DEPARTAMENTO NACIONAL DE PLANEACIÓN	INFORME DE EJECUCIÓN Y SUPERVISIÓN CONTRACTUAL	FECHA 31/08/2026 dd/mm/aaaa

CONTENIDO DEL INFORME

1. CONDICIONES DEL CONTRATO.
2. OBJETO DEL CONTRATO.
3. ACTIVIDADES EJECUTADAS, OBLIGACIONES CUMPLIDAS, PRODUCTOS ENTREGADOS Y/O BIENES ENTREGADOS.
4. OBSERVACIONES A LAS ACTIVIDADES EJECUTADAS, A LAS OBLIGACIONES CUMPLIDAS, Y A LOS PRODUCTOS Y/O BIENES ENTREGADOS.
5. OBSERVACIONES ADICIONALES, SI A ELLO HUBIERE LUGAR.
6. PORCENTAJES DE AVANCE PRESUPUESTAL Y EN EJECUCIÓN DEL CONTRATO.

1. CONDICIONES DEL CONTRATO

Número de Contrato: DNP-1198-2026 SGR-280-2026 de la vigencia 2026
Nombre del Contratista: UT INFRAESTRUCTURA TECNOLÓGICA DNP
Periodo informe: 1/07/2026 al 31/07/2026

Nombres Supervisor
Nelson Fabio Pinzon Barrantes
Orlando Benavides Santacruz
CLAUDIA ANGELICA BEN-AMY PAEZ

Nombre Interventor: No aplica
Área a que Pertenece: OTSI

2. OBJETO DEL CONTRATO

110406526 110408526 Prestar los servicios al Departamento Nacional de Planeación (DNP) y a la Subdirección General del Sistema General de Regalías (SG SGR) de Centro de Servicios de Soporte Tecnológico y Centro de Operación de Seguridad y de red (SOC/NOC), los cuales comprenden soporte técnico, mantenimiento preventivo y correctivo, monitoreo continuo de la seguridad informática, así como la administración y operación de la infraestructura tecnológica.

3. ACTIVIDADES EJECUTADAS, OBLIGACIONES CUMPLIDAS, PRODUCTOS ENTREGADOS Y/O BIENES ENTREGADOS.

3.1. ACTIVIDADES EJECUTADAS:

Nom: Claudia Angelica Ben-Amy Paez
Céd: 51960483
ORG: Departamento Nacional de Planeación - Bogotá
Fecha: 2026-08-31 08:19
RSION 4
D N P
Firmado digitalmente Sisgestion

Nombre Actividad	Descripcion	Observacion
Cumplir con los ofrecimientos adicionales presentados en la oferta, y que hacen parte integral del presente contrato.	Se mantiene la evidencia el licenciamiento de ShareGate renovado hasta el 12 de mayo de 2027. El ADManager Plus aun esta licenciado hasta el 31 de agosto de 2026, se renovará sobre esa fecha de vencimiento. El licenciamiento de Blancco esta hasta el 25 de enero de 2027. La certificación de FIRTS se encuentra activa al corte del periodo y se presenta la evuidencia de 10.000 EPS de SIEM, teniendo 2.000 mas de las 8.000 solicitadas. Evidencia: - Certificacón FIRST 2026.pdf - Evidencia de EPS del SIEM.pdf - Evidencia Licencia ADManager Plus DNP hasta 31082026.pdf - Evidencia licenciamiento Blancco hasta 25022027.pdf - Evidencia licenciamiento ShareGate hasta 12052027.pdf Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 1	Verificado por el Supervisor
Cumplir con los ofrecimientos adicionales presentados en la oferta, y que hacen parte integral del presente contrato.	Se mantiene la evidencia el licenciamiento de ShareGate renovado hasta el 12 de mayo de 2027. El ADManager Plus aun esta licenciado hasta el 31 de agosto de 2026, se renovará sobre esa fecha de vencimiento. El licenciamiento de Blancco esta hasta el 25 de enero de 2027. La certificación de FIRTS se encuentra activa al corte del periodo y se presenta la evuidencia de 10.000 EPS de SIEM, teniendo 2.000 mas de las 8.000 solicitadas. Evidencia: - Certificacón FIRST 2026.pdf - Evidencia de EPS del SIEM.pdf - Evidencia Licencia ADManager Plus DNP hasta 31082026.pdf - Evidencia licenciamiento Blancco hasta 25022027.pdf - Evidencia licenciamiento ShareGate hasta 12052027.pdf Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 1	Verificado por el Supervisor
Entregar un cronograma de trabajo que incluya las actividades y entregables que den cumplimiento a las obligaciones del contrato, servicios acordados con la supervisión, socializar los avances mensualmente, si se requieren modificaciones al plan deben ser acordado con la supervisión.	A nivel general el cronograma de trabajo va en un avance del 43%. Esto debido a que las fases de inicio y planeación ya están al 100%. Evidencia: - Cronograma del proyecto - V 1.1.mpp Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 2	Verificado por el Supervisor

