MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
EJÉRCITO NACIONAL
DIRECCIÓN DE PERSONAL

INFORME DE SUPERVISIÓN Y RECIBO A SATISFACCIÓN PARCIAL __X__ TOTAL ___
No. ___03___

Bogotá (Cundinamarca ABRIL 2026)

1. CONTRATISTA	Nombre completo: ERICK ENRIQUE SÁNCHEZ DIAZ Identificación 1.023.886.053 Nacionalidad Colombiana Dirección Carrera 7 #31-21 Sur Bogotá Teléfono de contacto 3163551894 E-mail de contacto: erick.eagle@gmail.com
2. SUPERVISOR	Nombre completo: CT. DAVID RODRIGUEZ CABRERA Cargo: Oficial Administrador Informático Resolución de nombramiento: Resolución No.00000412 fechada 19 de ENERO de 2026. Teléfono de contacto 3128792902 E-mail de contacto: david.rodriguez@ejercito.mil.co
3. No. DEL CONTRATO – FECHA DE SUSCRIPCIÓN	No. del contrato 396-CENACPERSONAL-2026 Fecha de suscripción 29/01/2026
4. PÓLIZA DE GARANTÍA ÚNICA	No. De la Póliza No. **360 47 994000063638** Entidad que expide la póliza: Aseguradora Solidaria de Colombia Fecha del certificado de aprobación de la Póliza: 04-FEB-2026 Aprobado por: TC. LIBARDO CERQUERA PASTRANA
5. CRP	No.29726 de fecha 03 de febrero del 2026 Fecha expedición: 03 de febrero del 2026 Unidas/Sub-unidad ejecutora CENAC PERSONAL Dependencia: DIPER Posición catálogo de gasto: (A-02.02.02.008.003-13) 10CSF Fuente: NACIÓN Recurso 10 Valor: $56.700.000.00
6. FECHA INICIO EJECUCIÓN CONTRACTUAL	5/FEB/2026
7. PLAZO DE EJECUCIÓN	15/DIC/2026
8. OBJETO CONTRACTUAL	PRESTAR LOS SERVICIOS PROFESIONALES COMO INGENIERO DE SISTEMAS CON EXPERIENCIA EN DESARROLLO DE SOFTWARE BAJO LA PLATAFORMA DE ORACLE FORMS & REPORTS Y DESARROLLO EN PL/SQL ORACLE
9. OBLIGACIONES CONTRACTUALES	OBLIGACIONES ESPECIFICACIONES 1. Realizar levantamiento, análisis y socialización de los requerimientos y mejoras de los sistemas de información bajo la tecnología java. 2. Realizar verificación y ajuste en los datos, los formularios, los reportes de los sistemas de información bajo la tecnología java.

