativos a los registros y la información

5.3.5.2.4.1 Registros de solicitantes, candidatos y personas certificadas

Los registros del proceso de evaluación y certificación como informe y certificado se almacenan magnéticamente en el Software único de gestión, y en archivo físico para los Centros de Reconocimiento que deseen imprimir los registros del proceso.

Los registros de certificación llevarán un consecutivo para cada Institución Especializada, solo podrán acceder a ellos personal autorizado como evaluadores y certificadores, con lo cual se salvaguarda la confidencialidad de la información.

Este numeral no aplica, ya que si una persona certificada pierde alguna de sus facultades no es posible retirar la certificación emitida.

5.3.5.2.5 Información Pública

Cada Institución Especializada podrá consultar en cualquier momento si una persona posee una certificación vigente, válida, y su respectivo alcance ingresando al Software de Gestión.

5.3.5.2.5.1 SELECCIÓN (Recepción)

Esta etapa comprende el proceso de recepción en el cual se selecciona a los aspirantes que ingresarán a la evaluación

DETERMINACIÓN (Evaluación)

ATESTACIÓN (Certificación)

Aquí se deben tener en cuenta los requerimientos que se han establecido para ser admitido en el proceso de evaluación y certificación.

Una vez que se ha cumplido con los Requerimientos definidos en la etapa de selección, se pasa al proceso de determinación que comprende 4 evaluaciones a saber: Psicomotriz, Audiometría, Visiometría, y por último y sin excepción alguna, se realiza la evaluación de medicina general.

Una vez han sido realizadas las 4 evaluaciones citadas en la etapa anterior, un profesional de la salud basado en los criterios de aprobación definidos en la normatividad legal vigente, tomará la decisión de otorgar la certificación de aptitud psicofísica.

Realizada la atestación, el certificado es publicado a la plataforma del DCCA Y/O DE LA SUPERVIGILANCIA.

5.3.5.2.5.2. Los Requerimientos para acceder al proceso de evaluación y certificación son los siguientes:

Personas civiles para el porte y tenencia de armas de fuego.	Personal de vigilancia y seguridad privada LEY 1539 DE 2012
• Cancelar el valor del examen • Ser mayor de edad	• Presentar cedula original • Ser mayor de edad

• Presentar el documento de identidad • Permitir tomar una fotografía • Permitir la captura de su huella • Permitir la captura de su firma manuscrita.	• Permitir tomar una fotografía • Permitir escanear el documento de identidad • Permitir la captura de su huella • Permitir la captura de su firma manuscrita • Ser remitido por una ARL. • Que la empresa en que labora cuente con orden de servicio vigente autorizada por la ARL.

Lo anterior según lo dispuesto en el artículo 2.6.1.1.10.1.2 en los numerales 1 al 8 del Decreto 26 de 2017.

5.3.5.2.6 Confidencialidad

La divulgación de la información solo podrá realizarse por intermedio del Software de Gestión y podrá acceder solo el personal autorizado con usuario, contraseña y autenticación biométrica dactilar, que son únicas e intransferibles.

Todo el personal que labora en La Institución Especializada, debe firmar las actas de conflicto de interés, confidencialidad e imparcialidad.

Las únicas fuentes autorizadas para recibir información sensible de los solicitantes / candidatos es el personal de Recepción, y evaluación (Psicólogo, Optometría, Fonoaudiología, Medicina General). Esta información solo puede ser divulgada por solicitud escrita cuando la ley así lo requiera.

La Institución Especializada debe registrar en la matriz de riesgos la manera en que asegura que los organismos relacionados no comprometen la confidencialidad.

5.3.5.2.7 Seguridad

5.3.5.2.7.1 Las medidas de seguridad que se deben implementar para evitar el fraude durante el proceso de certificación son las siguientes:

a) Una vez la institución Especializada ha entregado toda su documentación que soporta que es un establecimiento legal, se procederá a crear la institución especializada y sus usuarios en el Software de Gestión;

b) Todos los usuarios del Software de Gestión, deberán contar de un usuario y contraseña;

c) El sistema validará que un usuario con el rol de "Médico general/Psicólogo/Fonoaudiólogo/Optómetra/Profesional certificador" se encuentren totalmente enrolados, es decir que hayan cargado su documento de identidad, capturado su información biométrica (Foto, Firma, Huellas, multidactilar, rostro, y/o voz) y registrado su información personal. Si no se encuentran enrolados el Software de Gestión, no se permitirá su ingreso y por lo tanto no podrán participar en el proceso de evaluación de un examen médico;

d) Todos los solicitantes deberán tener una cita previa en una institución especializada para proceder a realizar un examen médico, el Software de Gestión valida con el recaudador que el solicitante tenga un PIN valido de lo contrario no se permite la creación de la cita;

e) Antes de iniciar el proceso de evaluación del examen médico el/la recepcionista carga el documento de identidad, captura la información biométrica (Foto, Firma, Huellas, multidactilar, rostro y/o voz) y registra la información personal del solicitante, el Software de Gestión valida la identidad del solicitante apoyado en RNEC y Centrales de riesgo.

f) Durante el proceso de evaluación del examen médico cada profesional de la salud y el paciente deberán validar biométricamente a través de su huella y/o multidactilar y/o rostro y/o voz, al inicio y al final de cada prueba, el Software de Gestión valida la identidad del paciente y del médico;

g) Durante todo el proceso, el sistema registra logs de auditoría que posteriormente se analizan con la ayuda de un correlator de eventos para generar alertas que indiquen procedimientos fuera del proceso establecido.