Entregar un cronograma de trabajo que incluya las actividades y entregables que den cumplimiento a las obligaciones del contrato, servicios acordados con la supervisión, socializar los avances mensualmente, si se requieren modificaciones al plan deben ser acordado con la supervisión.	A nivel general el cronograma de trabajo va en un avance del 43%. Esto debido a que las fases de inicio y planeación ya están al 100%. Evidencia: - Cronograma del proyecto - V 1.1.mpp Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 2	Verificado por el Supervisor
Mensualmente se debe entregar al supervisor, un informe de gestión en el cual se resuma la ejecución de actividades, cumplimiento de los servicios ejecutados y reportar las situaciones que afecten la operación de los servicios contratados, el contenido del informe debe ser acordado con la supervisión.	Se presenta el informe de Gestión de gestión del mes de julio de 2026 (Del 01 al 31 de Julio) Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 3	Verificado por el Supervisor
Mensualmente se debe entregar al supervisor, un informe de gestión en el cual se resuma la ejecución de actividades, cumplimiento de los servicios ejecutados y reportar las situaciones que afecten la operación de los servicios contratados, el contenido del informe debe ser acordado con la supervisión.	Se presenta el informe de Gestión de gestión del mes de julio de 2026 (Del 01 al 31 de Julio) Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 3	Verificado por el Supervisor

Disponer y mantener el talento humano mínimo requerido según lo especificado en el anexo técnico, cumpliendo con los roles y perfiles solicitados. Deberá cumplir con la entrega de los requisitos para presentar el talento humano solicitado. La distribución de turnos y cumplimiento de horario deben ser reportados a la supervisión mensualmente. Las novedades de personal deben ser informadas a la supervisión cumpliendo con los requisitos y tiempos definidos en el anexo técnico y en los ANS. El DNP podrá exigir al contratista el retiro del servicio de cualquiera de los miembros del personal que ejecuta el contrato, por motivos de seguridad del contratante, idoneidad profesional o incumplimiento de las actividades encomendadas, para lo cual el Contratista tendrá que reemplazar al integrante del equipo por un profesional que cumpla mínimo con el mismo perfil o superior al requerido sin costo adicional al DNP, el cambio debe realizar en el tiempo definido para la novedades de personal.	Se presenta la matriz de recurso humano con todos los roles solicitados. Las novedades se presentan en la misma matriz y en el informe de Gestión. Para el mes de julio de 2026 no se presentaron novedades de cambio de recursos. Las hojas de vida se presentaron, revisaron y aceptaron a la firma del acta de inicio y se mantienen actualizadas en el repositorio. Se ajustan las mallas de turno correspondientes al mes de julio, teniendo en cuenta el nuevo horario laboral establecido legalmente. Evidencia: - Equipo de trabajo - DNP 2026.xlsx - Carpeta: Hojas de vida - Carpeta: Malla de turnos Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 4	Verificado por el Supervisor

