

COMPONENTE LOGÍSTICO PARA LA AUTENTICACIÓN BIOMÉTRICA FACIAL DE ELECTORES Y JURADOS DE VOTACIÓN.....	2
1. ALCANCE.....	2
2. ESPECIFICACIONES TÉCNICAS.....	3
3. CAPACITACIÓN.....	17
4. RECURSO HUMANO	18
5. OTRAS OBLIGACIONES DEL CONTRATISTA.....	20
6. ENTREGABLES	21

COMPONENTE LOGÍSTICO PARA LA AUTENTICACIÓN BIOMÉTRICA FACIAL DE ELECTORES Y JURADOS DE VOTACIÓN

1. ALCANCE

Para la prestación del servicio de componente técnico y logístico para la Autenticación Biométrica, a puesto, de Electores y Jurados de Votación para las elecciones de Congreso, presidente y vicepresidente de la República que se realizarán en el año 2026, mediante técnicas de biometría facial, el futuro contratista deberá:

- Implementar una solución integral que contemple la puesta a disposición de mil trescientos (1.300) celulares con conectividad, instalados con el aplicativo de verificación biométrica electoral de la Registraduría Nacional del Estado Civil y la logística necesaria para la operación y puesta en producción del servicio de biometría electoral en los puestos de votación definidos por la Entidad.
- Implementar una solución logística electoral que contemple el alistamiento logístico previo alistamiento técnico realizado por la Entidad, mobiliario, empaque, transporte, conectividad, comunicaciones e instalación de doscientos (200) equipos de captura facial avanzado (MFACE) en las ciudades de Bogotá, Medellín y Barranquilla.
- Implementar una solución integral que contemple la puesta a disposición de quinientas (500) tabletas para las elecciones de Congreso de la República y nueve mil quinientas (9.500) tabletas para la elección de Presidente y Vicepresidente de la República, todas instaladas con el aplicativo fuera de línea de verificación biométrica electoral de la Registraduría Nacional del Estado Civil, junto con la logística necesaria para la operación y puesta en producción del servicio de biometría electoral en los puestos de votación definidos por la Entidad.
- Contar con el recurso humano (operarios, técnicos, logísticos, administrativos y de seguridad) necesario que garantice la prestación del servicio de autenticación biométrica y que brinde de manera ágil, oportuna y eficaz soluciones a las fallas, incidentes, eventos y problemas que se puedan presentar antes y durante la jornada electoral.
- Disponer de los aspectos técnicos, tecnológicos, el recurso humano y la logística necesaria para implementar la autenticación biométrica facial, en los puestos de votación definidos por la supervisión del contrato.

2. ESPECIFICACIONES TÉCNICAS

2.1. Solución integral para la implementación de celulares con autenticación biométrica facial.

Para la puesta en marcha este servicio, el futuro contratista deberá como mínimo:

- Disponer de mil trescientos (1.300) kits biométricos con celular, donde cada kit biométrico incluye:
 - Medio de conectividad (SIMCARD) con conexión a internet, suministrado por el futuro contratista.
 - Operador del kit, suministrado por el futuro contratista.
 - Silla sin brazos.
- Disponer del personal de soporte para atender casos como: conectividad, instalaciones eléctricas, daño del celular o cualquier otro daño no asociado a la aplicación de verificación biométrica electoral de la Registraduría Nacional del Estado Civil.
- Instalar en los kits biométricos con celular, la aplicación de verificación biométrica electoral (APK), teniendo en cuenta las licencias entregadas por la Registraduría Nacional del Estado Civil, una vez terminada la jornada se realizará el borrador seguro correspondiente de conformidad con los lineamientos definidos por la Entidad.
- Implementar un esquema de operación que integre las siguientes actividades:
 - Disponer de personal que opere cada uno de los kits biométricos con celular, que garantice la operación continua del servicio.
 - Verificar la correcta operación de los kits biométricos con celular, junto con la app de verificación biométrica electoral validando previamente:
 - ✓ Que el votante pertenezca al puesto de votación y al censo de la mesa, según aplique.
 - ✓ Que el jurado se encuentre designado para el puesto de votación donde prestará el servicio.
 - ✓ El correcto cargue y despliegue de la información biográfica del ciudadano.
 - ✓ Que el aplicativo muestre el puesto y mesa de votación habilitado para el ciudadano.

- ✓ Que los kits biométricos se encuentren sincronizados con la hora legal colombiana fijada por el Instituto Nacional de Metrología (<http://horalegal.inm.gov.co/>).

2.2. Solución logística electoral con uso de equipos de captura facial avanzado (MFACE).

Para la puesta en marcha este servicio, el futuro contratista deberá como mínimo:

- Contar con los doscientos (200) kits MFACE, donde cada kit MFACE se conforma por:
 - Dispositivo móvil MFACE suministrado por la RNEC.
 - Minicomputador, suministrado por la RNEC.
 - Pantalla externa de mínimo 17 pulgadas, suministradas por la RNEC

Nota: Los elementos descritos, una vez entregados al Contratista, deberán ser reintegrados a la Entidad en la fecha de terminación del contrato, en las condiciones establecidas por la supervisión.

- Mouse USB externo, suministrado por el futuro contratista.
- Mesa, cuyo tamaño no debe ser mayor a 1x1 metros, que incluya un hablador con una infografía, diseñada acorde con la imagen corporativa de la Entidad, , la cual deberá ser aprobada previamente por la supervisión del contrato
- Silla sin brazos.

Estos kits serán instalados y operados por personal del futuro contratista en los puestos de votación que defina la Entidad.

- Disponer de antena satelital con servicio de internet como medio de conectividad para los kits MFACE, en las cantidades requeridas que aseguren la continua prestación del servicio durante la jornada electoral que sea autoinstalable y configurada conforme a los requerimientos de la Registraduría Nacional del Estado Civil.
- Disponer del personal de soporte para atender casos como: conectividad, instalaciones eléctricas o cualquier otro daño no asociado a los elementos suministrados por la Registraduría Nacional del Estado Civil que conforman el kit MFACE.

- Implementar un esquema de operación que integre las siguientes actividades:
 - Alistar e instalar los kits MFACE requeridos para la prestación del servicio, conforme a los requerimientos definidos por la supervisión del contrato.
 - Disponer de personal que opere cada uno de los kits MFACE.
 - Verificar la correcta operación de los kits MFACE constatando que el dispositivo permite realizar consultas e identificación biométrica incluyendo:
 - ✓ Que el votante pertenezca al puesto de votación y al censo de la mesa, según aplique.
 - ✓ Que el jurado se encuentre designado para el puesto de votación donde prestará el servicio.
 - ✓ El correcto cargue y despliegue de la información biográfica del ciudadano.
 - ✓ Que el aplicativo muestre el puesto y mesa de votación habilitado para el ciudadano.
 - ✓ Validar que los Kits MFACE se encuentren sincronizados con la hora legal colombiana fijada por el Instituto Nacional de Metrología (<http://horalegal.inm.gov.co/>).

2.3. Solución integral para la implementación de tabletas con autenticación biométrica facial fuera de línea.

- Disponer de quinientos (500) para Congreso de la República y nueve mil quinientas (9.500) kits biométricos con tableta para Presidente, donde cada kit biométrico incluye:
 - Operador del kit suministrado por el futuro contratista.
 - Silla sin brazos.
- Disponer del personal de soporte para atender casos como: instalaciones eléctricas, daño de la tableta o cualquier otro daño no asociado a la aplicación fuera de línea de verificación biométrica electoral de la Registraduría Nacional del Estado Civil.
- Instalar en los kits biométricos con tableta, la aplicación fuera de línea de verificación biométrica electoral (APK), teniendo en cuenta las licencias entregadas por la Registraduría Nacional del Estado Civil.
- Implementar un esquema de operación que integre las siguientes actividades:

- Disponer de personal que opere cada uno de los kits biométricos con tableta, que garantice la operación continua del servicio.
- Instalar cada uno de los dispositivos móviles tipo tableta requeridos para la prestación del servicio.
- Verificar la correcta operación de los kits biométricos con tableta, junto con la app de verificación fuera de línea biométrica electoral validando:
 - ✓ Que el votante pertenezca al puesto de votación y al censo de la mesa, según aplique.
 - ✓ Que el jurado se encuentre designado para el puesto de votación donde prestará el servicio.
 - ✓ Que los mecanismos de control dispuestos para la solución minimicen la suplantación del elector.
 - ✓ El correcto cargue y despliegue de la información biográfica del ciudadano.
 - ✓ Que el aplicativo muestre el puesto y mesa de votación habilitado para el ciudadano.
 - ✓ Que los kits biométricos se encuentren sincronizados con la hora legal colombiana fijada por el Instituto Nacional de Metrología (<http://horalegal.inm.gov.co/>).
- Registrar y guardar la trazabilidad (Logs de auditoria) del servicio prestado, en donde se evidencien por mesa de votación y estación de autenticación datos como: fecha y hora de la transacción, jurados de votación, personas autenticadas, departamento, municipio, zona, puesto y mesa de votación donde realizó la autenticación, resultado del cotejo (HIT, NO HIT) y las inconsistencias relacionadas con la autenticación de los ciudadanos.

2.4. Requerimientos Logísticos

Para la prestación del servicio, el futuro contratista deberá transportar, instalar oportunamente, suministrar y administrar todos los recursos logísticos, técnicos y físicos de acuerdo con las cantidades y matriz de distribución definida por la supervisión del contrato o quien esta designe.