5.3.5.2.7.2 Los exámenes: Los exámenes que se aplican para evaluar la aptitud psicofísica y los rangos de aprobación, están publicados en la normatividad legal vigente, por lo cual todos los aspirantes / candidatos pueden conocer el material de los mismos. Sin embargo se han establecido los siguientes controles:

a) Para acceder al material de los exámenes cada evaluador debe ingresar al Software de Gestión con su respectivo usuario, contraseña y autenticación biométrica;

b) La naturaleza de los exámenes son electrónicos;

c) La seguridad se mantiene durante todo el proceso de examen, ya que solo acceden a ellos personal autorizado y que ha firmado acuerdos de confidencialidad e imparcialidad;

d) No se considera ninguna amenaza por el uso repetido de los exámenes.

5.3.5.2.7.3 Las Instituciones Especializadas deben evitar las tentativas de fraude en el examen:

a) Los candidatos al firmar el formulario de solicitud se comprometen a no divulgar los exámenes que se practican ni tomar parte en prácticas fraudulentas;

b) Los candidatos nunca pueden estar solos en los lugares de evaluación, se requiere de la permanente vigilancia de los evaluadores;

c) El Software de Gestión requiere la confirmación de identidad del aspirante / candidato en todo el proceso de evaluación y certificación. Si la verificación no es satisfactoria, no se puede iniciar el procedimiento;

d) En la entrada de cada lugar de evaluación se debe colocar un aviso en el que se informe la prohibición de utilizar durante la ejecución de los exámenes aparatos electrónicos como celulares, Tablet, etc.;

e) Los resultados de los exámenes quedan inmodificables una vez han sido guardados en las plantillas del Software de Gestión.

5.3.5.2.8. Esquemas de certificación

5.3.5.2.8.1 Las Instituciones Especializadas, deben aplicar el esquema de certificación definido en este documento, el cual está desarrollado con las evaluaciones y los criterios de aprobación establecidos en la normatividad legal vigente para la expedición del certificado de aptitud psicofísica.

5.3.5.2.8.2. El esquema de certificación desarrollado en el Sistema de Gestión de Calidad, contiene:

a) Alcance de la certificación

El alcance de las certificaciones de la aptitud psicofísica que pueden ser expedidas por Las Instituciones Especializadas son las siguientes:

- Certificado Médico de Aptitud Psicofísica para porte y tenencia de armas de fuego personal civil, para el trámite del salvoconducto.

- Certificado Médico de Aptitud Psicofísica para el personal de Vigilancia y Seguridad Privada.

b) Estos deberán estar publicados en un lugar de fácil visualización;

c) Una persona certificada en este esquema ha cumplido con uno de los Requerimientos para solicitar, renovar el permiso de salvoconducto o lo establecido por la Ley 1539 de 2012 y la norma que la reglamente, adicione, modifique o sustituya;

d) Para acceder al proceso de evaluación y certificación, no se requiere de competencia específica, ya que se certifican aptitudes físicas, mentales y de coordinación motriz que posee un individuo;

e) Las Aptitudes que se requieren para obtener la certificación son las establecidas por la normatividad legal vigente como son físicas, mentales y psicomotríz

f) Los pre-requerimientos son los establecidos en la normatividad legal vigente para la realización de los exámenes médicos de aptitud psicofísica;

g) El código de conducta que un aspirante y candidato es el siguiente:

1. Es obligación del aspirante o persona certificada mantener un trato cordial y respetuoso no utilizar lenguaje vulgar o soez con las personas que se encuentren dentro de las instalaciones del centro de certificación de personas, en especial hacia el personal administrativo, médicos y profesionales de la salud del centro.

2. Todo aspirante está obligado a no fumar, consumir bebidas alcohólicas o sustancia psicoactivas durante su permanencia en las instalaciones del centro de certificación de personas.

3. Es obligación de todo aspirante NO ofrecer dinero, dadivas o sobornos a los profesionales de la salud o cualquier otro funcionario del centro de certificación de personas para cambiar o mejorar los resultados de las evaluaciones psicofísicas practicadas, so pena de incurrir en prisión.

4. En caso que se requiera alguna información adicional para poder tomar la decisión de certificación, el aspirante está en la obligación de proveerla en un plazo menor a 60 días y de esta manera poder culminar el proceso de certificación.

5. Durante todas las declaraciones, interrogatorios y evaluaciones dadas durante el proceso de certificación el aspirante mantendrá un total apego a la verdad y es consciente de las implicaciones legales que le acarreará cualquier falta en este aspecto.

6. Está terminantemente prohibido el porte de armas durante la permanencia del aspirante en las instalaciones del centro de certificación de personas.

5.3.5.2.8.3. Los Requerimientos del proceso de certificación de la aptitud Psicofísica son los siguientes:
a) Criterios para la certificación inicial y la renovación.

Certificación inicial: Para otorgar un certificado de aptitud Psicofísica, se evalúa al candidato frente a los Requerimientos establecidos en la normatividad legal vigente los cuales han sido contemplados en este documento.

Renovación de la certificación: No es posible realizar renovación de las certificaciones aptitud psicofísica, ya que la normatividad que la reglamenta exige realizar la certificación sin tener en cuenta datos históricos, de tal manera que toda certificación se realiza como una solicitud inicial;

b) Métodos de evaluación, debido a que la normatividad legal vigente que reglamenta la expedición de la certificación de la aptitud psicofísica establece evaluaciones en áreas de la salud como audiometría, Visiometría, psicología y medicina general, los métodos de evaluación están definidos propiamente en ellas mismas.

