TIPO DE DOCUMENTO:	FORMATO	CODIGO: GC-FO-018
NOMBRE:	GESTIÓN CONTRACTUAL INFORME ACTIVIDADES CONTRATISTAS	VERSION: 08
RESPONSABILIDAD POR APLICACIÓN:	ÁREAS INTERNAS DE TODOS LOS PROCESOS	Página 1 de 6

INFORME ACTIVIDADES CONTRATISTAS

1. INFORME No. 03 de 2026

2. CONDICIONES DEL CONTRATO

Número de Contrato:	877 de 2026
Nombre del Contratista	SYSTEMS & SOLUTIONS LTDA
Periodo informe:	Julio/2026 a Noviembre /2026
Plazo del contrato:	Del 01/Junio/2026 hasta el 31/diciembre/2026
Nombre y Cargo del Supervisor:	Oscar Enrique Mendoza - Asesor Código 1020 Grado 06 del GIT de Servicios Tecnológicos
Dependencia perteneciente:	Grupo Interno de Trabajo Sistemas de Información Grupo Interno de Trabajo de Servicios Tecnológicos
Tipo de Contratista:	Persona Natural ___ Persona Jurídica _X__

3. OBJETO DEL CONTRATO

Prestación de servicios de ingeniería para la administración, soporte y mantenimiento de la plataforma tecnológica para la autenticación biométrica con la Registraduría Nacional del Estado Civil.

4. OBLIGACIONES DEL CONTRATO, ACTIVIDADES EJECUTADAS Y/O PRODUCTOS ENTREGADOS

Las obligaciones adquiridas son las siguientes:

OBLIGACIONES	ACTIVIDADES DESARROLLADAS	SOPORTE O EVIDENCIA DE CUMPLIMIENTO
Instalación, configuración		
Instalar y configurar sistema operativo, motores de bases de datos Oracle, Wildfly, Oracle Database Vault, Oracle Advance Security en servidores asignados por el Ministerio de Relaciones Exteriores.	Durante el periodo comprendido entre Julio y Noviembre se ejecutaron las actividades de instalación y configuración de las siguientes plataformas y componentes tecnológicos: • Motor de base de datos Oracle Database • Oracle Advanced Security. • Oracle RAC • Oracle Database Vault. • Oracle Database Firewall • WildFly. Los componentes anteriormente relacionados fueron configurados según los requisitos definidos en la Resolución, dentro de los cuales se realizaron las siguientes actividades:	• Informe_Instalacion_ Configuracion_ Oracle_ Cancilleria.pdf • Informe_Instalacion_ Configuracion_ Aplicaciones_ Cancilleria.pdf

	A. BASE DE DATOS ORACLE RAC 19c **1.** Se realizó la verificación de prerrequisitos técnicos para la instalación de Oracle Database 19c. **2.** Se validó el sistema operativo Oracle Linux Server 9.8, incluyendo versión, arquitectura y características del entorno. **3.** Se verificaron los recursos de hardware asignados a cada nodo, contemplando procesadores, memoria RAM y espacio de intercambio (SWAP). **4.** Se revisó la disponibilidad de almacenamiento, sistemas de archivos y puntos de montaje requeridos para la instalación. **5.** Se realizó la instalación y validación de Oracle Grid Infrastructure 19c Release 22 en los dos nodos. **6.** Se implementó y configuró la arquitectura de clúster Oracle Real Application Clusters (RAC) 19c, integrando ambos servidores. **7.** Se verificó el estado de los nodos y los servicios principales del clúster mediante las herramientas de administración de Oracle Clusterware. **8.** Se configuraron y validaron los recursos del clúster, incluyendo los componentes de almacenamiento compartido y servicios asociados. **9.** Se configuró y verificó Oracle Automatic Storage Management (ASM) en ambos nodos. **10.** Se realizó la configuración y validación de los servicios Oracle Listener, ASM Listener y SCAN Listener, necesarios para la conectividad de la base de datos. **11.** Se instaló y verificó el motor Oracle Database 19c Enterprise Edition en los dos servidores. **12.** Se configuró la base de datos bajo un esquema de alta disponibilidad mediante Oracle RAC. **13.** Se verificó la disponibilidad y el estado operativo de las dos instancias de base de datos, evidenciando su condición OPEN. **14.** Se realizaron validaciones finales sobre el estado de los recursos y servicios del clúster para comprobar su operación. **B. ORACLE AUDIT VAULT SERVER** **1.** Se realizó el alistamiento y verificación de prerrequisitos técnicos para la implementación de los dos servidores Oracle Audit Vault. **2.** Se verificó el sistema operativo Oracle Linux Server 8.10 de los appliances de auditoría. **3.** Se validaron los recursos de procesamiento, memoria RAM, SWAP, almacenamiento y puntos de montaje de	