Así mismo deberá disponer y proveer:

- **Pendón con infografía alusiva al proceso:** En material plástico de alta resistencia de 80x120cm, con el escudo y el logo de la RNEC. El diseño deberá estar acorde con la imagen corporativa de la Entidad, previa

aprobación de la supervisión del contrato y se instalará un pendón por cada puesto de votación.

- **Conectores, cableado eléctrico, tomas, multitomas y extensiones eléctricas** en cada uno de los puestos de votación de acuerdo con las necesidades para la prestación del servicio. Para ello el futuro contratista deberá como mínimo:
 - Garantizar que todo el cableado eléctrico utilizado se encuentre protegido con cintas de seguridad industrial autoadhesiva para tráfico pesado de color negro y amarillo o cualquier otro medio de protección que permitan evitar riesgos con el tránsito de los ciudadanos en los puestos y mesas de votación.
 - Prever y garantizar que todas las extensiones eléctricas que se utilicen sean las adecuadas para uso en exteriores e interiores según aplique. Razón por la cual, el futuro contratista deberá proveer la longitud (tamaño) adecuado para la puesta en marcha del servicio, utilizando cables que estén clasificados para manejar el voltaje de los dispositivos para los cuales serán utilizados.
 - Garantizar que el cableado y extensiones eléctricas a utilizar se encuentren en buen estado, sin uniones, enmendaduras y deterioros.
 - Organizar los cables y extensiones eléctricas, evitando que estos queden visibles y expuestos en las áreas de alto tráfico.
 - Prever que las extensiones eléctricas estén lejos del agua.
 - Evitar realizar conexiones en cadena, es decir, varias regletas de enchufes en una misma extensión.
 - Evitar conectar múltiples dispositivos con un solo cable.

2.5. Requerimientos técnicos, operativos y de control

Para el cumplimiento de este requerimiento, el futuro contratista deberá, adoptar antes y durante la ejecución de las actividades todas las medidas preventivas y correctivas destinadas a controlar adecuadamente los riesgos a que pueda estar expuesto el servicio a nivel funcional, operativo, técnico, tecnológico y de seguridad.

Así mismo deberá desarrollar, ejecutar e implementar como mínimo las actividades que se citan a continuación.

a. Actividades de instalación

- Para la elección de Presidente y Vicepresidente de la República, realizar una visita previa (pre-visitas) o de avanzada a los puestos de votación descritos conforme la matriz de distribución definida por la supervisión del contrato o quien esta designe, mediante la cual se deberá:

- Determinar las cantidades de materiales, insumos, acometidas eléctricas, localización de equipos y cantidad de personal de soporte técnico. Contar con materiales e insumos de contingencia para atender eventualidades.
- Precisar la ubicación de las estaciones biométricas, la antena satelital y la distribución de la infraestructura tecnológica a implementar en el puesto de votación, cuando aplique.
- Precisar la ubicación de las estaciones celulares y tabletas, así como la distribución a implementar en el puesto de votación.

Para la elección de Presidente y Vicepresidente de la República, estas pre-visitas se deberán realizar con los respectivos Registradores del Estado Civil, como responsables del proceso electoral en los puestos de votación, y con el acompañamiento de los funcionarios designados por la supervisión del contrato o quien esta designe, conforme al cronograma previamente acordado entre las partes y quienes fungirán como facilitadores del proceso para los asuntos específicos de la logística local y de la operación el día de las votaciones.

- Para la elección de Presidente y Vicepresidente de la República, entregar a la Entidad los resultados de las pre-visitas, mediante un informe que contenga los planos definitivos de distribución detallada de las estaciones biométricas de cada puesto de votación, incluyendo la información necesaria para la instalación de los kits biométricos en el puesto de votación. Este documento será firmado por el futuro contratista y el funcionario responsable de Biometría designado por la supervisión del contrato previo al despliegue de equipos, insumos y personal.

El documento suscrito resultante de las pre-visitas será la base del despliegue e instalación y sólo se modificará por asuntos de fuerza mayor decididos en conjunto entre la supervisión del contrato y el futuro contratista.

- Designar, por departamento y zona, un equipo técnico que se encargue de la ejecución, seguimiento y control del proceso de autenticación biométrica en los puestos de votación, así como el apoyo técnico, operativo y de soporte que se encuentre disponible desde el inicio hasta la entrega final de la prestación del servicio de autenticación biométrica, de acuerdo con el desarrollo de las actividades.
- Instalar, configurar y disponer de todos los recursos físicos, técnicos, tecnológicos, infraestructura, redes, humanos, logísticos, hardware, soporte, conectividad y comunicaciones que se requieran para la puesta en operación del servicio.

- Disponer de áreas locativas de almacenamiento para los dispositivos, los recursos físicos y demás elementos técnicos que hagan parte del servicio de autenticación biométrica contratado. Así mismo garantizar que éstas cuenten con las medidas y condiciones de seguridad física y ambiental y demás características que no representen riesgo para las personas que permanecen en estos sitios y afecte el cumplimiento de la obligación y los tiempos de entrega de los equipos. El futuro contratista deberá anexar la relación del (los) sitio(s), con sus direcciones, en donde estarán ubicadas estas áreas.
- Disponer de un lugar físico que cuente con las condiciones técnicas, físicas y ambientales necesarias (electricidad, temperatura, aire acondicionado, sillas, mesas, conectividad, servicios públicos y demás requerimientos de acuerdo con el lugar geográfico donde se encuentre ubicado), para la realización de pruebas técnicas, cuando aplique, así como presentaciones del proceso de autenticación biométrica, que garanticen la correcta ejecución de estas.
- Transportar, organizar, ubicar, instalar, custodiar, asegurar y desmontar cada uno de los equipos e insumos que se requieran para la prestación del servicio y el correcto funcionamiento y operatividad del proceso de autenticación biométrica en los puestos de votación designados a través de la matriz de distribución entregada por la supervisión del contrato.
- Transportar y recoger las estaciones de trabajo hacia y desde el puesto de votación a los sitios de almacenamiento definidos.
- Distribuir los kits MFACE, celulares, tabletas y los recursos físicos y técnicos necesarios para la prestación del servicio, hacia los municipios o sitios definidos por la Entidad, dentro del plazo establecido por la Entidad con el fin adelantar las labores técnicas, operativas y de seguridad respectivas para el alistamiento logístico pertinente, previa alistamiento técnico realizado por la RNEC.
- Disponer, organizar, ubicar y proveer las señalizaciones respectivas (pendones), en los sitios en donde se ubiquen las estaciones biométricas MFACE, tabletas y celulares incluyendo, donde aplique, la infografía, así como los habladores requeridos, de acuerdo con el diseño previamente aprobado por la supervisión del contrato o quien esta designe.
- Disponer del recurso humano (capacitado y con experiencia): técnicos, tecnológicos, de seguridad, administrativos y logísticos que sean

necesarios para garantizar el correcto funcionamiento, instalación y operatividad del servicio.

- Desinstalar y recoger los elementos instalados en los puestos de votación habilitados para la prestación del servicio de autenticación biométrica al finalizar la jornada electoral; para los puntos en los cuales por orden público o seguridad no sea posible realizarlos al finalizar la jornada electoral, se deben retirar a más tardar a las 10:00 a.m. del día siguiente.
- Resolver oportunamente a través del personal de soporte técnico dispuesto y del personal operativo en sitio, todos los incidentes, fallas, eventos y problemas que puedan presentarse durante la jornada electoral, garantizando la prestación continua del servicio. La atención por parte del personal operativo del futuro contratista se limita a temas de conectividad, conexión eléctrica y funcionamiento de los monitores. Los eventos relacionados con las máquinas MFACE y la aplicación de verificación de identidad, el software y la respuesta de los dispositivos, serán atendidos por el personal de soporte dispuesto por la RNEC desplegados en los sitios donde se instalen dichos dispositivos.
- Asumir y ser responsable de la administración logística, horarios y supervisión de las funciones del personal a su cargo el día de la jornada electoral.
- Capacitar, previo a la jornada electoral, al recurso humano que hará parte de la prestación del servicio de autenticación biométrica facial de electores y jurados de votación.
- Realizar, con acompañamiento de los funcionarios designados por la supervisión del contrato o quien esta designe, la verificación de los elementos de identificación para el personal dispuesto como apoyo en los puestos de votación, de acuerdo con la distribución entregada por parte de la Registraduría Nacional del Estado Civil. Esta actividad deberá efectuarse en el tiempo establecido por la Entidad previo la jornada electoral.
- Mantener informado al supervisor del contrato o quien esta designe, sobre el desarrollo de las actividades que se encuentran bajo su responsabilidad.
- Responder por la calidad y cumplimiento de las actividades designadas para la puesta en marcha del servicio, antes y durante las instalaciones de los kits MFACE, tabletas y celulares, incluyendo el día electoral.
- Adoptar, todas las medidas preventivas destinadas a controlar adecuadamente los riesgos a que puedan estar expuestos el personal

operativo y los electores durante la instalación de los kits MFACE, tabletas y celulares antes y durante el día electoral.

b. Esquema funcional y operativo de la solución

El futuro contratista deberá como mínimo:

- Conformar un equipo de trabajo, debidamente capacitado, que lidere la planeación y ejecución de las actividades del proceso de autenticación biométrica facial y garantice la organización y calidad del servicio prestado.
- Implementar políticas de operación mediante procedimientos u otros mecanismos que den cuenta de su aplicación en materia de control para la puesta en marcha del servicio de autenticación biométrica facial.
- Definir y desarrollar actividades de control que contribuyan a la mitigación de los riesgos físicos/lógicos para garantizar la correcta prestación del servicio.
- Acompañar y brindar soporte al personal que operará los kits MFACE, tabletas y celulares, durante la totalidad de la jornada electoral en los puestos de votación designados por la supervisión del contrato.
- Realizar la instalación y alistamiento logístico de los kits de autenticación biométrica facial en los puestos de votación, conforme la distribución definida y entregada por la supervisión del contrato o quien esta designe, de acuerdo con los requerimientos tecnológicos y logísticos mínimos establecidos para ello.
- Proveer los insumos y recursos lógicos, técnicos y logísticos que sean necesarios para capacitar de forma clara, concisa y práctica al personal que hará parte de la operación.
- Verificar, permanentemente, que la ejecución de las actividades, el cumplimiento de los requisitos, requerimientos y el uso y provisión de los recursos físicos, técnicos, tecnológicos y logísticos correspondan con lo programado, autorizado y solicitado por la supervisión del contrato.
- Implementar estrategias que permitan fortalecer aquellos aspectos del proceso que presenten debilidades.
- Identificar y subsanar las posibles causas de las fallas, incidentes y problemas que se puedan presentar antes y durante el proceso de autenticación biométrica facial, de manera oportuna y confiable, en lo relacionado con temas de conectividad e instalaciones eléctricas.
- Reportar al personal de soporte técnico dispuesto por la RNEC en cada uno de los puestos de votación, que apliquen, los incidentes y problemas que se puedan presentar antes y durante el proceso de autenticación biométrica facial, de manera oportuna y confiable, en lo relacionado con temas de funcionamiento de la aplicación y de los equipos MFACE, tabletas y celulares.

c. Etapas a desarrollar dentro del proceso

Para el desarrollo de las actividades inherentes al proceso de autenticación biométrica facial, el futuro contratista deberá cumplir como mínimo con las etapas que se citan a continuación:

i. Levantamiento de Información:

El futuro contratista será responsable de:

- Disponer del personal capacitado y con experiencia que permita cumplir con el desarrollo de esta actividad.
- Para la elección de Presidente y Vicepresidente de la República, visitar previamente los puestos de votación en los que se prestará el servicio de autenticación biométrica facial, en coordinación con los respectivos registradores del estado civil y los funcionarios designados por la supervisión del contrato.
- Para la elección de Presidente y Vicepresidente de la República, establecer la cantidad y tipo de insumos que sean necesarios para la adecuación de la logística del proceso de autenticación biométrica facial y el plano donde se identifique la distribución de las estaciones, la ubicación de la antena satelital y el flujo del votante. Como resultado de esta visita se deberá elaborar un documento que incluya los planos definitivos de distribución detallada de las estaciones biométricas de cada puesto de votación, incluyendo la información necesaria para la instalación de los kits biométricos en el puesto de votación. Este documento será firmado por el futuro contratista y el funcionario responsable de Biometría designado por la supervisión del contrato previo al despliegue de equipos, insumos y personal.

El documento suscrito resultante de las pre-visitas será la base del despliegue e instalación y sólo se modificará por asuntos de fuerza mayor decididos en conjunto entre la supervisión del contrato y el futuro contratista.

Para la elección de Presidente y Vicepresidente de la República, una vez finalizadas las pre-visitas, el futuro contratista deberá presentar a la supervisión del contrato un informe que consolide los resultados obtenidos de esta actividad.

ii. Desarrollo y ajustes.

La RNEC deberá suministrar al futuro contratista:

- Los equipos MFACE necesarios, que permitan brindar continuidad y eficiencia del servicio.
- Equipos configurados para cada puesto de votación con la información de los votantes y jurados asignados.

- Usuarios y contraseñas para ingresar a los equipos por parte de los operarios del futuro contratista, que les permita poner en funcionamiento las MFACE el día electoral.
- Licencias para instalación en los celulares y tabletas, suministradas por la RNEC.

iii. Implementación y puesta en marcha de la solución

El futuro contratista deberá como mínimo:

- Coordinar con el registrador del Estado Civil del respectivo municipio, la logística para la instalación de los kits MFACE, tabletas y celulares en los puestos de votación, conforme las previsitas realizadas para las elecciones de Presidente y Vicepresidente de la República.
- Cumplir con la implementación de todos los requerimientos mínimos de infraestructura, recurso humano y conectividad establecidos por la RNEC para llevar a cabo el proceso de autenticación biométrica facial y puesta en operación del servicio contratado.
- Identificar, definir, unificar y coordinar los diversos procesos, recursos logísticos y demás actividades que hagan parte del servicio, a fin de garantizar la prestación continua del mismo.
- Definir actividades, secuencias y estimación de los recursos, con el fin que se prevea con suficiente tiempo de antelación todo lo necesario para la puesta en operación del servicio.
- Planificar, analizar, monitorear y controlar las actividades inherentes a la prestación del servicio.
- Realizar las pruebas técnicas que sean necesarias, para garantizar que el servicio contratado se encuentra en óptimas condiciones de funcionalidad y operatividad para su puesta en operación.
- Disponer de los operarios requeridos para llevar a cabo el proceso de autenticación biométrica facial durante la jornada electoral, cumpliendo a cabalidad y en todo momento, con el esquema de disponibilidad del servicio.
- Garantizar la continua prestación del servicio de conectividad durante la jornada electoral.
- Reportar al personal técnico dispuesto por la RNEC, las novedades que se presenten y que impidan garantizar la continua prestación del servicio durante la jornada electoral, donde aplique.
- Garantizar que el día de la elección, los equipos para la autenticación biométrica facial estén dispuestos, disponibles, instalados, configurados, funcionando y en operación, en todos los puestos de votación definidos por la supervisión del contrato o quien esta designe, antes de las 7:00 a.m., con el fin de tener la capacidad de reacción ante posibles incidencias que se

presenten con los kits MFACE tabletas y/o los celulares, antes de iniciar la prestación del servicio.

- Disponer del personal de backup suficiente, para garantizar la prestación del servicio, durante la jornada electoral.

iv. Soporte

El futuro contratista deberá como mínimo:

- Brindar soporte logístico (conectividad – cuando aplique- e instalaciones eléctricas) a la RNEC respecto a la funcionalidad, rendimiento y operatividad de la solución MFACE, tabletas y celulares en las pruebas definidas y previamente notificadas por la Entidad así como la jornada electoral, cumpliendo en todo momento con el esquema de respuesta y atención a requerimientos y disponibilidad de la solución.
- Brindar asistencia técnica oportuna a los operarios que harán parte del servicio.
- Notificar de forma inmediata a la supervisión del contrato, al personal técnico dispuesto por la entidad, las fallas, incidencias, eventos y problemas que se presenten sobre la prestación del servicio de autenticación biométrica facial.

v. Operación de las estaciones biométricas MFACE, tabletas y celulares

El futuro contratista deberá como mínimo:

- Disponer de los operarios requeridos para llevar a cabo el proceso de autenticación biométrica facial durante la jornada electoral, cumpliendo a cabalidad, en todo momento, con el esquema de disponibilidad del servicio.
- Garantizar la continua prestación del servicio durante la jornada electoral.
- Notificar de forma inmediata al personal dispuesto por la entidad en cada puesto de votación, las fallas, incidencias, eventos y problemas que se presenten sobre la prestación del servicio de autenticación biométrica facial.
- Disponer del personal de contingencia necesario (backup), para garantizar la prestación del servicio, durante la jornada electoral.
- Implementar medidas y planes de contingencia, que garanticen la capacidad de reacción ante posibles incidencias o eventualidades que se presenten con el personal operativo o de backup.

d. Herramienta de registro de casos en mesa de ayuda

Disponer de una herramienta que realice la administración, monitoreo, seguimiento y control centralizado del proceso de autenticación biométrica facial, que permita como mínimo:

- Generar estadísticas de la información generada del proceso.
- Generar informes y reportes del proceso.