Disponer y mantener el talento humano mínimo requerido según lo especificado en el anexo técnico, cumpliendo con los roles y perfiles solicitados. Deberá cumplir con la entrega de los requisitos para presentar el talento humano solicitado. La distribución de turnos y cumplimiento de horario deben ser reportados a la supervisión mensualmente. Las novedades de personal deben ser informadas a la supervisión cumpliendo con los requisitos y tiempos definidos en el anexo técnico y en los ANS. El DNP podrá exigir al contratista el retiro del servicio de cualquiera de los miembros del personal que ejecuta el contrato, por motivos de seguridad del contratante, idoneidad profesional o incumplimiento de las actividades encomendadas, para lo cual el Contratista tendrá que reemplazar al integrante del equipo por un profesional que cumpla mínimo con el mismo perfil o superior al requerido sin costo adicional al DNP, el cambio debe realizar en el tiempo definido para la novedades de personal.	Se presenta la matriz de recurso humano con todos los roles solicitados. Las novedades se presentan en la misma matriz y en el informe de Gestión. Para el mes de julio de 2026 no se presentaron novedades de cambio de recursos. Las hojas de vida se presentaron, revisaron y aceptaron a la firma del acta de inicio y se mantienen actualizadas en el repositorio. Se ajustan las mallas de turno correspondientes al mes de julio, teniendo en cuenta el nuevo horario laboral establecido legalmente. Evidencia: - Equipo de trabajo - DNP 2026.xlsx - Carpeta: Hojas de vida - Carpeta: Malla de turnos Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 4	Verificado por el Supervisor

Implementar y operar en el DNP una Mesa de Ayuda con procesos alineados a ITIL, todos los casos se deben gestionar, registrar y cerrar en la herramienta ITSM (CA Service Management), cumplir con las especificaciones del servicio requerido dadas en el anexo técnico y atender las solicitudes realizadas por la supervisión.	Se presenta la matriz de recurso humano con todos los roles solicitados. Las novedades se presentan en la misma matriz y en el informe de Gestión. Para el mes de julio de 2026 no se presentaron novedades de cambio de recursos. Las hojas de vida se presentaron, revisaron y aceptaron a la firma del acta de inicio y se mantienen actualizadas en el repositorio. Se ajustan las mallas de turno correspondientes al mes de julio, teniendo en cuenta el nuevo horario laboral establecido legalmente. Evidencia: - Equipo de trabajo - DNP 2026.xlsx - Carpeta: Hojas de vida - Carpeta: Malla de turnos Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 4 Dentro de la estructura operativa del proyecto se tienen 6 recursos para atención en la mesa de ayuda y 10 recursos para soporte en sitio. Todos las solicitudes ingresan a la mesa de servicio como punto único de contacto por los diferentes medios de ingreso y se registran en la herramienta de gestión para ITSM (CA Service Management). En el mes de julio de 2026 se realizaron 5 reuniones semanales de seguimiento al registro de casos atendidos por la mesa de servicio. Se evidencias las actas de las reuniónes y la información presentada. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Gestión de Mesa de Servicios - Carpeta: Seguimiento semanal Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 5	Verificado por el Supervisor