Estos métodos están detallados en los instructivos de evaluación visual, auditiva, psicomotriz y medicina general, los cuales hacen parte integral del Sistema de Gestión de Calidad;

c) Métodos y criterios de vigilancia, suspender y retirar la certificación. Los criterios de vigilancia, suspensión y retiro de la certificación no aplican, ya que la normatividad legal vigente que reglamenta la expedición de la certificación de la aptitud Psicofísica no los establece.

d) Criterios para efectuar cambios en el alcance o en el nivel de la certificación. La normatividad legal vigente que reglamenta la expedición de la certificación de la aptitud psicofísica establece toda certificación como una solicitud inicial, por lo cual una vez emitida la misma no es posible realizar modificaciones en su alcance o nivel ya certificado.

El esquema de certificación al ser propiedad del Estado colombiano, el desarrollo, revisión y validación le corresponde a este.

Las Instituciones Especializadas no son dueños del esquema de certificación de la aptitud psicofísica, pero deben asegurar que aplica lo

establecido en este ibídem comentario anterior, así como los demás Requerimientos contemplados en este documento.

5.3.5.3. REQUERIMIENTOS RELATIVOS AL PROCESO DE CERTIFICACIÓN

5.3.5.3.1. PROCESO DE SOLICITUD

El Sistema de Gestión de Calidad, suministrará a todos Las Instituciones Especializadas del país, el formato SOLICITUD, el cual contendrá como mínimo los siguientes elementos:

a) Número de PIN;
b) Nombres y apellidos completos del solicitante;
c) Fecha de nacimiento AAAA/MM/DD;
d) Estado civil;
e) Grupo sanguíneo y RH;
f) Afiliación a EPS;
g) Dirección de residencia;
h) Domicilio;
i) Teléfono;
j) Escolaridad;
k) Categoría;
l) Trámite;
m) Autorizaciones y consentimientos:
    1) Acepto cumplir con las disposiciones, obligaciones y deberes pertinentes al esquema de certificación.
    2) Autorizo que la información de mi historia clínica y mis datos personales, biométricos, confidenciales y sensibles, sean tratados, procesados, examinados, verificados y custodiados por La Institución Especializada.
    3) Autorizo el reporte ante el Departamento de Comercio de Control y Comercio de Armas (DCCA Y/O DE LA SUPERVIGILANCIA), del Ministerio de Defensa, solamente el contenido de la información de mi historia clínica que sea requerida para la expedición de mi certificado de Aptitud Psicofísica para el Porte y Tenencia de Armas de fuego.
    4) Declaro que haré buen uso del certificado de aptitud expedido por el Centro de Reconocimiento de y que no presentaré declaraciones relativas a la certificación.
    5) Acepto el tratamiento de mis datos sensibles o revisión de la información y registros asociados contenidos en mi historia clínica por: Organismo Nacional de Acreditación de Colombia, Superintendencia de Vigilancia Privada, Ministerio de Defensa Nacional – Dirección General de Sanidad Militar – Subdirección

de Salud o alguna otra entidad diferente a las autorizadas por Ley? SÍ ____ NO _____
Nota: Los datos sensibles son aquellos que afectan la intimidad del titular o cuyo uso indebido pueda generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las condiciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición como los datos relativos a la salud, a la vida sexual y los datos biométricos.

6) Si al final del proceso de certificación se expide el certificado, me comprometo a informar sin demora sobre cuestiones que puedan afectar mi capacidad para la certificación ofrecida, si este evento ocurre antes de realizar el trámite ante el organismo de tránsito.
7) Me comprometo a no divulgar ningún material de los exámenes confidenciales realizados, ni tomar parte en prácticas fraudulentas de examen en la institución ESPECIALIZADA.
8) Me comprometo a no adulterar, falsificar, ni utilizar este certificado y emitir declaraciones de manera engañosa o no autorizada, so pena de responder civil, penalmente ante las autoridades de la República de Colombia.
9) Conozco el procedimiento y evaluaciones médicas de certificación psicosensométrica que se me van a practicar en la institución ESPECIALIZADA y doy mi CONSENTIMIENTO INFORMADO al INSTITUCIÓN ESPECIALIZADA para realizar dichas evaluaciones definidas en el esquema de certificación, el cual me ha sido explicado por el personal de recepción de la institución ESPECIALIZADA. Así mismo he leído y comprendo el esquema de certificación descrito en la cartelera de la INSTITUCIÓN ESPECIALIZADA. Expreso voluntariamente mi intención de participar en las evaluaciones médicas, después de haber comprendido la información que se me ha dado acerca de los objetivos de las evaluaciones, mis derechos y responsabilidades.
10) Firmo este documento al frente LEGITIMANDO mi capacidad legal para consentir.

En esta etapa del proceso de certificación, el Software de Gestión debe validar la identidad de la persona que realiza la solicitud confrontándola contra la réplica de la base de datos del operador de validación biométrica de la Registraduría Nacional del Estado Civil. Registrará en la

base de datos la información obtenida de la validación para efectuar las comprobaciones de identidad en cada punto del proceso de evaluación y certificación. Conforme a lo anterior según lo dispuesto en el artículo 2.6.1.1.10.1.3. Numeral 4. del Decreto 026 de 2017

Igualmente en esta etapa se dará a conocer el proceso de certificación, los derechos de los solicitantes y deberes de las personas certificadas y las tarifas

Cada Institución Especializada, deberá verificar la solicitud para confirmar que el solicitante cumple con los Requerimientos para acceder al proceso de evaluación y certificación de la aptitud psicofísica.