2.6. Generalidades del servicio de autenticación biométrica facial

El futuro contratista deberá como mínimo garantizar:

- El suministro e instalación de los insumos requeridos para la puesta en operación de los kits MFACE, tabletas y celulares, así como acondicionar los puestos de votación donde funcionará la solución de biometría facial, de acuerdo con las condiciones particulares de cada puesto, según el modelo de operación definido previamente por la Entidad.
- El embalaje, bodegaje, seguros, custodia, traslado y transporte de los equipos, elementos, materiales y demás insumos necesarios para el traslado y recogida de los equipos hacia los puestos de votación y a su lugar de origen.
- Que el día de la elección, los kits MFACE, tabletas y celulares estén dispuestos, disponibles, instalados, configurados, funcionando y en operación, en todas las mesas y puestos de votación antes de las 7:00 a.m., con el fin de tener la capacidad de reacción ante posibles incidencias que se presenten con los dispositivos e instalaciones antes de iniciar el proceso electoral y la autenticación biométrica facial de los jurados de votación.
- Que antes de las 7:00 a.m. el día de la elección, se suscriba un acta de instalación de las estaciones de autenticación biométrica facial en coordinación con el registrador del Estado Civil o con el delegado del puesto de votación, donde conste la instalación, adecuación y configuración de cada puesto de biometría facial, el cual deberá estar funcionando y operando de conformidad con los requerimientos de la Entidad.
- La suscripción de un acta, al finalizar la jornada electoral, que detalle las novedades, eventualidades e incidencias presentadas con la prestación del servicio durante la jornada electoral.
- La logística necesaria en los puestos de autenticación biométrica, así como las condiciones óptimas de funcionalidad y operatividad para realizar las actividades inherentes de este proceso contractual, previniendo las condiciones climáticas que se puedan presentar.
- La elaboración de los pendones 80x120cm con infografía alusiva al proceso, material plástico de alta resistencia, escudo y logo de la RNEC, identificando el servicio prestado. El futuro contratista deberá disponer de un pendón por cada puesto de autenticación biométrica facial. El diseño deberá estar acorde con la imagen corporativa de la Entidad, previa aprobación de la supervisión del contrato.
- La capacitación al recurso humano que interviene en este proceso, haciendo énfasis en la funcionalidad y operatividad del servicio contratado. Esta

capacitación deberá realizarse con antelación y acompañamiento de la RNEC.

- El recurso humano idóneo, capacitado y necesario, que garantice la prestación óptima y continua del servicio.
- Que la rotación del personal contratado no afecte el normal desarrollo, operación y funcionalidad del servicio contratado.
- La distribución de recursos, relación del personal dispuesto y descripción del esquema operativo para cada sitio y ciudad. Esta información deberá ser entregada a la supervisión del contrato en la fecha que de común acuerdo se establezca entre las partes.
- Los coordinadores técnicos que sean necesarios el día de la elección, para cubrir las labores mínimas que se citan a continuación:
 - Suministrar, coordinar y brindar el soporte permanente, en sitio, frente a cualquier problema de conectividad e instalaciones eléctricas que se pueda presentar con los dispositivos de autenticación biométrica facial en los puestos de votación.
 - Verificar que los medios de conectividad dispuestos para el proceso de autenticación biométrica facial se encuentren disponibles y funcionando en las mesas y puestos de votación según aplique.
- Los recursos logísticos y técnicos necesarios para la implementación del proceso de autenticación biométrica facial requerido por la Registraduría Nacional del Estado Civil, para cubrir la totalidad de los puestos donde se implemente esta tecnología.
- Prestar el servicio de autenticación biométrica facial en los puestos de votación, desde las 7:00 a.m. hasta culminar la jornada electoral.
- Proveer e incorporar todos los recursos técnicos, físicos y humanos que garanticen que el servicio de autenticación biométrica facial cumple con condiciones óptimas para la prestación del servicio.

2.7. Soporte técnico y mesa de ayuda del contratista

Para el desarrollo y ejecución de esta actividad se deberá disponer y estructurar el servicio de mesa de ayuda y soporte técnico funcional y operativo de la plataforma contratada como punto único de contacto para la atención, gestión y solución oportuna y eficiente de los requerimientos, reportes, consultas, interrupciones y tratamiento de todos los eventos, incidentes, fallas y problemas que se reporten referente a la funcionalidad y operatividad del servicio durante su implementación y puesta en marcha, contando con la disponibilidad del recurso humano capacitado y con experiencia que sea necesario para garantizar la prestación permanente de este servicio. La supervisión del contrato dispondrá de personal técnico especializado en las MFACE, tabletas y celulares en la mesa de ayuda dispuesta por el futuro contratista, para dar el soporte correspondiente.

3. CAPACITACIÓN

La supervisión del contrato o quien esta disponga deberá:

- Para el proceso de Presidente y Vicepresidente deberá capacitar a los colaboradores del contratista y al personal dispuesto por la Entidad (máximo 60), asegurando la transferencia del conocimiento en lo que se refiere a la funcionalidad y operatividad de los kits MFACE, tabletas y celulares, las herramientas y plataformas que lo componen, incluyendo las políticas y procedimientos relacionados con el uso apropiado de los recursos tecnológicos utilizados para la prestación del servicio. Esta capacitación deberá ser teórica y práctica, tipo taller, y deberá incluir el hardware respectivo, que permita verificar y evidenciar el funcionamiento y operatividad del servicio.

Así mismo, esta actividad se deberá efectuar con antelación a la puesta en marcha de la solución, previamente coordinado con la supervisión del contrato. La logística, organización (Lugar, Fecha y Hora) y la cantidad de máquinas MFACE, tabletas y celulares a utilizar para estas capacitaciones, deberán ser consensuadas entre las partes antes de su ejecución.

- Las capacitaciones deberán ser realizadas por personal con experiencia en el proceso, que conozca y transmita de forma clara los temas inherentes a la prestación del servicio de autenticación biométrica y se encuentre en la capacidad de resolver y aclarar las dudas e inquietudes de los participantes.

El futuro contratista deberá:

- Capacitar a todo el personal operativo, técnico, logístico que hará parte del proyecto en cada uno de los municipios en donde se prestará el servicio de autenticación biométrica facial. Esta capacitación deberá ser teórica y práctica, tipo taller, y deberá incluir temas como: procedimientos, funcionamiento, operatividad, diagnóstico e instalación de cada kit de autenticación biométrica facial, entre otros.
- Capacitar a los miembros de la fuerza pública y a los actores del proceso autorizados por la Entidad, en el/los sitio(s) que la supervisión del contrato designe, previo acuerdo con el registrador respectivo, a fin de unificar criterios y competencias de cada una de las partes.
- Poner a disposición de la RNEC una plataforma E-Learning, que permita realizar la capacitación a los funcionarios electorales y demás personal designado por la Entidad, sobre el proceso de autenticación biométrica facial.

- Brindar acompañamiento y soporte en el uso y administración de la plataforma E- Learning.

La RNEC será la responsable de convocar a los funcionarios y a los diferentes actores del proceso que asistirán a la capacitación.

Por lo anterior, el futuro contratista deberá incluir dentro de su esquema de capacitación, todos los recursos que sean necesarios, incluyendo videos, presentaciones, y todo el material didáctico que permita asimilar, de forma clara y amigable, todo lo que técnica y conceptualmente se debe conocer sobre la solución contratada, sin que con ello se incurra en costos adicionales para la RNEC.

4. RECURSO HUMANO

Para la prestación del servicio de autenticación biométrica, el futuro contratista deberá proveer el personal técnico y logístico requerido y relacionado a continuación, para la operación de los equipos de autenticación biométrica facial en los puestos de votación, conforme a la distribución definitiva entregada por la supervisión del contrato que garantice su correcta ejecución e implementación.

ROL	FUNCIONES MÍNIMAS A DESARROLLAR
Líder de Puesto de votación Uno (1) por puesto de votación.	- Coordinar el personal de soporte en sitio. - Validar el correcto funcionamiento de los kits MFACE, tabletas y celulares al inicio de la jornada, así como reportar a la mesa de ayuda las incidencias o eventos que se lleguen a presentar. - Reportar al personal dispuesto por la RNEC cualquier novedad que se presente en el funcionamiento del SW de las estaciones MFACE, tabletas y celulares. - Reportar inconsistencias en la operación del puesto y aumento de afluencia de ciudadanos. - Coordinar con el delegado de puesto de la registraduría del Estado Civil, cualquier decisión de carácter electoral que pueda afectar el derecho al voto de los ciudadanos, en el puesto de votación. - Coordinar con la policía y el delegado de puesto de la registraduría nacional del Estado Civil cuáles son las rutas de ingreso y salida del puesto de votación, de acuerdo con el plano previamente aprobado por la Entidad. - Firmar un acta de recibo y devolución de los kits MFACE, tabletas y celulares y demás elementos que hagan parte

	de los kits de autenticación biométrica facial instalados en el puesto de votación.
Operarios de biometría Uno (1) por cada dispositivo MFACE, tableta y celular dispuesto para la operación.	- Operar los dispositivos para la autenticación biométrica facial. - Al finalizar la jornada entregar la estación de validación biométrica facial al líder de puesto.
Logísticos de los puestos de votación. Los necesarios para la correcta operación y control del flujo de votantes en el puesto de votación	- Coordinar el ingreso de los jurados de votación y los electores para evitar aglomeraciones en el acceso del puesto y mesa de votación. - Direccionar a la ciudadanía hacia las máquinas MFACE, tabletas y/o celulares conforme aplique. - Implementar estrategias de descongestión en los puestos de votación que sean definidas en conjunto con la registraduría nacional del Estado Civil.
Grupo de Soporte e Instalaciones	Deberá estar compuesta como mínimo por un (1) líder técnico y dos (2) auxiliares para desarrollar las siguientes actividades: - Pre Electoral: efectuar las visitas de campo, por parte del líder técnico, para determinar los materiales que se necesitan para el montaje del puesto (antenas satelitales, cantidad de cable o extensiones, plantas eléctricas, switches, mesas, sillas y carpas entre otros). - Elaborar los planos del puesto de votación con el fin de efectuar el montaje de los filtros biométricos para aprobación de los registradores del Estado Civil y la supervisión del contrato. - Realizar el montaje de los kits de autenticación biométrica facial en los puestos de votación, de conformidad con los planos aprobados por la RNEC. - Día de la elección: Dar soporte en sitio a los puestos de votación que tengan problemas de conectividad y/o eléctricos que afecten la prestación del servicio. - Poner a disposición plantas eléctricas, para dar respuesta a posibles contingencias.