DIPER

	3. Realizar propuestas de solución de acuerdo a los requerimientos para ajustes de presentación de datos en los diferentes módulos reportes de los sistemas de información bajo la tecnología java. 4. Diseñar o desarrollar formularios y reportes para el manejo de la información de acuerdo a la verificación de los requerimientos. 5. Realizar todos los demás ajustes adicionales a los formularios, reportes, procesos y procedimientos requeridos por el supervisor del contrato cuando se presente la necesidad inmediata relacionada con el funcionamiento de los sistemas de información bajo la tecnología java. OBLIGACIONES CONTRACTUALES GENERALES: ✓ Observar durante el tiempo de ejecución del contrato, buena disposición y actitud favorable hacia el trabajo, respeto hacia sus compañeros y miembros del Ejército Nacional, al igual que la aplicación permanente de principios y valores propios de la institución militar. ✓ Dar estricto cumplimiento durante todas sus actuaciones, al marco normativo correspondiente a la integridad, trasparencia y lucha contra la corrupción. ✓ Guardar y mantener la debida reserva y confiabilidad frente a los temas y asuntos tratados y conocidos dentro del desarrollo y ejecución del presente contrato, reserva que se hará extensiva a los derechos de autor que de los mismos se derive. ✓ Aplicar medidas pasivas de seguridad con la documentación según clasificación con el fin de evitar la fuga de información de acuerdo con la normatividad vigente. ✓ De conformidad con el artículo 3 del Decreto 2609 de 2012, el contratista será responsable por la gestión documental de las actividades realizadas durante la ejecución del Contrato, presentando en el cronograma de actividades y en su informe de forma mensual el barrido de los documentos en físico y el término del almacenamiento del Orfeo hasta el archivo de los documentos. ✓ El contratista debe custodiar y a la terminación del presente contrato devolver los insumos, suministros, herramientas, dotación, implementación, inventarios y/o materiales que sean puestos a su disposición para la prestación del servicio objeto de este contrato. ✓ Entregar al final de la prestación del servicio, backup de la información producto ejecución del contrato. ✓ El contratista autoriza al MDN – EJÉRCITO NACIONAL a realizar los estudios de seguridad, comprobación de lealtad, realización de los exámenes de poligrafía y pruebas sicométricas antes y durante la contratación. ✓ Las demás obligaciones establecidas en el estudio previo, documento que el contratista declara conocer, y que hace parte del presente contrato. ✓ Las demás obligaciones que se deriven del objeto del contrato. PARÁGRAFO PRIMERO: Independencia del Contratista. El Contratista es independiente del Ministerio de Defensa – Ejército Nacional, y en consecuencia, el Contratista no es su representante, agente o mandatario. El Contratista no tiene la facultad de hacer declaraciones, representaciones o compromisos en nombre del Ministerio de Defensa – Ejército Nacional, ni de tomar decisiones o iniciar acciones que generen obligaciones a su cargo

DIPER

<table>
<tr><td>10. PERIODO DEL INFORME</td><td>ABRIL 2026</td></tr>
<tr><td>11. DOCUMENTOS QUE SOPORTAN EL CUMPLIMIENTO DE LAS OBLIGACIONES CONTRACTUALES</td><td>
<table>
<tr><th>No</th><th>No. Obligación</th><th>No. Radicado</th><th>Descripción</th></tr>
<tr><td>1</td><td>1,2,3,4,5</td><td>No Aplica</td><td>1. Realizar levantamiento, análisis y socialización de los requerimientos y mejoras de los sistemas de información bajo la tecnología java.

REALIZACIÓN DEL PROCESO DE CONCILIACIÓN E INTEGRACIÓN DE MÚLTIPLES RAMAS CON LA NUEVA VERSIÓN DE infoCandidatosPop

Se realizó un proceso de conciliación e integración de múltiples ramas que contenían ajustes relacionados con la nueva versión de infoCandidatosPop. Debido a la concurrencia de cambios sobre componentes y archivos comunes, fue necesario ejecutar una revisión detallada de las diferencias existentes entre ramas para consolidar una versión final estable, consistente y funcional.

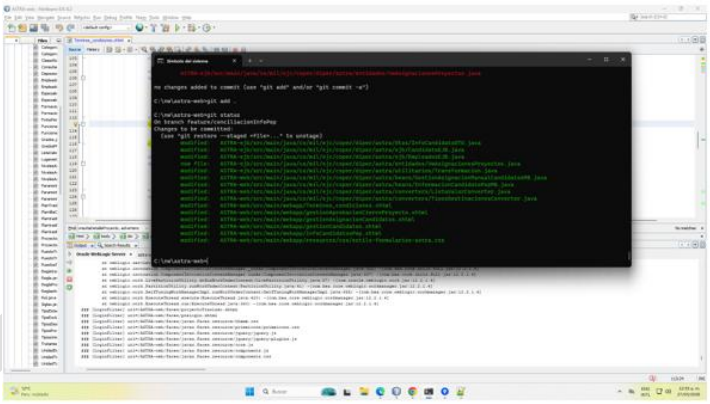
A nivel técnico, la actividad incluyó el análisis y comparación de múltiples archivos impactados por los desarrollos paralelos. La validación se efectuó línea a línea, con el objetivo de identificar cambios compatibles, resolver solapamientos, depurar diferencias funcionales y asegurar que la versión consolidada conservara correctamente los ajustes requeridos en infoCandidatosPop y en los componentes relacionados con su invocación, carga de datos y visualización.