	ambos nodos. **4.** Se realizó la instalación de Oracle Audit Vault Server versión 20.17.0.0.0 en los dos servidores. **5.** Se verificó la instalación de los appliances mediante consultas de versión y características del sistema. **6.** Se configuraron y validaron las interfaces de red y direcciones IP asignadas a cada servidor. **7.** Se realizaron ajustes y verificaciones de conectividad de red para la administración de la solución. **8.** Se habilitó y verificó el acceso a la consola web de administración de Oracle Audit Vault and Database Firewall. **9.** Se configuró el esquema de alta disponibilidad (HA) de Oracle Audit Vault Server. **10.** Se establecieron los roles de servidor primario y servidor secundario (standby) dentro del esquema de alta disponibilidad. **11.** Se verificó desde la consola de administración la habilitación del mecanismo de alta disponibilidad y la identificación del nodo standby. **C. ORACLE DATABASE FIREWALL** **1.** Se verificaron los prerrequisitos de instalación y las características del sistema operativo Oracle Linux 8.10. **2.** Se validaron los recursos de procesamiento, memoria RAM, SWAP, almacenamiento y puntos de montaje disponibles en ambos servidores. **3.** Se realizó la instalación de Oracle Database Firewall versión 20.17.0.0.0 en los dos nodos. **4.** Se verificó la versión instalada y las características de los appliances mediante consultas desde el sistema operativo. **5.** Se configuraron las interfaces de red y direcciones IP correspondientes a cada servidor Database Firewall. **6.** Se realizaron validaciones de los parámetros de red y conectividad requeridos para el funcionamiento de los componentes. **7.** Se verificó la disponibilidad de los dos servidores Database Firewall dentro de la infraestructura implementada. **8.** Se efectuaron las validaciones de instalación y configuración de los appliances como componentes de la solución Oracle AVDF. **D. INSTALACIÓN Y CONFIGURACIÓN DE SERVIDORES DE APLICACIONES WILDFLY** **1.** Se realizó el alistamiento técnico de los dos servidores	

	destinados a la capa de aplicaciones de la plataforma de autenticación biométrica. **2.** Se verificaron las direcciones IP y la identificación de los servidores correspondientes al Nodo de Aplicaciones 1 y Nodo de Aplicaciones 2. **3.** Se realizó la instalación y configuración del entorno de ejecución Java JDK 21, requerido para el funcionamiento de las aplicaciones. **4.** Se verificó la versión de Java instalada en ambos servidores mediante la ejecución del comando java -version. **5.** Se realizó la instalación del servidor de aplicaciones WildFly 30.0.0.Final en los dos nodos. **6.** Se configuró el servicio WildFly dentro del administrador de servicios systemd de los servidores Linux. **7.** Se realizó la configuración y parametrización de WildFly para su funcionamiento dentro de la infraestructura tecnológica. **8.** Se verificaron los archivos de configuración de WildFly, incluyendo los parámetros de interfaces y enlaces de red (socket bindings) definidos para su operación. **9.** Se verificó el estado operativo del servicio WildFly **10.** Se validó que los procesos asociados al servidor de aplicaciones se encontraran activos en ambos nodos. **11.** Se realizaron verificaciones finales sobre la instalación, configuración y funcionamiento de los servicios WildFly en los dos servidores. **E. INSTALACIÓN Y CONFIGURACIÓN DEL SERVICIO DE LICENCIAMIENTO MULTIPROTECT IMTS** **1.** Se realizó el alistamiento de los componentes requeridos para la implementación del servicio de licenciamiento Multiprotect IMTS On-Premises. **2.** Se verificó la disponibilidad de los dos servidores destinados al servicio de licenciamiento. **3.** Se realizó la instalación del componente Multiprotect IMTS On-Premises Installer, requerido para la gestión del licenciamiento de la plataforma. **4.** Se verificó la estructura de directorios y archivos asociados a los componentes Multiprotect instalados. **5.** Se realizó la instalación y validación del componente Multiprotect Console License Manager en los nodos de aplicaciones. **6.** Se verificó la versión del servicio Multiprotect License Manager, identificada como 6.3.2. **7.** Se validó la identificación del componente de licenciamiento BCL (Biometric Control License) mediante	