5.3.5.3.2. PROCESO DE EVALUACIÓN

El proceso de evaluación establecido en el Sistema de Gestión de Calidad, implementa el esquema de certificación establecido en la norma legal vigente, así:

Cumplir con los Requerimientos establecidos en el presente documento para ser admitido en el proceso de certificación.

La Institución Especializada deberá aplicar los métodos de evaluación definidos en el sistema de gestión.

Aplicar las evaluaciones valiéndose de personal calificado, medios tecnológicos y sistematizados requeridos para cada evaluación.

Aplicar criterios de aprobación establecidas en la norma vigente para la certificación de la aptitud psicofísica.

Validar la identidad del candidato al inicio y al final de cada prueba.

Validar la identidad del profesional de la salud al inicio y al final de cada prueba.

El proceso podrá iniciar por cualquiera de las áreas de optometría, audiometría y psicología.

Para acceder a la evaluación de medicina general, el candidato deberá haber practicado previamente las evaluaciones de optometría, audiometría y psicología.

Una vez registradas las primeras cien mil pruebas en el Software de Gestión, esta herramienta establecerá los tiempos mínimos para cada una de las evaluaciones. En caso de error por parte del evaluador en la utilización del Software de Gestión, se deberá generar la evidencia necesaria.

No se podrá iniciar simultáneamente dos pruebas para el mismo evaluado.

No se podrá iniciar simultáneamente dos pruebas por el mismo evaluador salvo en el área de psicología, en donde se permitirá máximo tres candidatos al mismo tiempo.

La Institución Especializada deberá garantizar la realización de todas las pruebas establecidas en la normatividad vigente para expedir la certificación de la aptitud psicofísica.

5.3.5.3.3. PROCESO DEL EXAMEN

El proceso del examen establecido en el Sistema de Gestión de Calidad, aplica el esquema de certificación establecido en la norma legal vigente, así:

El salón destinado para cada uno de los exámenes, deberá contar con un área mínima de 10 m2 y el menor de los lados deberá medir mínimo 2.5 metros.

El examen de audiometría deberá realizarse en un medio sonoamortiguado, empleando una cabina insonora.

El proceso de examen deberá ser realizado por profesionales en cada una de las áreas correspondientes a psicología, optometría, fonoaudiología y medicina general, de conformidad en la norma legal vigente.

Cada Institución Especializada deberá garantizar la legalidad de los documentos que soporten los evaluadores dispuestos para el examen.

El examen se debe realizar teniendo en cuenta lo establecido en la norma legal vigente que reglamenta la expedición de la certificación de la aptitud psicofísica.

5.3.5.3.4. DECISIÓN DE LA CERTIFICACIÓN

La decisión de certificación debe ser tomada por un profesional de la salud competente e idónea que conoce los rangos de aprobación definidos en el esquema de certificación y que no participó en la evaluación del candidato a certificar.

– Esta actividad deberá ser realizada empleando el Software de Gestión.

– Cada Institución Especializada es responsable directo del otorgamiento de la certificación y, por ende, conserva su autoridad al respecto sin delegar, o poder delegar, a terceros sus decisiones pertinentes a la certificación.

– La Institución Especializada, como organismo de certificación de personas, garantiza el cumplimiento de la normatividad legal vigente sobre las cuales realiza la certificación de personas.

– Cada Institución Especializada, deberá emitir un certificado el cual será generado por el Software de Gestión y contendrá como mínimo la siguiente información:

Referencia a las normas por las cuales se expide el certificado.

Referencia al organismo de certificación.

NIT del organismo de certificación. Dirección y teléfono del organismo.

Registro IPS del organismo.

Fecha de expedición y vencimiento.

Registro de habilitación ante el Ministerio de Defensa.

Número de registro de inscripción ante secretaria de salud.

Logo de acreditación del ONAC con su respectivo código.

Fotografía del candidato.

Tipo de trámite y categoría certificada. Servicio solicitado.

Información básica del candidato como nombres, apellidos, número de documento, teléfono, fecha de nacimiento, dirección y ocupación.

Concepto de cada una de las áreas evaluadas.

Firma de los profesionales que evaluaron (optómetra, fonoaudiólogo, psicólogo y medico evaluador)

Firma del certificador.

Firma y huellas de la persona certificada.

5.3.5.3.6. PROCESO DE RENOVACIÓN DE LA CERTIFICACIÓN

La renovación de la certificación no aplica debido a que la norma legal vigente que reglamenta la expedición de la certificación de la aptitud psicofísica, establece evaluaciones de aptitud física, mental y de coordinación motriz, las cuales pueden variar con el tiempo, por ello las

condiciones de certificación no se pueden mantener y toda solicitud de certificación debe ser realizada como inicial.

5.3.5.3.7. USO DE CERTIFICADOS, LOGOS Y MARCAS

Las Instituciones Especializadas que proporcionan una marca o logo de certificación, deberán documentar las condiciones de uso y gestionar adecuadamente los derechos de uso y representación.

5.3.5.3.8. APELACIONES CONTRA DECISIONES DE CERTIFICACIÓN

El Sistema de Gestión de Calidad proporcionará el procedimiento para la gestión de las apelaciones contra las decisiones de certificación en el cual se establece la metodología para recibir, evaluar y tomar decisiones relativas a las apelaciones.

La Institución Especializada deberá entregar a cada apelante un recibido de su solicitud.

En el software de Gestión cada Institución Especializada, deberá registrar las apelaciones que reciba, así como su respectivo seguimiento y respuesta.

Este procedimiento debe estar publicado en las carteleras de la Institución Especializada.

QUEJAS

El Sistema de Gestión de Calidad proporcionará el procedimiento para la gestión de las quejas en el cual se establece la metodología para recibir, evaluar y tomar decisiones relativas a las quejas.