Como apoyo al proceso de conciliación, se utilizó GitLab para revisar los cambios en modo comparativo side by side, lo que permitió inspeccionar de manera precisa las diferencias introducidas en cada rama, validar el origen de los ajustes y tomar decisiones de integración con mayor trazabilidad. Esta revisión visual facilitó la detección de bloques modificados, cambios sobre la misma sección de código y posibles inconsistencias derivadas de desarrollos simultáneos.

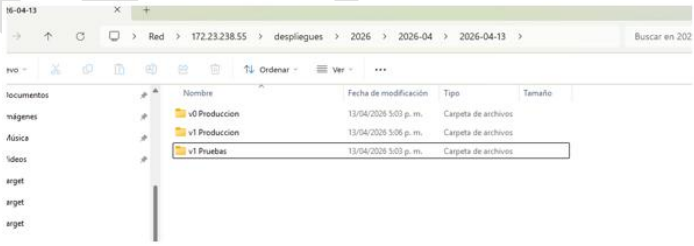
De forma complementaria, se utilizó Git en entorno local para construir una rama intermedia de integración. Esta rama se empleó como espacio controlado para unificar los cambios provenientes de las distintas ramas, resolver conflictos de merge, ajustar manualmente los archivos que presentaban incompatibilidades y validar el comportamiento del código antes de publicar una versión consolidada. Este enfoque permitió aislar el proceso de integración y reducir el riesgo de afectar directamente ramas de trabajo o ramas de mayor estabilidad.

Una vez completada la conciliación técnica, se realizaron pruebas funcionales sobre la versión resultante para confirmar el correcto comportamiento de las funcionalidades finales asociadas a infoCandidatosPop y a los flujos impactados por la integración.</td></tr>
</table>
</td></tr>
</table>

DIPER

					Después de validar que la versión consolidada respondía adecuadamente, la nueva rama fue subida al repositorio como resultado del proceso de merge e integración.  Imagen 1.
		2	1,2,3,4,5	No Aplica	2. Realizar verificación y ajuste en los datos, los formularios, los reportes de los sistemas de información bajo la tecnología java. **IMPLEMENTACIÓN DE UN CÓDIGO JAVA PARA LA DIFERENCIACIÓN DE CREDENCIALES, PUNTOS DE ACCESO Y URL DE RETORNO ASOCIADOS AL PROCESO DE AUTENTICACIÓN CON ZOHO** Se implementó en código Java para la diferenciación de credenciales, puntos de acceso y URL de retorno asociados al proceso de autenticación con Zoho, con el fin de soportar de manera controlada la operación en distintos ambientes. Esta adecuación permite que la aplicación disponga de una configuración diferenciada para producción y pruebas, manteniendo un comportamiento específico según el entorno en el que se ejecute el artefacto desplegado. A nivel técnico, el ajuste consistió en establecer por código la separación de los parámetros críticos del flujo de login OAuth con Zoho, incluyendo las credenciales de autenticación, los endpoints de entrada al proveedor y las rutas o direcciones de retorno utilizadas después del proceso de validación. Con ello, se evita que ambos ambientes compartan exactamente la misma configuración operativa y se garantiza que cada ejecutable invoque el flujo correspondiente a su contexto de despliegue. Como resultado de esta implementación, se pueden generar ejecutables diferenciados para ambiente de producción y ambiente de pruebas, cada uno con su propia configuración de acceso y retorno, sin alterar la base funcional del desarrollo. Esto permite