Por lo anterior, el futuro contratista será responsable de:

- La contratación y remuneración del personal requerido para el proyecto, el cual no tendrá vínculo de ninguna naturaleza con la RNEC y serán los encargados de apoyar y soportar el servicio de autenticación biométrica facial, objeto del presente contrato
- Identificar al personal con prendas que tengan el distintivo de Biometría y su correspondiente escarapela, la cual deberá ser alusiva al servicio que presta y tendrá logo de la Registraduría Nacional del Estado Civil. El diseño de los elementos distintivos para el proceso de Autenticación Biométrica facial será aprobado por la supervisión del contrato o quien esta designe.
- De los costos correspondientes a tiquetes de transporte aéreo y terrestre, hospedaje, alimentación, viáticos y manutención del personal desplegado que atenderá las actividades propias del contrato.
- Disponer del personal de contingencia o Backup necesario para suplir las necesidades que se llegasen a presentar, sin afectar la prestación del servicio.

5. OTRAS OBLIGACIONES DEL CONTRATISTA

El futuro contratista se comprometerá a realizar todas las actividades plasmadas en el presente documento, incluyendo el cumplimiento de los hitos que se citan a continuación:

- Poner a disposición de la supervisión del contrato la solución logística contratada con todos sus componentes y herramientas que lo integran, en condiciones óptimas de rendimiento, funcionalidad y operatividad.
- Instalar, administrar, monitorear y dar soporte a los dispositivos de conectividad y eléctricos utilizados para la puesta en operación del servicio.
- Disponer de un área locativa centralizada para el cumplimiento de cada una de las actividades del proceso de Biometría facial, garantizando la seguridad de la información y cumpliendo a cabalidad con las políticas de seguridad de la información de la RNEC (Resolución No 27161 del 22 de noviembre de 2023) y los acuerdos establecidos en el compromiso de confidencialidad firmada entre las partes contractuales.
- Disponer de los recursos humanos idóneos, suficientes y necesarios, para el desarrollo y puesta en producción del servicio contratado, el cual deberá estar disponible 100% durante la ejecución del contrato.
- Notificar de forma inmediata, a la supervisión del contrato, cuando se presenten situaciones que atenten contra la eficiencia y funcionamiento correcto del servicio contratado.
- Reportar de manera oportuna e inmediata los requerimientos, reportes de fallas, incidentes y problemas que se presenten con la prestación del servicio, a los técnicos de las MFACE, tabletas y celulares dispuestos por la RNEC.

- Atender de manera inmediata cualquier anomalía que se presente con la solución contratada, en lo relacionado con conectividad de internet y eléctrica.
- Impartir capacitación sobre el proceso y protocolo a emplear en el proceso de autenticación biométrica facial.
- Disponer de un grupo de trabajo multidisciplinario, para funciones relacionadas directamente con el servicio.
- Para la elección de Presidente y Vicepresidente de la República, hacer entrega a la supervisión del contrato del cronograma de actividades correspondiente a la puesta en marcha del servicio.
- Tomar y ejecutar las medidas conducentes para el debido y oportuno cumplimiento de las obligaciones contractuales.
- Acatar las instrucciones que durante el desarrollo del contrato se impartan por parte del supervisor del contrato o quien esta designe.
- Analizar el contexto interno y externo del proceso de autenticación biométrica facial para la identificación de los riesgos y sus posibles causas.
- Poner a disposición de la RNEC, un directorio actualizado del personal de soporte técnico y nivel gerencial que hará parte del proceso de autenticación biométrica facial a quien la supervisión del contrato o a quien esta designe, pueda acudir y reportar los casos a los haya lugar.
- Suscribir el compromiso de confidencialidad, no divulgación, y de transparencia de datos, propuesto por la Registraduría Nacional del Estado Civil.
- Definir y documentar la manera de cómo lograr los resultados de un servicio óptimo y seguro, teniendo en cuenta los insumos necesarios, planes de acción, estrategias, actividades, responsables, la forma en que se organizarán y operarán, el talento humano requerido y puntos de control que se requieran para la puesta en marcha del servicio.
- Cumplir cabalmente con el compromiso de confidencialidad de la información suscrito, en el sentido de abstenerse de utilizar la información entregada por la RNEC para cualquier fin distinto a la ejecución de este proceso, toda vez que la misma, es de alta complejidad e interés para la Organización Electoral, y se encuentra catalogada de seguridad nacional; por lo tanto, debe mantener la reserva que corresponda, so pena de las sanciones legales a que haya lugar.
- Garantizarla continuidad del servicio de Internet, en los puestos de votación donde se implementará la autenticación biométrica facial, salvo situaciones de fuerza mayor y/o caso fortuito debidamente documentadas.

6. ENTREGABLES

➤ Por parte de la Registraduría Nacional del Estado Civil

La RNEC, entregará al futuro contratista:

- Matriz de distribución definitiva para la instalación de estaciones de autenticación Biométrica facial, con la información de tipo de biometría (a puesto).
- Personal técnico en los sitios donde se instalen los kits MFACE, tabletas y celulares.
- Credenciales para el personal operativo del futuro contratista.
- Usuario para registrar en la plataforma de la RNEC el personal que operará las máquinas MFACE, celulares y tabletas en cada puesto de votación.
- Licencias de verificación de identidad (APK) para instalar en los celulares y tabletas en calidad de servicio.

➤ **Por parte del futuro contratista.**

- Servicio de biometría facial funcional y operativo.
- Planes de contingencia eléctrica y operativa de los puestos de biometría facial a instalar.
- Informe que contiene la información levantada de cada uno de los puestos y plano a mano alzada, para las elecciones de Presidente y Vicepresidente de la República.
- Reportes y estadísticas con su respectivo análisis de las incidencias que se presentaron con el servicio de biometría facial en la jornada electoral.
- Actas de instalación y desinstalación de los puestos de biometría facial.
- Manuales y material de capacitación.
- Herramienta y manual de uso de la plataforma E-learning.
- Matriz de distribución de recurso humanos, logísticos y dispositivos biométricos MFACE, tabletas y celulares.
- Informe con evidencia fotográfica de todas las actividades relacionadas con el proceso.

7. REQUERIMIENTOS DE INFRAESTRUCTURA

7.1. Alcance General del Servicio

El oferente deberá suministrar un servicio integral de Infraestructura como Servicio (IaaS), completamente administrado y bajo su responsabilidad, que garantice la operación estable, segura, escalable y continua de las cargas de trabajo requeridas por la entidad para el proceso de Biometría.

El servicio deberá incluir, entre otros:

- Provisión, operación y administración de los recursos de cómputo necesarios (máquinas virtuales y/o servidores dedicados, según corresponda).
- Administración integral de red, conectividad, seguridad, almacenamiento y demás componentes requeridos.
- Garantía total del desempeño, disponibilidad y continuidad del servicio.

7.2. Responsabilidades del Oferente

El oferente será responsable de:

7.2.1. Diseño y Dimensionamiento

- Definir y entregar la arquitectura IaaS óptima para satisfacer los requerimientos de la entidad.
- Dimensionar CPU, memoria, almacenamiento, red y demás recursos necesarios que satisfagan la necesidad de la entidad para cubrir el performance óptimo requerido por el proceso.

7.2.2. Prestación del Servicio

- Proveer la infraestructura necesaria asegurando:
 - Capacidad suficiente para el procesamiento.
 - Rendimiento adecuado para las cargas de trabajo.
 - Cumplimiento de las tasas de transferencia en comunicaciones y redes.
- Mantener la infraestructura disponible conforme a buenas prácticas de continuidad, seguridad y escalabilidad.

7.3. Cumplimiento de Políticas de Seguridad

- Garantizar que la infraestructura se encuentre protegida mediante mecanismos de seguridad administrados por el proveedor (red, firewalls, segmentación, controles de acceso, etc.).
- Integrar las soluciones en redes privadas virtuales o entornos equivalentes provistos por el oferente.

7.4. Escalabilidad y Flexibilidad

- Permitir la expansión de recursos (CPU, memoria, almacenamiento o red) sin interrupciones del servicio.
- Garantizar la capacidad de adaptar la infraestructura a necesidades sin requerir rediseños mayores.

7.5. Condiciones de Desempeño y Disponibilidad

El servicio deberá garantizar:

- Desempeño consistente y adecuado para soportar las cargas de trabajo asignadas.
- Capacidad mínima de red suficiente para tráfico interno y externo, asegurando baja latencia.
- Alta disponibilidad de la infraestructura, conforme a estándares reconocidos del sector.
- Continuidad operativa bajo esquemas de tolerancia a fallos definidos por el oferente.

7.6. Obligaciones de Entrega y Soporte

El proveedor deberá entregar:

- Infraestructura completamente funcional.
- Soporte especializado 24/7.
- Monitoreo proactivo (NOC) del estado y rendimiento de los recursos.
- Gestión integral de incidentes (SOC) , problemas y mantenimiento.