La Institución Especializada deberá entregar a cada persona un recibido de la queja que ha registrado

En el Software de Gestión cada Institución Especializada, deberá registrar las quejas que reciba, así como su respectivo seguimiento y resolución de la misma.

Este procedimiento debe estar publicado en las carteleras de la Institución Especializada.

5.3.6. REQUERIMIENTOS RELATIVOS AL SISTEMA DE GESTIÓN

El sistema de gestión se desarrolla siguiendo los lineamientos de la norma NTC ISO/IEC 17024:2013, o su versión vigente, la cual define los Requerimientos que debe cumplir una organización que se dedica a la certificación de personas.

El Sistema de Gestión de Calidad tendrá una sola estructura documental para todos Las Instituciones Especializadas, capaz de apoyar y demostrar el cumplimiento coherente de los Requerimientos de la norma NTC ISO/IEC 17024:2013.

El Sistema de Gestión de Calidad documenta cada uno de los Requerimientos aplicables a la norma NTC ISO/IEC 17024:2013, y cuenta con procedimientos para el control de documentos, control de registros, acciones correctivas, acciones preventivas, auditorías internas, y revisión por la dirección.

5.3.7. IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE CALIDAD

El Sistema de Gestión de Calidad, entrará en vigencia una vez sea promulgado el acto administrativo y tendrá un periodo de transición de máximo 90 días para ser implementado por todos y cada uno de Las Instituciones Especializadas. Solamente una vez extinguido este plazo será exigible la implementación del Sistema de Gestión de Calidad por los organismos de acreditación.

5.3.7.1. SEGUIMIENTO AL CUMPLIMIENTO DEL SISTEMA DE GESTIÓN DE CALIDAD

El seguimiento al cumplimiento del Sistema de Gestión de Calidad estará a cargo del Organismo Nacional de Acreditación de Colombia o quien haga sus veces, para lo cual se apoyará en los medios tecnológicos y sistematizados del Software de Gestión.

Las Instituciones Especializadas serán auditadas continuamente por la Superintendencia de Vigilancia Privada y la institución ESPECIALIZADA que no cumpla con las exigencias establecidas en el Sistema de Gestión de Calidad, se le aplicarán las medidas pertinentes.

5.3.7.2. SEGURIDAD

El Sistema de Gestión de Calidad, para evitar el fraude durante el proceso de evaluación y certificación, deberá documentar e implementar el cumplimiento de los siguientes protocolos de seguridad:

Se deberá validar la presencia del solicitante/candidato y del personal evaluador durante todo el proceso de evaluación y certificación mediante los protocolos de seguridad definidos por el Ministerio de Defensa y la Superintendencia de Vigilancia Privada.

El personal evaluador y certificador solo podrá ingresar al Software de Gestión del Sistema de Control y Vigilancia con usuario, contraseña y autenticación de la huella dactilar.

5.4. SOFTWARE DE GESTIÓN DEL SISTEMA INTEGRADO DE SEGURIDAD

El Software de Gestión del Sistema Integrado de Seguridad, implementado por Las Instituciones Especializadas, deberá contar con los siguientes módulos integrados con las funcionalidades que se describen a continuación:

5.4.1. Módulo de Agendamiento Único de Citas

Deberá contener una plataforma web para el solicitante que requiera agendar una cita para el servicio de Examen de Aptitud Psicofísica en las Instituciones Especializadas autorizadas.

El solicitante para poder agenciar su cita, deberá haber comprado un (1) PIN del servicio para el examen médico de aptitud a través de los aliados de recaudo de los proveedores del Sistema Integrado de Seguridad.

Las plataformas de agendamiento de citas deberán validar antes de asignar una cita la veracidad del PIN y que no haya sido utilizado.

Las plataformas de agendamiento deberán permitir al solicitante la búsqueda geográfica de las Instituciones Especializadas autorizados a través de un mapa georreferenciado donde pueda indicar la ubicación donde realizará dicha búsqueda.

Las plataformas de agendamiento deberán permitir generar el formulario de datos básicos para el diligenciamiento previo al examen al asignar la cita.

Las plataformas de agendamiento deberán permitir verificar, reprogramar o cambiar las citas de los solicitantes. Para reprogramar o cambiar una cita de un solicitante, este lo deberá hacer con una antelación mínima de veinticuatro (24) horas.

5.4.2. Módulo de Software del Sistema de Gestión de Calidad

Se definirán y validarán las siguientes funcionalidades y requerimientos:

1. Registro del Centro (NIT, Nombre, Matrícula Mercantil, Registro de Prestador, Resolución de Habilitación del Ministerio de Defensa, Registro de Acreditación ante el ONAC y sus anexos) y de los equipos de evaluación (Audiómetros, Visiómetros, Baterías Psicomotrices, fonendoscopios, tensiómetros, entre otros), con su respectiva marca, modelo, referencia y seriales.

2. Registro de las calibraciones de los equipos de cada INSTITUCIÓN ESPECIALIZADA, de la fecha de calibración y de su vigencia, entidad

que expide el certificado o documento de calibración con su soporte. El software deberá llevar el histórico de todas las calibraciones de los equipos.

3. Registro de mantenimientos preventivos y correctivos de los equipos.

4. Registro y control de la verificación de equipos diariamente, conforme a lo dispuesto en el Sistema de Gestión de Calidad, generación de alarmas por no realizar el registro de la verificación de los equipos diariamente en los periodos establecidos.