DIPER

					conservar una sola línea de mantenimiento del código, pero con comportamiento parametrizado según el ambiente objetivo. Adicionalmente, se mantuvo en el código fuente y en el repositorio la definición de las credenciales correspondientes a ambos ambientes, siguiendo el esquema actual de administración de configuración del proyecto. Bajo este enfoque, la lógica de selección permite identificar qué conjunto de parámetros debe utilizarse en cada compilación o despliegue, garantizando coherencia entre el ejecutable generado y el ambiente al que va dirigido. Desde la perspectiva funcional y operativa, esta separación reduce riesgos de configuración cruzada entre pruebas y producción, evita redirecciones incorrectas en el proceso de autenticación y mejora la trazabilidad del comportamiento del login en cada entorno. También facilita las labores de soporte y despliegue, ya que permite identificar de forma más clara qué configuración está asociada a cada versión entregada.  Imagen 2.
		3	1,2,3,4,5	No Aplica	3. Realizar propuestas de solución de acuerdo a los requerimientos para ajustes de presentación de datos en los diferentes módulos reportes de los sistemas de información bajo la tecnología java. **IMPLEMENTACIÓN DE UN EMERGENTE ACTIVABLE EN EL MÓDULO DE GESTIÓN DE PROYECTOS** Se implementó un emergente activable en el módulo de Gestión de Proyectos, disponible al seleccionar un proyecto. Este emergente permite ingresar manualmente el número de documento de un candidato y transferir dicho valor al componente infoCandidatosPop, encargado de mostrar la información detallada correspondiente. La mejora se diseñó para que la consulta no dependa de que el candidato se encuentre asociado al proyecto seleccionado. El proyecto actúa únicamente como contexto funcional dentro del módulo, mientras que la búsqueda y visualización de la información se realizan de forma directa por identificación.

DIPER

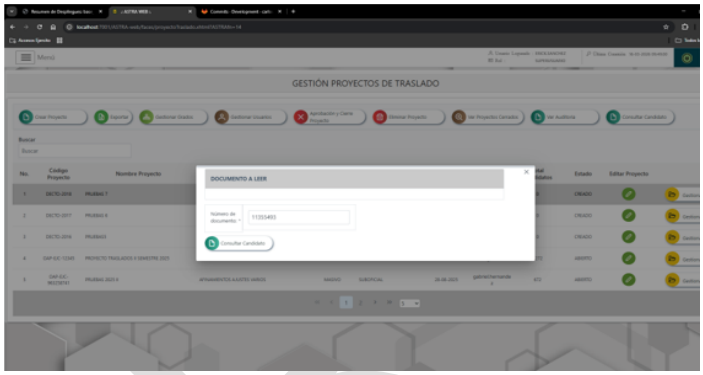


Imagen 3.

Técnicamente, la solución reutiliza el componente infoCandidatosPop, evitando duplicidad de lógica y manteniendo centralizada la presentación de datos del candidato. Esto mejora la mantenibilidad, amplía la flexibilidad del módulo y facilita consultas rápidas, validaciones y revisiones de información sin necesidad de incluir previamente al candidato dentro del proyecto.