7.7. Consideraciones Generales

- El oferente podrá utilizar tecnologías, arquitecturas o componentes equivalentes o superiores, bajo su propia responsabilidad operativa.
 - La entidad no deberá realizar tareas técnicas de configuración, aprovisionamiento o mantenimiento; el proveedor se encargará de todo el ciclo operativo.
- El futuro contratista deberá implementar estrategias de alta disponibilidad (Activo/Activo) y escalabilidad teniendo en cuenta el hardware y software que sean necesarios para garantizar la funcionalidad, operatividad y mejora continua de los servicios contratados.
 - El futuro contratista proporcionará a modo de servicio todos los recursos físicos (instalaciones, mobiliario, comunicaciones, entre otros), la infraestructura técnica (hardware, software, licencias, entre otros), física y logística (procedimientos, manuales, instructivos, entre otros), así como recurso humano calificado que sean necesarios para el cumplimiento de las obligaciones del presente documento y los servicios requeridos de cada uno de los componentes del servicio a contratar.
 - Para la salida a producción de los servicios contratados se deberán realizar previamente las siguientes actividades:

- Pruebas de carga y estrés.
 - Pruebas de alta disponibilidad.
 - Pruebas de seguridad, ethical hacking.
 - Análisis de vulnerabilidades y sus respectivas remediaciones.
-
- Cumplir con los parámetros y lineamientos que expida la supervisión del contrato en relación con el procedimiento de borrado seguro de los equipos y dispositivos dispuestos para este proceso.
 - Ejecutar las ventanas de mantenimiento preventivas y/o correctivas que sean necesarias, con el fin de mantener estable y actualizado los sistemas de información y/o aplicaciones que hagan parte del servicio.
 - Generar y entregar a la supervisión del contrato o a quien esta designe, los reportes y estadísticas con su respectivo análisis de los eventos, fallas, incidentes y problemas de ciberseguridad, seguridad informática y de la información relevantes de todos los componentes descritos en el presente documento, presentados durante el periodo contractual.
 - Disponer de los elementos de contingencia que sean necesarios para solucionar daños de hardware oportunamente.
 - El futuro contratista deberá garantizar que las redes de comunicación y lógicas que manejan los diferentes procesos se encuentren separadas física y lógicamente de las redes que exponen servicios e información en internet y que son de libre consulta por los diferentes actores externos de los procesos electorales, usando en los casos requeridos únicamente conexiones de firewall a firewall tipo Site to Site para la segura comunicación entre las redes o conexiones de pivote restringidas.
 - El futuro contratista entregará una matriz de comunicación con todos los datos de contacto según los servicios y criticidad, tanto para infraestructura tecnológica como de seguridad perimetral.
 - Los servicios de Datacenter, nube privada o pública que disponga el futuro contratista debe contar con respaldo y soporte en Colombia cuando el servicio que se requiera exponer en internet a los ciudadanos. Esta plataforma deberá cumplir los criterios de protección de datos personales y manejo de la información acordes con la normatividad legal colombiana vigente.
 - El futuro contratista deberá definir los lineamientos y mecanismos necesarios para el control de acceso de los usuarios finales a las estaciones de trabajo, con el fin de prevenir fugas de la información y garantizar la

confidencialidad, integridad, no repudio y disponibilidad de los procesos contratados.

- El futuro contratista deberá seguir los lineamientos para el proceso de control de cambio para toda la infraestructura tecnológica de acuerdo con la política vigente de la entidad.
- El futuro contratista pondrá a disposición los requerimientos mínimos suficientes del borrado seguro a realizar en servidores, computadores portátiles y de escritorio, así como todos los componentes que manejen información relacionada con los procesos descritos en el presente documento.
- Para cada una de las plataformas tecnológicas que soportan los diferentes procesos, deberán contar con sus respectivos modelos de alta disponibilidad, manejo de riesgos y operación tecnológica y de seguridad perimetral que garanticen los servicios.
- Presentar a la supervisión del contrato un documento de carácter técnico, en donde se contemple la infraestructura y/o arquitectura de la solución contratada para cada una de las plataformas que hacen parte del servicio, indicando el modelo de alta disponibilidad; así mismo, deberá contener el esquema de comunicaciones y seguridad perimetral que empleará para que el sistema opere en condiciones óptimas.
- Definir estándares y lineamientos para la gestión de la infraestructura tecnológica que soporta los sistemas y los servicios informáticos y de información contratados, así como los servicios requeridos para su operación.
- Para los eventos e incidentes que afecten la integridad, disponibilidad, confidencialidad y no repudio de información procesada en las plataformas de los procesos, el futuro contratista deberá reportarlos de manera inmediata al SOC de Registraduría para el tratamiento y gestión correspondiente, según los lineamientos de seguridad de la información de la Registraduría Nacional del Estado Civil – RNEC.
- El futuro contratista debe contar con los procesos de gestión de capacidad que garanticen la ejecución de los servicios contratados a nivel de infraestructura tecnológica y seguridad perimetral.
- El futuro contratista contara con los procedimientos de actualización y mantenimiento a nivel de infraestructura tecnológica y seguridad perimetral que soportan los servicios contratados.

- El futuro contratista diseñará y desarrollará los respectivos procedimientos actualizados para el mantenimiento de los servicios que se encuentran en operación y recuperación en caso de presentarse fallas.
- El futuro contratista desarrollará e implementará las respectivas prácticas de seguridad de la información en las capas del modelo del servicio a nivel de infraestructura tecnológica y seguridad perimetral.
- El futuro contratista definirá los respectivos mecanismos de protección, como las credenciales de acceso a los aplicativos, capacidades de almacenamiento definidas, así como garantizar la respectiva protección a los aplicativos que manejan datos críticos y no críticos.
- El futuro contratista deberá entregar informes y cuadros de mando con el estado actualizado de la seguridad perimetral.
- El futuro contratista elaborará los respectivos informes de seguimiento con la información recopilada a nivel de: disponibilidad, fiabilidad, mantenibilidad y cumplimiento del SLA, cuando la supervisión del contrato lo requiera.
- Diagrama detallado de todos los componentes de la solución, incluyendo la arquitectura de seguridad perimetral provista para el proceso.
- Certificación del Data Center (Centro de Datos) que cumpla como mínimo con las características contenidos en la norma TIA-942 TIER III o superior o ICREA IV o superior.
- Documentación del proceso de hardening, para todos los elementos de la infraestructura de cómputo utilizados en el proceso.
- Documentación de los lineamientos de seguridad implementados sobre las estaciones de trabajo de los usuarios finales, a fin de garantizar la seguridad de la información de los procesos contratados.
- El futuro contratista dispondrá de los recursos técnicos, humanos y logísticos que le permitan definir las medidas preventivas y reactivas ante incidentes en la conectividad, infraestructura tecnológica, servicios alternos a la operación, así como responder de manera rápida, efectiva y coordinada a los incidentes, alertas, de los componentes de las plataformas contratadas, con el fin de eliminar y/o minimizar el impacto de éstos en los procesos a contratar, por lo tanto, se deberá entregar un plan de respuesta a incidentes, para que la RNEC lo pueda poner a prueba durante la prestación del servicio. Los esquemas de servicio contratados deben ser premium en modalidad 7x24x365.

- El servicio de NOC debe ser centralizado, que integre el monitoreo y el procesamiento de la información de los procesos contratados, considerando que se requiere infraestructura alterna para continuidad de procesos, el NOC debe contar con la contingencia que permita el monitoreo y gestión del centro de datos.
- El futuro contratista deberá realizar la activación de los logs de acceso de los dispositivos de la infraestructura tecnológica, seguridad perimetral y aplicaciones de software que componen la plataforma.

7.8. CUMPLIMIENTO NORMATIVO

- Cumplir con las políticas y procedimientos de la Registraduría Nacional del Estado Civil - RNEC para garantizar la seguridad informática en la operación de la solución, cumpliendo con los objetivos de control y controles (en los casos que aplique) de la Norma Técnica Colombiana NTC-ISO/IEC 27001:2013.
- Dar cumplimiento a la Resolución No. 3308 de 2024 de Políticas de Seguridad de la Información, emitida por la Registraduría Nacional del Estado Civil – RNEC y todos sus anexos.
- Disponer de los controles necesarios para dar cumplimiento a lo establecido en las Leyes 1581 de 2012 (Ley de protección de datos personales) y la Ley 1712 de 2014 (ley de transparencia y del Derecho de acceso a la información Pública Nacional) y sus decretos reglamentarios.
- El futuro contratista, deberá generar un inventario de activos de información, y análisis de riesgos en materia de hardware, software y servicios de la infraestructura tecnológica y de seguridad perimetral que deban ser incluidos en la gestión de riesgos de la entidad.
- Implementar las directrices y/o lineamientos que apliquen referentes a las TIC y Seguridad Digital dispuestos por el Gobierno Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia – MinTIC para las entidades públicas y los procesos que estas contraten, tales como:
- Directiva Presidencial 03 del 15 de marzo de 2021, donde se establecen Lineamientos para el Uso de Servicios en la Nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos.
- Resolución 00500 de marzo 10 de 2021 del Ministerio de las TIC, bajo el cual se indican los lineamientos generales para la implementación del

Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, junto con los lineamientos y estándares para la estrategia de seguridad digital.