5. Registro de los médicos autorizados por el Ministerio de Defensa con su registro de soporte expedido por dicha Entidad, se deberá incluir el respectivo registro médico de cada profesional o especialista con su respectivo registro ante la Secretaría de Salud en que se encuentra inscrito el profesional de la salud.

6. Además de las funcionalidades incorporadas en los demás módulos.

5.4.3. Módulo de Administración

En este módulo se definirán las Instituciones Especializadas con datos tales como: NIT, Nombre o Razón de la Empresa, Sedes acreditadas o establecimientos de comercio, ID DCCA Y/O DE LA SUPERVIGILANCIA, Departamento, Municipio, Zona a la que pertenece, Dirección, Teléfono, Datos del Representante Legal (Tipo ID, No. de ID, Nombres, Apellidos, Registro y Validación de Identidad), Horarios y Cupos de cada sede o establecimiento donde se guardará el soporte del Anexo de la acreditación en su última versión, Resolución de Habilitación del Ministerio de Defensa y su soporte.

El representante legal o administrador que delegue el representante legal realizará el registro de todos los usuarios (administradores, recepcionistas, especialistas y médicos).

5.4.4. Módulo de Enrolamiento o Registro

Se realizará el registro de todos los actores que intervienen en el proceso y de los solicitantes. El registro del solicitante se realizará previa verificación del PIN y de su utilización, se escaneará toda la información del documento de identificación la que se encuentra impresa y en el código de barras bidimensional para la verificación de la legitimidad del documento, luego se procederá al registro de las huellas de los índices derecho e izquierdo a través de los lectores dispuestos, y se enviará al operador tecnológico de la RNEC, la cual responderá con el hit de validación positivo o negativo con su certificación digital y estampado cronológico al Software de Gestión del Sistema de Control y Vigilancia,

adicionalmente se registrará el multidactilar, el rostro y/o registro de la voz que servirán como mecanismo redundante de identificación y autenticación durante todas las evaluaciones.

5.4.5. Módulo de Evaluación de Pruebas

En este módulo solo deberán tener permisos de acceso, particulares a su perfil, los médicos o especialistas designados para cada labor y creados previamente por el Representante Legal de la institución ESPECIALIZADA. Se realizará la validación de identidad del especialista o médico a través del sistema multibiométrico como mecanismo redundante al principio y al final de cada prueba (psicomotriz, auditiva, visión y médica), además del control de los tiempos mínimos de cada prueba y el registro y validación de los criterios de evaluación conforme a lo dispuesto en la normatividad vigente.

5.4.6. Módulo de Certificación

En este módulo solo deberán tener permisos de acceso, particulares a su perfil, los médicos designados para esta labor y creados previamente por el Representante Legal de la institución ESPECIALIZADA. Se realizará la validación de identidad del médico a través del sistema multibiométrico (huella, multidactilar, rostro o voz) como mecanismo redundante al final de la decisión de certificación del examen. Dentro de las funcionalidades está el verificar el cumplimiento de los criterios de evaluación de cada una de las pruebas realizadas y aprobar o requerir aclaraciones a los especialistas que deberán quedar registrados en el Software de Gestión del Sistema de Control y Vigilancia.

5.4.7. Expedición del Certificado

En la expedición del certificado de aptitud Psicofísica realizada por los médicos o especialistas de cada INSTITUCIÓN ESPECIALIZADA autorizado, serán emitidos a través del Software de Gestión del Sistema de Control y Vigilancia una vez validado todo el proceso.

Conforme a lo anterior según lo dispuesto en el artículo 2.6.1.1.10.1.2. del Decreto 026 de 2017, donde se reglamenta todo el proceso de registro, evaluación y certificación como protocolo de seguridad a través del sistema integrado de seguridad en su componente de software de gestión.

5.5. VISITAS DE VERIFICACIÓN A LOS ASPIRANTES A PROVEEDORES DEL SISTEMA INTEGRADO DE SEGURIDAD

Se realizarán las siguientes visitas en máximo dos (2) días hábiles. En estas visitas el evaluador tomará evidencia, fotográfica y fílmica para verificar el cumplimiento de los requerimientos.

Se deberá tener a disposición los recursos necesarios para poder realizar las verificaciones. En la visita se verificarán los siguientes requerimientos:

a) Verificación de mapa de ubicaciones de centros y máquinas. Se deberá mostrar la ubicación de por lo menos dos centros de reconocimiento en la cual se muestre el estado de su conexión;

b) Verificación de la extracción de la información del documento de identidad;

c) Verificación de tramitación del PIN contra la entidad de recaudo.

5.5.1. Visita al Centro de Operaciones de Seguridad

b) El centro de operaciones de seguridad deberá contar con un control de acceso biométrico;

c) El centro de operaciones de seguridad deberá contar con un sistema de circuito cerrado de televisión;

d) El centro de operaciones de seguridad deberá estar ubicada en territorio nacional;

e) Se deberá tener a disposición de los recursos necesarios para poder realizar las verificaciones;

f) Prueba de ataque perimetral. El especialista de hacking presentado en el equipo de trabajo del SOC, deberá ejecutar un escaneo de puertos a una de las direcciones de red utilizadas por el sistema presentado a homologar. Posterior a esto el IPS deberá identificar, registrar y reaccionar ante este escaneo procediendo a interrumpir la comunicación entre el escáner atacante y el sistema. Posterior a esto el evento deberá quedar registrado en la herramienta de SIEM;

g) Verificación en la base de datos de información biométrica cifrada. El aspirante deberá mostrar la ubicación en la cual se almacene la información biométrica con el fin de verificar que esta se encuentre cifrada;

h) Verificación de Endpoint. Se deberá demostrar que se encuentran instaladas en los servidores la solución de antimalware.