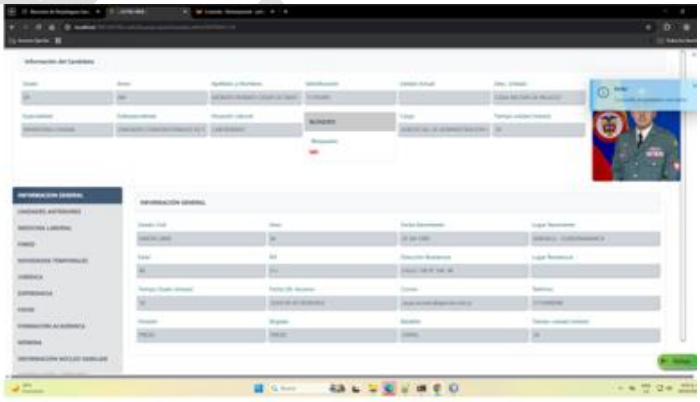


Imagen 4

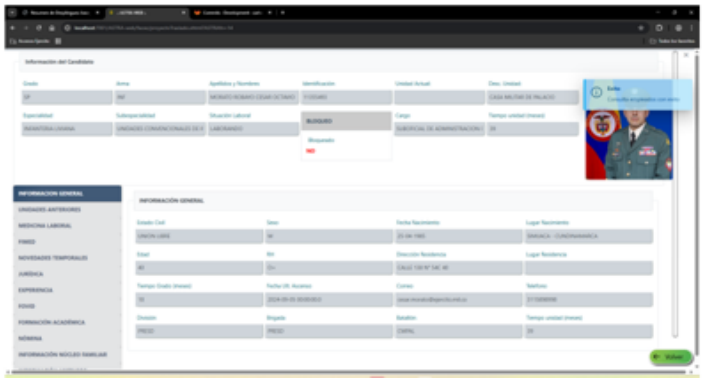
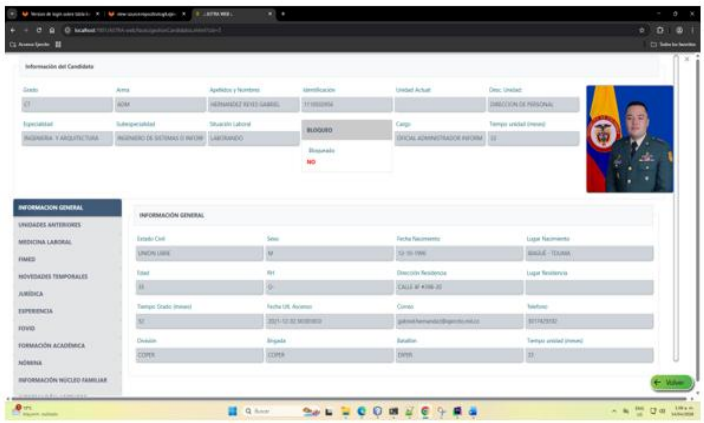


Imagen 5.

		4	1,2,3,4,5	No Aplica	4. Diseñar o desarrollar formularios y reportes para el manejo de la información de acuerdo a la verificación de los requerimientos. **REALIZACIÓN DE AJUSTES EN EL MANEJO DE CONSULTA Y DESCARGA DE FOTOS REMOTAS PARA RESOLVER EL PROBLEMA DE INCONSISTENCIAS EN LA EXTENSIÓN DE LOS ARCHIVOS ALMACENADOS EN EL SERVIDOR SFTP** Se realizaron ajustes en el manejo de consulta y descarga de fotos remotas para resolver el problema de inconsistencias en la extensión de los archivos almacenados en el servidor SFTP. El cambio principal consistió en agregar una lógica de resolución previa del nombre real del archivo, de manera que el sistema pueda ubicar correctamente la foto aun cuando la extensión haya sido registrada en mayúsculas o minúsculas, por ejemplo .jpg, .JPG o combinaciones equivalentes. Con esto se evita que la recuperación falle por diferencias de capitalización en la extensión, manteniendo intacto el nombre base del archivo, que en este caso es numérico y llega de forma exacta desde la aplicación. También se trabajó la validación de credenciales para el login local, fortaleciendo especialmente la contraseña. Se implementó una validación previa que controla campos vacíos y exige una estructura mínima de seguridad en la clave, incluyendo longitud mínima de 6 caracteres, presencia de al menos una letra mayúscula y al menos un carácter especial. Con esto se mejora la calidad de las contraseñas definidas por los usuarios y se reduce el riesgo de claves débiles o triviales dentro del acceso local de la aplicación. Desde el punto de vista técnico, esta validación se incorporó antes del procesamiento de autenticación para detener de forma temprana entradas inválidas y entregar mensajes claros al usuario. Esta decisión reduce carga innecesaria sobre la lógica de negocio y evita intentos de autenticación con datos incompletos o contraseñas que no cumplen el estándar mínimo definido. Además, centralizar estas reglas en un método dedicado facilita futuras ampliaciones, por ejemplo, agregar validación de números, restricciones de reutilización o controles de complejidad más exigentes. En cuanto al almacenamiento, las contraseñas locales son transformadas mediante MD5 antes de persistirse en base de datos, con el objetivo de no guardar el valor en texto plano y ofrecer una capa adicional de protección frente a exposición directa del dato. Esto permite que el sistema compare huellas de la contraseña en lugar de operar con la clave visible del usuario. Complementariamente, la política de complejidad implementada