- Anexo 1_Seg Digital MSPI_05.02.2021, Modelo de Seguridad y Privacidad de la Información – MSPI y se precisan los lineamientos para la implementación de la estrategia de seguridad digital.
- La plataforma dispondrá de los controles necesarios para dar cumplimiento a lo establecido en la Ley 1581 de 2012 Ley de Protección de Datos Personales y Ley 1217 de 2014 Ley de Transparencia y Acceso a la Información Pública y sus respectivos decretos reglamentarios.
- Procedimiento de gestión de riesgos, junto con la matriz de gestión de riesgos (identificación, valoración y mitigación) según la metodología seleccionada y evidencias de la remediación de estos.
- Inventario de activos de información, con su respectiva clasificación y categorización acorde a la metodología indicada por la supervisión del contrato y que corresponde al alcance de los procesos definidos y la gestión de la infraestructura tecnológica y seguridad informática.

7.9. EVALUACIONES TÉCNICAS

- El futuro contratista se obliga a implementar en el plazo establecido por la Supervisión, las medidas correctivas resultantes de las recomendaciones realizadas por la supervisión del contrato o las evaluaciones de seguridad realizadas por los terceros designados por los mismos, una vez éstas sean comunicadas. Como producto, el futuro contratista deberá presentar un informe detallado de las remediaciones realizadas en donde conste el cierre de estas, junto con las respectivas evidencias que soporten las acciones realizadas.
- El futuro contratista garantizará, que todos los registros del DNS que se requieran configurar en el dominio de la entidad, para los sitios web de los diferentes componentes sean aprobados por la supervisión del contrato.
- El futuro contratista con base en el análisis de riesgo realizado a la Infraestructura Tecnológica adoptará las medidas proactivas para la prevención del riesgo identificado, dejando como mínimo los riesgos residuales en bajos o mínimos para esta.

- El futuro contratista diseñará, desarrollará, implementará, socializará y realizará seguimiento a los planes de contingencia de la Infraestructura Tecnológica para los procesos electorales de la Registraduría Nacional del Estado Civil – RNEC.
- El futuro contratista garantizará dentro del servicio una disponibilidad de los canales de comunicación para el datacenter de un 99,98%.
- El futuro contratista garantizará los respectivos controles y mecanismos de acceso para los usuarios finales que hagan uso de los aplicativos de los procesos electorales contratados por la Registraduría Nacional del Estado Civil – RNEC.
- El futuro contratista garantizará que el servicio de nube privada, nube pública, nube híbrida e instalaciones propias de terceros, contará con una protección automatizada contra ataques distribuidos de denegación de servicio DDoS (Sistema contra la denegación de servicios) y contará con una protección a nivel de capa de aplicación con un Firewall de aplicaciones web WAF (Sistema de protección de aplicaciones tipo Firewall), proteger los sitios web contra una amplia gama de amenazas online, inyecciones SQL y filtros de scripts de sitios (XSS), CDN con parámetros de seguridad y traza debidamente activados y configurados.
- El futuro contratista garantizará que la plataforma cuente con la capacidad de detener ataques, aprovechando la visibilidad sobre el tráfico de web global para adoptar medidas frente a las amenazas más recientes en el mercado.
- El futuro contratista deberá realizar pruebas de penetración con enfoque de explotación real en seguridad ofensiva sobre todas las aplicaciones que componen los procesos electorales con herramientas del futuro contratista, de las cuales se deberán presentar los reportes entregados por cada una de las herramientas utilizadas a la supervisión del contrato o a quien este designe para dicho fin, junto con el informe detallado de la remediación de las vulnerabilidades encontradas y su respectiva evidencia. Estas deberán ser de caja negra (Black Box) y/o caja gris (Gray Box), acorde con lo definido con la supervisión del contrato.
- Informe de las pruebas técnicas de carga, stress y rendimiento, realizadas a los diferentes procesos contratados que se encuentren publicados en la web.

- Las pruebas de penetración o Ethical Hacking se deberán ejecutar sobre todas las aplicaciones de los procesos electorales contratados y que sean de exposición o publicación, y los sistemas, protocolos, comunicaciones, tanto propias, como de terceros delegados que participen a través del contrato en el proceso electoral, sin generar indisponibilidad alguna y a fin de evaluar los controles de seguridad informática y seguridad de la información, de lo cual deberá entregar el correspondiente análisis de vulnerabilidades, acorde a las vulnerabilidades identificadas.
- Los análisis de seguridad automatizados y manuales deben realizarse con estándares mínimos como OWASP (versión más reciente) para las aplicaciones WEB, y para el caso de las aplicaciones de escritorio se realizará el análisis bajo estándares de modelado ATT&CK, y resultados de vulnerabilidades sobre CVE, CVSS V3, siempre que se pueda. Estos análisis deben realizarse utilizando una herramienta que cumpla con los estándares internacionales de seguridad de la información en su última versión.
- Para los análisis de código estático y dinámico, el futuro contratista deberá realizar las actividades de remediación de las vulnerabilidades identificadas, ejecutando estos análisis tantas veces como sean necesarias para cada aplicación de los componentes contratados, con el fin de verificar que las vulnerabilidades identificadas se encuentren cerradas oportunamente y de manera efectiva, presentando los informes entregados por la herramienta, junto con el informe detallado de la remediación, en donde conste el cierre de las vulnerabilidades identificadas, así mismo como una comunicación continua a la RNEC del estado de seguridad y evolución de su remediación y la representación de la misma en los informes de riesgo y la valoración global de seguridad. De presentarse restricciones sobre la remediación, el futuro contratista presentara los controles compensatorios para mitigar la afectación.
- Para los análisis de vulnerabilidades, el futuro contratista deberá realizar las actividades de remediación de las vulnerabilidades identificadas, ejecutando estos análisis tantas veces como sean necesarios para cada servidor de la infraestructura de cada aplicación de los procesos electorales, con el fin de verificar que las vulnerabilidades identificadas se encuentren cerradas oportunamente y de manera efectiva, presentando los informes entregados por las herramientas, junto con el informe detallado de la remediación en donde conste el cierre de las vulnerabilidades identificadas. De presentarse restricciones sobre la remediación, el futuro contratista presentara los controles compensatorios para mitigar la afectación.
- Prestar el servicio de infraestructura tecnológica o Nube pública/privada en Colombia en un modelo de Datacenter con cobertura a nivel nacional y que

cuenta con una disponibilidad mínima de 99,98% y en donde se maneje para los actores del proceso información no crítica y ésta debe ir alineada a la Ley 1581 de 2012 (Ley de Protección de Datos Personales).

- El futuro contratista deberá realizar pruebas de carga y estrés para los aplicativos de los componentes contratados, conforme al requerimiento de peticiones mínimas que se deben superar y presentar a la Supervisión del Contrato el resultado de éstas. Estas pruebas se realizarán con la participación del equipo técnico designado por la Supervisión del Contrato.

Nota: Los umbrales de aceptación de las pruebas de carga y estrés serán definidas y concertadas entre las partes teniendo en cuenta las necesidades específicas del componente.

- Realizar los respectivos análisis continuos de vulnerabilidades, con comunicación continua a la RNEC de vulnerabilidades técnicas, con herramientas certificadas y licenciadas a todos los servidores que componen la infraestructura de las diferentes plataformas involucradas en el servicio contratado, de las cuales se deberán presentar los reportes entregados por la herramienta a la supervisión del contrato o a quien este designe para dicho fin, junto con el informe detallado de la remediación de las vulnerabilidades encontradas y su respectiva evidencia.

7.10. INFRAESTRUCTURA TECNOLÓGICA Y DE COMUNICACIONES

- Administración de sistema de prevención de intrusos (IPS) para protegerse de amenazas conocidas y no conocidas, permitiendo verificar, prevenir y alertar sobre comportamiento sospechoso sobre el flujo de tráfico entre diferentes zonas de seguridad.
- Deberá contar con mecanismos de cifrado, con algoritmos seguros para las comunicaciones internas y externas de los diferentes componentes de la infraestructura de los procesos contratados. Para el acceso seguro desde Internet a los diferentes aplicativos vinculados a los procesos electorales, a través del uso del protocolo HTTPS, mediante certificados SSL con mínimo TLS 1.2, proporcionando a la RNEC los certificados requeridos para la ejecución de este contrato.
- Disponer de un Data center (Centro de Datos) en alta disponibilidad (Activo/Activo) que cumpla como mínimo con las características contenidas en la norma TIA 942 TIER III o ICREA IV o superior, con la cual se debe garantizar la estabilidad en la operación, replicación y consolidación de la información para la solución planteada.