Implementar y operar en el DNP una Mesa de Ayuda con procesos alineados a ITIL, todos los casos se deben gestionar, registrar y cerrar en la herramienta ITSM (CA Service Management), cumplir con las especificaciones del servicio requerido dadas en el anexo técnico y atender las solicitudes realizadas por la supervisión.	Se presenta la matriz de recurso humano con todos los roles solicitados. Las novedades se presentan en la misma matriz y en el informe de Gestión. Para el mes de julio de 2026 no se presentaron novedades de cambio de recursos. Las hojas de vida se presentaron, revisaron y aceptaron a la firma del acta de inicio y se mantienen actualizadas en el repositorio. Se ajustan las mallas de turno correspondientes al mes de julio, teniendo en cuenta el nuevo horario laboral establecido legalmente. Evidencia: - Equipo de trabajo - DNP 2026.xlsx - Carpeta: Hojas de vida - Carpeta: Malla de turnos Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 4 Dentro de la estructura operativa del proyecto se tienen 6 recursos para atención en la mesa de ayuda y 10 recursos para soporte en sitio. Todos las solicitudes ingresan a la mesa de servicio como punto único de contacto por los diferentes medios de ingreso y se registran en la herramienta de gestión para ITSM (CA Service Management). En el mes de julio de 2026 se realizaron 5 reuniones semanales de seguimiento al registro de casos atendidos por la mesa de servicio. Se evidencias las actas de las reuniónes y la información presentada. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Gestión de Mesa de Servicios - Carpeta: Seguimiento semanal Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 5	Verificado por el Supervisor

Dar soporte técnico de nivel 1 y 2 a la infraestructura tecnológica del DNP, gestionando cada caso en la herramienta ITSM (CA Service Management), gestionar los casos que requieran soporte de nivel 3, notificar a los líderes técnicos de la Oficina de Tecnología y Sistemas de Información (OTSI), los casos que sean escalados a nivel 3 y los casos que no puedan ser resueltos en los tiempos definidos.	Se realiza la atención de todos los casos que ingresan a la mesa de servicio. Se da atención, solución y escalamiento a nivel 2 y 3 de los casos que requieran. Toda la gestión se realiza mediante la herramienta de gestión para ITSM (CA Service Management). Seguimiento a los casos se realiza semanalmente en comité de seguimiento, donde se controlan todos los casos en registro, documentación, escalamiento, backlog, etc. Evidencia: - Carpeta: Seguimiento semanal Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 6	Verificado por el Supervisor
Dar soporte técnico de nivel 1 y 2 a la infraestructura tecnológica del DNP, gestionando cada caso en la herramienta ITSM (CA Service Management), gestionar los casos que requieran soporte de nivel 3, notificar a los líderes técnicos de la Oficina de Tecnología y Sistemas de Información (OTSI), los casos que sean escalados a nivel 3 y los casos que no puedan ser resueltos en los tiempos definidos.	Se realiza la atención de todos los casos que ingresan a la mesa de servicio. Se da atención, solución y escalamiento a nivel 2 y 3 de los casos que requieran. Toda la gestión se realiza mediante la herramienta de gestión para ITSM (CA Service Management). Seguimiento a los casos se realiza semanalmente en comité de seguimiento, donde se controlan todos los casos en registro, documentación, escalamiento, backlog, etc. Evidencia: - Carpeta: Seguimiento semanal Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 6	Verificado por el Supervisor
Gestionar, monitorear y mantener la operación de la infraestructura tecnológica del DNP, cumpliendo con los requisitos de los servicios solicitados en el anexo técnico, entregar reportes del estado de la infraestructura tecnológica, realizar análisis de causa de los incidentes e indisponibilidades de servicios que se presenten, cumplir con las tareas que le sean asignadas en la ejecución de controles de cambios, y atender las solicitudes realizadas por los especialistas técnicos de la Oficina de Tecnología y Sistemas de Información (OTSI).	Durante el mes de julio de 2026 se operó la infraestructura tecnológica del DNP por parte de la UT Infraestructura Tecnológica DNP. El registro de la atención de los incidentes, solicitudes, cambios y demás se registran en la herramienta de gestión para ITSM y se presentan y analizan en el informe de gestión del mes. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Gestión de Mesa de Servicios Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Informe de Gestión \Obligaciones específicas\Actividad 7	Verificado por el Supervisor