5.5.2. Visita a una Institución Especializada

Se deberá mostrar el funcionamiento del Sistema de Control y Vigilancia. Se procederá a realizar visita a una (1) INSTITUCIÓN ESPECIALIZADA en el cual se encuentre instalada la solución y se permita verificar los siguientes escenarios:

1. Verificación del proceso de pago. Se deberá demostrar el pago del valor del examen de aptitud directamente sobre la red de recaudo del actor del aliado de recaudo. Esto deberá cumplir con todos los requerimientos exigidos en la lista de chequeo del anexo técnico. En el caso de requerirse participación del aliado de recaudo para realizar esta verificación, el aspirante será el encargado de coordinar todos los Requerimientos para poder realizar la prueba. Se verificará además la consulta de validez y consumo de un (1) número PIN con un solicitante y un convenio.

2. Verificación del proceso de enrolamiento y operación de los diferentes actores de las Instituciones Especializadas. Se deberá demostrar que el Software de Gestión del Sistema Integrado de Seguridad, realice el registro de empresas, establecimientos comerciales u organismos certificadores de personas y sus respectivos Representantes Legales, Personal Administrativo, Médicos, Especialistas con su correspondiente perfil y de los solicitantes; así como capturar la información biométrica, biográfica y datos complementarios conforme al Sistema de Gestión de Calidad definido en este documento, a través de los siguientes dispositivos:

i. Lector biométrico de huellas con funcionalidad activa de dedo vivo (LFD).

ii. Cámara con sensor digital de alta definición que genera imágenes nítidas, deberá soportar el esquema estándar de reconocimiento facial a través de software.

iii. Captura y extracción de la información del Código Bidimensional contenido en la cédula de ciudadanía con los parámetros de la ficha técnica vigente a través de Pistola y/o Escáner de lectura de código bidimensional.

iv. Captura y digitalización de firmas manuscritas a través de un Pad de firmas Tableta digitalizadora.

v. Se aceptará proveedores que planteen una opción tecnológica que incluya todas o algunas de las funciones requeridas anteriormente en un solo dispositivo (Lector biométrico de huellas, lector multidactilar, cámara digital, pistola y Pad de firmas, entre otros).

vi. Verificación de validación de equipos. Se deberá demostrar que un dispositivo de hardware interno incorporado en cada PC del INSTITUCIÓN ESPECIALIZADA, permita la identificación y realice la validación geofísica de los PCS registrados, cada 60 minutos integrado con el SOC en el servidor de validación de geo-posicionamiento. Además deberá extraer la información de la dirección MAC y el número de serie de la tarjeta madre del PC.

Verificaciones a realizar:

vii. Verificación de la integración con la plataforma del Operador tecnológico de la RNEC a través de la validación de la template de la huella dactilar capturada las huellas dactilares tomadas temporalmente en la institución ESPECIALIZADA en el proceso de enrolamiento contra un ambiente de pruebas, verificando pertenecen y NO pertenecen al Médico, Especialista y solicitantes.

viii. Verificación de la presencia del solicitante y de los médicos o especialistas en todo el proceso de evaluación. Se deberá demostrar que el usuario se valide a través de la huella, multidactilar, rostro y/o voz al principio y final de cada evaluación, como mecanismo redundante de identificación y validación.

ix. La aplicación deberá contar con mecanismos alternos de validación en el proceso de enrolamiento para tramitar las excepciones de solicitantes con discapacidades que no les permita registrar y validar la huella dactilar requerida, mediante el multidactilar, el rostro y/o la voz.

1. Verifique que la aplicación continúa dentro del proceso de validación de identidad cuando no se pueda realizar la comparación de huellas dactilares mediante validación del multidactilar, el rostro y/o la voz contra la réplica de la base de datos de la RNEC para determinar la identidad del solicitante.

2. Verifique que la aplicación realice como mínimo cuatro (4) preguntas sociodemográficas del solicitante.

3. Verifique que las preguntas contengan un grupo de posibles respuestas en donde solo una es la correcta.

4. Verifique que la aplicación inicie el proceso de enrolamiento con otra IDENTIFICACIÓN BIOMÉTRICA diferente a la huella, en este caso del multidactilar, rostro y/o voz y EL NÚMERO DE CÉDULA, si el solicitante respondió correctamente las preguntas.

5. Verifique que la aplicación continúe en el proceso de validación de identidad si no se puede confirmar la identidad con el grupo de preguntas

y que la aplicación vuelva a presentar un segundo grupo de preguntas diferentes a las iniciales.

6. Verifique que la aplicación no realice más de dos intentos para validar la identidad del solicitante.

i. Validación de identidad con el proceso alternativo para Tarjetas de Identidad "TI" y Cédulas de Extranjería "CE".

ii. Compruebe que la aplicación realiza el escaneo del anverso y reverso del documento y valida que el documento es válido y no es falso.

iii. Compruebe que la aplicación almacena las imágenes como soporte del documento presentado por el candidato.

iv. Compruebe que se extrae la información legible del documento del código de barras del documento una vez este sea establecido como valido con tecnología de reconocimiento de caracteres "OCR".

v. Verifique que los datos han sido extraídos tanto del anverso como del reverso del documento "TI".

vi. Compruebe que se realiza una comparación de las huellas dactilares (huella extraída de la TI contra la huella capturada en el lector biométrico) y Compare el rostro extraído de la TI con el rostro capturado por el lector biométrico.

Conforme a lo anterior, según lo dispuesto en los artículos 2.6.1.1.10.1.2 y 2.6.1.1.10.2.3. del Decreto 26 de 2017.