- Disponer de una nube privada o pública con respaldo y soporte en Colombia cuando el servicio se exponga en internet a los ciudadanos, que permitirá gestionar y personalizar los recursos y servicios de escalabilidad con crecimiento horizontal y verticalmente.
- El futuro contratista adquirirá, instalará, configurará y administrará un sistema de antivirus el cual debe permitir el control de vulnerabilidades sobre los sistemas operativos y con el cual cumpla con las mejores prácticas a nivel de despliegues de parches y actualizaciones y la respectiva validación sobre los componentes de la solución a fin de poder verificar la no persistencia de dificultades aún después de ser aplicados parches y actualizaciones mencionadas, por lo cual entregará los informes, con las debilidades identificadas y los planes de acción relacionados, así como la entrega de logs en raw al SOC.
- El futuro contratista contará con análisis comportamental de la infraestructura monitoreada de tal forma que se identifiquen desviaciones inmediatas respecto a cambios o comportamientos sospechosos sobre la infraestructura monitoreada.
- Disponer e implementar herramientas informáticas orientadas a detectar, diagnosticar, monitorear, e informar sobre posibles fallas, eventos, intermitencias, problemas e incidentes de seguridad de la solución contratada, con el objetivo de tomar las medidas preventivas y correctivas que permitan mantener el servicio funcional y operativo de forma permanente.
- El futuro contratista debe proporcionar una herramienta especializada en el registro de incidentes de infraestructura en donde se registren las acciones de investigación, remediación y/o respuesta, y se pueda conectar con la infraestructura de seguridad de la RNEC para obtener información en tiempo real, para lo cual deberá generar los siguientes servicios reactivos:
- Análisis, respuesta y tratamiento de eventos e incidentes de conectividad, infraestructura tecnológica, servicios alternos a la operación ofrecida por el proveedor para los procesos contratados.
- Análisis y coordinación de la respuesta ante las vulnerabilidades técnicas identificadas sobre los componentes de la solución que puedan representar un riesgo en la operación de los procesos contratados.
- El futuro contratista garantizará que todo el tráfico de información que se almacene, procese y transmita sobre la solución informática, transitará en forma segura, confiable y cumpliendo con la confidencialidad, integridad, no

repudio y disponibilidad de éstos, entre los componentes de la solución ofrecida para la Registraduría Nacional del Estado Civil - RNEC aplicando técnicas de cifrado y/o encriptación seguros, permitiendo la trazabilidad de los datos e información y a nivel del sistema operativo, mediante el uso de mecanismos como canales VPN, Sistema PKI (Public Key Infraestructura) y certificados SSL como mínimo TLS 1.2 o superior, suministrados por la RNEC.

- El futuro contratista deberá suministrar los medios y la infraestructura para realizar la conectividad y los servicios de telefonía que sean requeridos para la ejecución del contrato actual.
- El futuro contratista deberá suministrar un diagrama de alto nivel de todos los componentes de la solución, incluyendo la arquitectura de seguridad provista para el proceso, manteniéndolo actualizado y comunicándolo al personal responsable de seguridad de la RNEC.
- El futuro contratista deberá utilizar el dominio oficial de la Registraduría Nacional del Estado Civil, por tanto, deberá informar los registros de DNS y certificados digitales que requiera para los sitios web de los diferentes componentes requeridos. Los nombres de registros de DNS serán aprobados por la Supervisión del Contrato. La Registraduría Nacional del Estado Civil dispondrá del wild card para los certificados digitales.
- El futuro contratista dispondrá de una plataforma tecnológica, medios de comunicación y los equipos necesarios de infraestructura de red: lógica y física, para garantizar la disponibilidad y prestación continua del servicio al proceso contratado.
- El futuro contratista distribuirá las aplicaciones entre nodos, atendiendo al consumo de recursos que hace cada una de forma que finalmente haya un cierto equilibrio entre los nodos.
- El futuro contratista estará en la capacidad de integrar e interoperar todos los componentes de infraestructura y telecomunicaciones solicitados según el diseño de data center con servicios en alta disponibilidad para el manejo de continuidad de negocio con las especificaciones mínimas requeridas en el presente documento.
- El futuro contratista garantizará que el servicio de NOC debe generar visibilidad para el proceso contratado de los incidentes de infraestructura tecnológica, canales y medios de comunicación mediante el monitoreo 7x24 durante el tiempo de ejecución del contrato, respondiendo de forma oportuna a un posible ataque; este servicio debe estar conectado e intercambiando información con el SOC de la RNEC.

- El futuro contratista garantizará que el sistema deba permitir la detección del comportamiento de los usuarios y detectar cualquier comportamiento anormal que identifique situaciones en las que hay desviaciones de los patrones normales, por lo cual se deberá notificar todo cambio anómalo de forma inmediata al SOC de la RNEC, con un análisis de las causas y el plan de acción a aplicar.
- El futuro contratista instalará un sistema de detección/prevención de intrusos (IDPS) para la respectiva protección de amenazas comunes y amenazas avanzadas persistentes, la cual permitirá verificar, prevenir y alertar sobre cualquier comportamiento sospechoso a nivel del flujo de tráfico entre diferentes zonas de seguridad, enfocándose a la protección sobre los activos críticos con mayor riesgo del proceso y contando con más de 4.000 firmas predefinidas para la protección de diferentes tipos de tráfico contra amenazas enfocadas a las aplicaciones y al análisis inteligente de patrones y comportamientos.
- El futuro contratista no podrá almacenar las bases de datos con información biográfica de los colombianos en nube pública.
- El futuro contratista ofrecerá e instalará el servicio de Firewall de red de última generación bajo, el cual se realizará el respectivo control de flujo de tráfico entre las diferentes zonas de seguridad ya sea entrante o saliente, evitando que los intrusos puedan acceder a los datos e información confidencial, minimizando el riesgo de permisos o denegaciones, basado en direccionamiento IP fuente, dirección IP destino y protocolos, así mismo deberá permitir el envío de forma pasiva de los logs al SOC de la RNEC y establecer medidas a las recomendaciones suministradas.
- El futuro contratista ofrecerá el servicio de balanceo de cargas y/o de las aplicaciones WEB que se encuentren en alta disponibilidad y entre nodos para todas las aplicaciones publicadas que sean usadas en los respectivos procesos a contratar.
- El futuro contratista tendrá la capacidad de almacenar, administrar, transmitir y procesar datos de una manera organizada, íntegra y controlada que garanticen la integridad y disponibilidad de los datos del proceso contratado.
- El Data Center dispondrá de Protección de Seguridad de red UTM, protección de End Point, integración con los logs de la plataforma de seguridad en la Nube, así como la retroalimentación de otras fuentes de datos para la gestión de amenazas cibernéticas.

- El futuro contratista deberá contar con un sistema de antivirus centralizado y controlado por consola para la infraestructura tecnológica que soporta el servicio, con el fin de garantizar el monitoreo, actualizaciones automáticas, validación de las aplicaciones, bases de datos y los servicios de la infraestructura central, garantizando la continuidad de los servicios y sin problemas aún después de ser aplicados los parches.
- El futuro contratista una vez finalizadas todas las actividades en función del marco de este contrato, deberá realizar el borrado seguro de la información de la infraestructura tecnológica, la cual deberá ser verificada.
- El hardware deberá contar con las capacidades técnicas suficientes y necesarias para cumplir con los ANS que sean acordados con la RNEC, que permitan garantizar el cumplimiento de las obligaciones del contrato y el funcionamiento de cada proceso.
- El servicio de infraestructura deberá de ser operada y administrada en modalidad 7x24, con soporte y mantenimiento, manteniendo la contingencia y continuidad de la operación.
- Garantizar que toda la infraestructura usada para procesar los datos directos e indirectos de los procesos a contratar con las especificaciones mínimas exigidas por la RNEC, cumplan con todas las normas y reglamentación vigente en cuanto a seguridad, integridad, no repudio y confidencialidad de la información.
- La infraestructura puede estar en arquitectura en modalidad de balanceo de cargas y procesamiento entre los Data Centers definidos para el servicio, siempre y cuando se garanticen los tiempos de respuesta y continuidad de los procesos de acuerdo con los ANS requeridos por la RNEC.
- El futuro contratista diseñará e implementará un NOC (Network Operations Center), a través del cual prestará el servicio único y centralizado de monitoreo de eventos de la infraestructura crítica, canales y medios de comunicación, servicios de telefonía y dispositivos de red provisionados para todos los procesos de las elecciones, el cual deberá estar interconectado con el SOC de la RNEC.
- Para el caso de la información alojada en servidores y/o bases de datos de los aplicativos vinculados a los procesos electorales, el futuro contratista deberá contar con mecanismos de cifrado proporcionados a nivel del Sistema Operativo del dispositivo y/o mecanismos de cifrado a nivel del software de la solución.

- Para el servicio de NOC dispondrá de una infraestructura tecnológica en alta disponibilidad para un 99,98% que realice monitoreo tanto a la infraestructura del Datacenter como a la infraestructura de la nube, cumpliendo las calidades sistémicas de escalabilidad, seguridad, baja latencia, alta tasa de transferencia efectiva (throughput), que garanticen la recepción, procesamiento, consolidación y entrega de la información, enmarcada en el proceso contratado; disponer de los componentes a nivel de almacenamiento, redes y procesamiento a nivel de hardware para las actividades planteadas en el contrato.
- Proporcionar las herramientas, componentes, procesos y servicios tecnológicos para cumplir, integrar e interoperar con el modelo de seguridad de la información y seguridad informática definido para el proceso contratado, el proveedor podrá ofrecer los servicios de Infraestructura, telecomunicaciones y seguridad en las mismas ubicaciones que definan como data center, nube privada o nube pública que garanticen la disponibilidad, integridad y confidencialidad de la información y mantengan las restricciones de exposición de la información biométrica dentro del marco del territorio nacional.
- Todas las soluciones de software necesarias para el cumplimiento deben estar catalogadas con licencias o suscripciones debidamente instaladas o configuradas y soportadas para el fin contractual.
- El futuro contratista deberá entregar de forma pasiva los logs necesarios de la infraestructura de seguridad perimetral que sean requeridos por el supervisor del contrato de la RNEC, con el fin de utilizarlos en los diferentes procesos de seguridad y análisis forense.



JAIME HERNANDO SUÁREZ BAYONA
Registrador Delegado en lo Electoral



HOSLANDER ADLAI SÁENZ BARRERA
Gerente de Informática