DIPER

					en la validación aporta un nivel adicional de seguridad, ya que incrementa la entropía de la contraseña y dificulta ataques básicos por adivinación o uso de claves comunes. A nivel de arquitectura, ambas decisiones buscan fortalecer el sistema en dos frentes distintos pero relacionados con la robustez operativa: por un lado, la tolerancia controlada en la búsqueda de archivos remotos mejora la disponibilidad funcional del módulo de fotos frente a inconsistencias históricas del repositorio; por otro lado, la validación de contraseñas y su almacenamiento transformado mejoran el control de acceso local y reducen exposición de credenciales. En conjunto, estos ajustes apuntan a un comportamiento más confiable, predecible y seguro de la aplicación, minimizando fallos por diferencias de nomenclatura en archivos y elevando el estándar de seguridad en autenticación.  Imagen 6.
		5	1,2,3,4,5	No Aplica	5. Realizar todos los demás ajustes adicionales a los formularios, reportes, procesos y procedimientos requeridos por el supervisor del contrato cuando se presente la necesidad inmediata relacionada con el funcionamiento de los sistemas de información bajo la tecnología java. **IMPLEMENTACIÓN DE UN MECANISMO ALTERNO DE AUTENTICACIÓN, PARALELO AL LOGIN FEDERADO CON ZOHO MEDIANTE UNA INTERFAZ PROPIA DEL SISTEMA** Se implementó un mecanismo alterno de autenticación, paralelo al login federado con Zoho, mediante una interfaz propia del sistema que permite el acceso con credenciales internas administradas por la aplicación. Esta solución amplía la capacidad operativa del proceso de ingreso, al incorporar un segundo canal de autenticación controlado por la plataforma, independiente del proveedor externo, pero coexistente con el esquema principal de login corporativo.

					Desde el punto de vista funcional, el login alterno permite que la aplicación continúe operando en escenarios donde el acceso por Zoho no sea viable, por ejemplo, en ambientes de desarrollo, pruebas controladas, redes sin exposición pública suficiente para recibir correctamente el callback OAuth, validaciones internas o contingencias sobre el proveedor externo. Con ello, se reduce la dependencia exclusiva del servicio de autenticación federada y se mejora la continuidad operativa del sistema. A nivel de arquitectura, la solución puede interpretarse bajo un enfoque alineado con patrones de diseño orientados a desacoplar la autenticación. El uso de dos mecanismos de ingreso, Zoho e interno, encaja con una lógica tipo Strategy, donde el sistema puede resolver distintas estrategias de autenticación según el contexto, el ambiente o la ruta utilizada por el usuario. De forma complementaria, la centralización del proceso de validación, carga de usuario, control de acceso y registro de eventos puede describirse bajo un enfoque tipo Facade o Service Layer, ya que concentra en un único punto la coordinación del flujo de autenticación, independientemente del origen de las credenciales. Asimismo, la consulta de usuarios y contraseñas persistidas en base de datos corresponde naturalmente a un patrón DAO, al separar la lógica de acceso a datos de la lógica de negocio del login. La creación de esta interfaz paralela aporta ventajas técnicas relevantes. La principal es la disponibilidad de un mecanismo de contingencia plenamente controlado por la aplicación, útil cuando el flujo OAuth depende de factores externos como conectividad, certificados, URL públicas, callbacks válidos o configuraciones del proveedor. También facilita pruebas funcionales y soporte técnico, ya que permite validar acceso, perfiles y comportamiento de la aplicación sin depender en todo momento de integraciones externas. En ambientes restringidos o de desarrollo local, este enfoque evita bloqueos operativos y acelera actividades de diagnóstico, despliegue y validación. En materia de seguridad, la clave propia del sistema se almacena en base de datos en formato MD5, lo cual representa una mejora frente al almacenamiento de contraseñas en texto plano. Entre las ventajas operativas de MD5, especialmente en sistemas heredados, se encuentra su simplicidad de implementación, alta compatibilidad con plataformas Java antiguas, rapidez de cálculo y facilidad de integración con módulos ya existentes. Además, permite que la contraseña persistida no sea legible directamente en la base de datos, lo cual introduce una capa básica de protección frente a exposición directa del valor original. En la imagen, acceso con login de base de datos.