5.6. Infraestructura Tecnológica en las Instituciones Especializadas

El aspirante a proveedor deberá suministrar y soportar los siguientes dispositivos, suministros y periféricos en Las Instituciones Especializadas con las siguientes características y/o funcionalidades:

– Un lector Biométrico de huellas dactilares con las siguientes especificaciones:
i. Tipo de Sensor Óptico, Resolución del Sensor: 500 dpi, Área de captura de la Imagen: 16 x 24 mm o superior, certificado por el FBI

ii. Observaciones: El lector biométrico serán propiedad del proveedor homologado y cualquier daño o pérdida de estos en los Centros será asumido por las Instituciones Especializadas donde se asignaron dichos elementos.

iii. Los elementos que sean asignados a una Institución Especializada, no podrán ser trasladados de ubicación (a otro INSTITUCIÓN ESPECIALIZADA u otro lugar).

iv. En los casos de detectar con evidencias el intento de manipulación o traslado de los dispositivos y suministros, el proveedor homologado impedirá a que continúen las validaciones de identidad desde la institución ESPECIALIZADA identificado y se le informará a la Superintendencia de Vigilancia Privada para lo pertinente.

– Pistola o Escáner Lector de Código de Barras Bidimensional.

– Cámara con sensor digital de alta definición y que genera imágenes nítidas, deberá soportar el esquema de reconocimiento facial ISO/IEC 197945 a través de software.

– Pad de firmas.

– Dispositivo de Identificación de Geoposición. Hardware interno que deberá cumplir la función de identificar la geoposición del Centro y PC mediante el uso de tecnología GPS:

i. Sincronización. GPS Mínimo 30 canales, Cobertura Nacional. El sistema de posicionamiento debe garantizar la permanente georreferenciación de la máquina en todo el territorio Nacional.

ii. Seguridad. El Representante Legal de la institución especializada será el responsable de la buena utilización del sistema de acuerdo a las recomendaciones del proveedor homologado con quien contrate el servicio, con el fin de evitar manipulación y/o daños que se puedan causar deliberadamente o de manera accidental al sistema.

iii. Precisión de ubicación. Radio máximo de veinte (20) metros de margen de error en la posición geográfica donde esté ubicada la antena en área urbana y (treinta) 30 metros en área rural en cobertura satelital.

iv. Actualización máxima de la georreferenciación, comunicación celular y/o satelital. Marcación del posicionamiento interno cada 60 minutos.

v. Envío de la información de la ubicación al centro de control y/o plataforma de monitoreo cada 60 minutos enviará una (1) posición con la identificación del PC, dirección MAC y número de serie de la tarjeta madre.

vi. Compatibilidad. Con los prestadores de servicios móviles de comunicación en cuanto a tecnología, cobertura y disponibilidad requerida, existentes en el mercado.

Los computadores de Las Instituciones Especializadas autorizados que interactúen con el Sistema de Control y Vigilancia deberán tener las siguientes características:

Línea de producto	Equipo corporativo certificado por el fabricante
Formato	Formato tipo Small Form Factor, Formato de Torre ó Mini PC, CPU – Monitor – Teclado Mouse, (original de fábrica.) (Equipo de Escritorio Corporativo)
Procesador	Core i5 3ª Generación ó superior
Memoria RAM	4 GB DDR3 ó superior
Almacenamiento Interno	Mínimo 320 GB ó Superior
Tarjeta de red	Tarjeta y Puerto 10M/100M/1000M Gb Ethernet
Ranuras de expansión	1 PCI Express X1 como mínimo
Sistema Operativo	Windows 7 Profesional Licenciado o Superior
Puerto serial	Uno como mínimo
Puertos USB	4 puertos USB 2.0 como mínimo
Comunicaciones	Tarjeta de Red 10M/100M/1000M Gb Ethernet.

5.7. Compromisos Posteriores

El aspirante a homologarse debe generar una carta de compromiso firmada por el representante legal, en la cual establezca que una vez reciba la homologación se comprometerá a realizar las siguientes actividades:

5.7.1. Los aspirantes a proveedores deberán presentar un documento de compromiso posterior, que la disponibilidad del servicio (ANS o SLA) con las Instituciones Especializadas deberá ser al iniciar la operación como mínimo del 98,5% con base en el horario de atención de las Instituciones Especializadas.

5.7.2. Antes de entrar en operación realizar las integraciones con la plataforma DCCA Y/O DE LA SUPERVIGILANCIA a través de webservices para que el DCCA Y/O DE LA SUPERVIGILANCIA valide si

la solicitud de registro en HQDCCA Y/O DE LA SUPERVIGILANCIA cumple con registro completo en Sistema de Control y Vigilancia a través del Software de Gestión. Y a establecer un canal dedicado con el sistema DCCA Y/O DE LA SUPERVIGILANCIA a cuenta del proveedor homologado.

5.7.3. Antes de entrar en operación realizar todas las integraciones con un operador tecnológico avalado por la Registraduría Nacional del Estado Civil para cumplir con el proceso de validar la identidad de los usuarios contra la Base de Datos de la RNEC. El operador tecnológico avalado por la Registraduría Nacional del Estado Civil deberá garantizar la validación de identidad a través de una réplica, licenciamiento y personal certificado conforme a los requerimientos de la RNEC, además deberá entregar junto con el hit de validación de identidad una certificación digital y estampado cronológico, además de seguridad e integridad en el log.

5.7.4. Establecer un canal dedicado y VPN a cuenta del proveedor homologado con el centro de monitoreo de la Superintendencia de Vigilancia Privada.