Gestionar, monitorear y mantener la operación de la infraestructura tecnológica del DNP, cumpliendo con los requisitos de los servicios solicitados en el anexo técnico, entregar reportes del estado de la infraestructura tecnológica, realizar análisis de causa de los incidentes e indisponibilidades de servicios que se presenten, cumplir con las tareas que le sean asignadas en la ejecución de controles de cambios, y atender las solicitudes realizadas por los especialistas técnicos de la Oficina de Tecnología y Sistemas de Información (OTSI).	Durante el mes de julio de 2026 se operó la infraestructura tecnológica del DNP por parte de la UT Infraestructura Tecnológica DNP. El registro de la atención de los incidentes, solicitudes, cambios y demás se registran en la herramienta de gestión para ITSM y se presentan y analizan en el informe de gestión del mes. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Gestión de Mesa de Servicios Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Informe de Gestión \Obligaciones específicas\Actividad 7	Verificado por el Supervisor
Implementar y operar un servicio de NOC, cumpliendo con las especificaciones del servicio requerido dadas en el anexo técnico, entregar los reportes y el informe del monitoreo, administración, gestión de fallos, alertas y tickets, así como cualquier otra información que sea requerida por la supervisión.	Al cierre del mes de julio de 2026, la plataforma Zabbix se mantiene operativa y estable, garantizando la continuidad del monitoreo sobre la infraestructura tecnológica de la entidad. Durante el periodo, la gestión se enfocó en fortalecer los mecanismos de notificación y escalamiento mediante la actualización de los responsables de cada área y la habilitación de grupos de Telegram segmentados por tipo de activo. Estos grupos son de uso interno y acceso exclusivo para el equipo SOC, y complementan las alertas enviadas por correo electrónico, facilitando el seguimiento y la atención oportuna de los eventos detectados. Asimismo, se amplió la cobertura mediante la incorporación de nuevos servidores Linux y se realizaron actividades de depuración sobre elementos de prueba y configuraciones temporales que ya no hacían parte del alcance vigente. Estas acciones permiten mantener una plataforma más organizada, reducir alertas innecesarias y mejorar la calidad y oportunidad de la información entregada al equipo de operación. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Zabbix Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 8	Verificado por el Supervisor

Implementar y operar un servicio de NOC, cumpliendo con las especificaciones del servicio requerido dadas en el anexo técnico, entregar los reportes y el informe del monitoreo, administración, gestión de fallos, alertas y tickets, así como cualquier otra información que sea requerida por la supervisión.	Al cierre del mes de julio de 2026, la plataforma Zabbix se mantiene operativa y estable, garantizando la continuidad del monitoreo sobre la infraestructura tecnológica de la entidad. Durante el periodo, la gestión se enfocó en fortalecer los mecanismos de notificación y escalamiento mediante la actualización de los responsables de cada área y la habilitación de grupos de Telegram segmentados por tipo de activo. Estos grupos son de uso interno y acceso exclusivo para el equipo SOC, y complementan las alertas enviadas por correo electrónico, facilitando el seguimiento y la atención oportuna de los eventos detectados. Asimismo, se amplió la cobertura mediante la incorporación de nuevos servidores Linux y se realizaron actividades de depuración sobre elementos de prueba y configuraciones temporales que ya no hacían parte del alcance vigente. Estas acciones permiten mantener una plataforma más organizada, reducir alertas innecesarias y mejorar la calidad y oportunidad de la información entregada al equipo de operación. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Zabbix Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 8	Verificado por el Supervisor
Implementar y operar un servicio de SOC, cumpliendo con las especificaciones del servicio requerido definidas en el anexo técnico, gestionar las alertas, realizar la recolección de evidencia y análisis de los incidentes informáticos relacionados con la infraestructura tecnológica que se presenten, y entregar los reportes del monitoreo, así como cualquier otra información que sea requerida por la supervisión.	La implementación de las herramientas del servicio SOC se realizó en el primer mes de operación. Para este mes realiza operación normal y los ajustes que la operación requiera. La evidencia de cada una de ellas se encuentra en el informe de gestión mensual. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Centro de operaciones de seguridad (SOC) y centro de operaciones de red (NOC) Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 9	Verificado por el Supervisor