DIPER

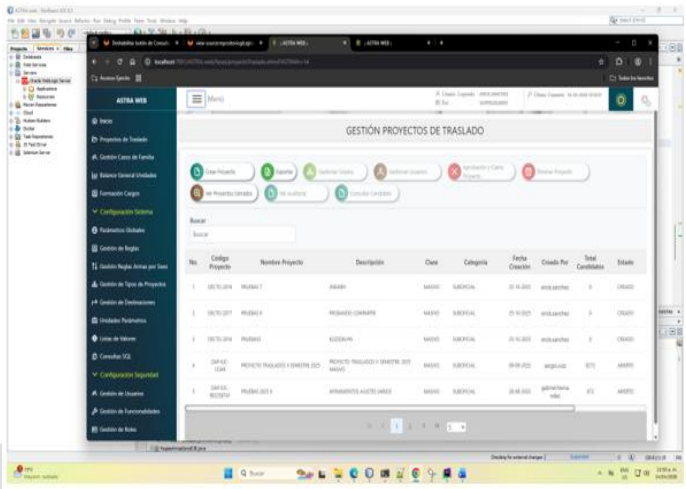
<table>
<tr><td></td><td colspan="4">

Imagen 7.</td></tr>
<tr><td>12. VALOR DEL CONTRATO</td><td colspan="4">Valor total: Valor: $56.700.000.00
Valor autorizado a pagar: $5.400.000.00</td></tr>
<tr><td>13. CUMPLIMIENTO PAGO SEGURIDAD SOCIAL</td><td colspan="4"><table>
<tr><th>Obligación</th><th>Entidad</th><th>Valor Pago</th></tr>
<tr><td>PENSIÓN</td><td>PORVENIR</td><td>$345.600</td></tr>
<tr><td>SALUD</td><td>SALUD TOTAL</td><td>$270.000</td></tr>
<tr><td>ARL</td><td>POSITIVA</td><td>$11.275</td></tr>
</table></td></tr>
<tr><td>14. DOCUMENTOS QUE HACEN PARTE DEL INFORME</td><td colspan="4">1. Cuenta de cobro

2. Informe de gestión sobre el cumplimiento del objeto contractual, firmado por el CONTRATISTA y el recibido a satisfacción del supervisor del contrato, de acuerdo al formato establecido.

3. Planilla de seguridad social: copia discriminada de los soportes de pago de los aportes mensuales obligatorios al sistema general de seguridad social en salud y pensión, sobre un ingreso base de cotización del 40% del valor mensual del contrato, con aporte del 16% en pensiones y el 12,5% en salud, ARL 0,522%

Nota: Lo anterior, conforme lo establece la normatividad legal vigente, la reglamentación de la materia y de acuerdo con la afiliación efectuada a la A.R.L.

4. Comprobante de pago de la planilla de seguridad social

5. Pantallazo SECOP II - Numeral 7 actualizada</td></tr>
<tr><td>15. CONSTANCIAS</td><td colspan="4">En el presente informe se deja constancia que el/la contratista cumplió con las obligaciones contractuales y legales reguladas para este tipo de contrato y como consecuencia se recibe a satisfacción de forma PARCIAL X TOTAL ____

Así mismo, se deja constancia que durante la ejecución del contrato no se han configurado los presupuestos legales que regulan el contrato laboral.</td></tr>
</table>

DIPER

16. RECOMENDACIONES	
17. CONCLUSIONES	

Para constancia se firma en, **(Bogotá),** en el mes de **ABRIL 2026**



FIRMA SUPERVISOR
Contrato No. 396-CENACPERSONAL-2026
Grado y Nombre completo: **CT. DAVID RODRIGUEZ CABRERA**
Cargo: Oficial Administrador Informático
Resolución de nombramiento: Resolución No.00000412 fechada 19 de ENERO de 2026.

DIPER