	las herramientas de consulta de Multiprotect. **8.** Se verificó la información de licenciamiento reportada por el componente Multiprotect, incluyendo identificación del servidor y datos de las licencias. **9.** Se revisó la disponibilidad de los directorios asociados a los componentes de licenciamiento en los servidores destinados para este servicio. **F. DESPLIEGUE Y VALIDACIÓN DE APLICACIONES** **1.** Se realizó el alistamiento de los directorios de despliegue de aplicaciones en los dos servidores WildFly. **2.** Se efectuó el despliegue del aplicativo proporcionado por la Registraduría Nacional del Estado Civil (RNEC), mediante el archivo Rep2WebService.war. **3.** Se verificó la disponibilidad del archivo de despliegue .WAR dentro del directorio deployments de WildFly en el Nodo de Aplicaciones 1. **4.** Se verificó la disponibilidad del archivo de despliegue .WAR dentro del directorio deployments de WildFly en el Nodo de Aplicaciones 2. **5.** Se validó la generación del archivo de confirmación Rep2WebService.war.deployed, como evidencia del despliegue realizado en ambos servidores. **6.** Se verificaron los archivos y permisos asociados al aplicativo desplegado en los dos nodos.	
Realizar acompañamiento técnico en el proceso de presentación y asignación de nueva infraestructura tecnológica al servicio de autenticación biométrica con la Registraduría Nacional del estado civil.	Se presto el acompañamiento técnico requerido y solicitado por la entidad en los procesos relacionados con la evaluación, presentación y asignación de nueva infraestructura tecnológica destinada al servicio de autenticación biométrica. revisión de compatibilidad técnica y verificación.	• N/A.

RUTA DE ACCESO A LA EVIDENCIA: Toda la información y evidencia de la ejecución de este contrato se encuentra cargada en la carpeta con la siguiente ruta: **https://minrelext.sharepoint.com/:f:/r/sites/679ba6c472/Documentos%20compartidos/General/Actividades%20de%20apoyo%20GITST/Contratos/2026/CTO_877-2026_SYS_LTDA?d=w587a9100a9d14ca7a9a3414770489be2&csf=1&web=1&e=RqASk7**

TIPO DE DOCUMENTO:	FORMATO	CODIGO: GC-FO-018
NOMBRE:	GESTIÓN CONTRACTUAL INFORME ACTIVIDADES CONTRATISTAS	VERSION: 08
RESPONSABILIDAD POR APLICACIÓN:	ÁREAS INTERNAS DE TODOS LOS PROCESOS	Página 6 de 6



GUSTAVO ADOLFO GARZON OCHOA
Representante Legal
SYSTEMS & SOLUTIONS LTDA

Observaciones: De **Julio a Noviembre** de 2026 el contratista SYSTEMS & SOLUTIONS cumplió a cabalidad con las obligaciones establecidas en el contrato 877 de 2026.

Aprobado por: OSCAR ENRIQUE MENDOZA LAGUNA - ASESOR CODIGO 1020 GRADO 06 DEL GIT DE SERVICIOS TECNOLOGICOS

NOTA: Certifico que se ha realizado la revisión de los soportes, anexos, y/o productos entregados por el contratista, los cuales evidencian y cumplen a entera satisfacción las obligaciones contractuales relacionadas.

OSCAR ENRIQUE MENDOZA LAGUNA
ASESOR CODIGO 1020 GRADO 06 DEL GIT DE SERVICIOS TECNOLOGICOS
Supervisor

Anexo:
*Copia Pagos al Sistema de Seguridad Social Integral
*Factura. (si aplica)
*Certificado de cumplimiento del Supervisor/ interventor

El Ministerio de Relaciones Exteriores y su Fondo Rotatorio, en cumplimiento de la Ley 1581 de 2012 ¨Por la cual se dictan disposiciones generales para la protección de datos personales¨, y sus decretos reglamentarios actuará bajo la calidad de Responsable del Tratamiento de sus Datos Personales. La información aquí registrada tiene como finalidad informarle sobre asuntos relacionados con la gestión de la Entidad en desarrollo de nuestras funciones y; para solicitarle que evalúe la calidad de nuestros servicios.

El Titular de los Datos Personales pueda ejercer los derechos que le asisten en el marco de la mencionada Ley a través del correo electrónico; contactenos@cancilleria.gov.co o a la dirección: Carrera 5 No 9 – 03 Edificio Marco Fidel Suárez, Bogotá, Colombia; dirigido a Protección de Datos Personales, Ministerio de Relaciones Exteriores.

Sus datos personales pueden ser transmitidos y/o transferidos a nivel nacional y/o internacional. Más información para conocer nuestra Política de Tratamiento de Datos Personales y los cambios sustanciales que se produzcan en ella en http://www.cancilleria.gov.co"