Implementar y operar un servicio de SOC, cumpliendo con las especificaciones del servicio requerido definidas en el anexo técnico, gestionar las alertas, realizar la recolección de evidencia y análisis de los incidentes informáticos relacionados con la infraestructura tecnológica que se presenten, y entregar los reportes del monitoreo, así como cualquier otra información que sea requerida por la supervisión.	La implementación de las herramientas del servicio SOC se realizó en el primer mes de operación. Para este mes realiza operación normal y los ajustes que la operación requiera. La evidencia de cada una de ellas se encuentra en el informe de gestión mensual. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Centro de operaciones de seguridad (SOC) y centro de operaciones de red (NOC) Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 9	Verificado por el Supervisor
Implementación y operación del SIEM cumpliendo con lo requerido en el anexo técnico, realizar la configuración y puesta en funcionamiento del SIEM, La arquitectura de seguridad asociada al servicio se debe alinear con la plataforma tecnológica de la Entidad. Entregar los reportes que sean acordados con la supervisión, y se debe presentar la licencia del SIEM.	Actualmente, la plataforma FortiSiem opera de manera continua, garantizando la recolección, normalización, correlación y análisis de eventos de seguridad provenientes de las diferentes fuentes tecnológicas integradas. Durante el periodo se registraron 660.636 eventos, de los cuales el 70,35% correspondió a Seguridad y el 27,14% a Disponibilidad. Estas dos categorías concentraron el 97,49% del total, evidenciando que la operación estuvo orientada principalmente a la identificación de eventos de ciberseguridad y al seguimiento de la disponibilidad de la infraestructura. Frente al periodo anterior, en el que se registraron 327.607 eventos, se presentó un incremento del 101,65%, impulsado principalmente por el aumento de los eventos de Seguridad y Disponibilidad. Este comportamiento requiere mantener el seguimiento sobre las fuentes integradas, las reglas de correlación y los umbrales configurados, con el fin de determinar si la variación corresponde a condiciones operativas, cambios en la ingesta o situaciones que requieran acciones de afinamiento Como parte del proceso de mejora continua, se avanzó en el afinamiento de reglas de correlación, actualización de indicadores de compromiso (IOC) y optimización de casos de uso. Adicionalmente, se realizaron mesas de trabajo con los especialistas de las diferentes áreas para analizar el comportamiento de los dispositivos y las tendencias de los eventos, con el fin de reducir falsas alarmas, optimizar la generación de alertas y fortalecer la eficiencia operativa del Centro de Operaciones de Seguridad (SOC). Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: FortiSiem - Evidencia licenciamiento FortiSiem.pdf - Carpeta: Reportes FortiSiem Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 10	Verificado por el Supervisor

Implementación y operación del SIEM cumpliendo con lo requerido en el anexo técnico, realizar la configuración y puesta en funcionamiento del SIEM, La arquitectura de seguridad asociada al servicio se debe alinear con la plataforma tecnológica de la Entidad. Entregar los reportes que sean acordados con la supervisión, y se debe presentar la licencia del SIEM.	Actualmente, la plataforma FortiSiem opera de manera continua, garantizando la recolección, normalización, correlación y análisis de eventos de seguridad provenientes de las diferentes fuentes tecnológicas integradas. Durante el periodo se registraron 660.636 eventos, de los cuales el 70,35% correspondió a Seguridad y el 27,14% a Disponibilidad. Estas dos categorías concentraron el 97,49% del total, evidenciando que la operación estuvo orientada principalmente a la identificación de eventos de ciberseguridad y al seguimiento de la disponibilidad de la infraestructura. Frente al periodo anterior, en el que se registraron 327.607 eventos, se presentó un incremento del 101,65%, impulsado principalmente por el aumento de los eventos de Seguridad y Disponibilidad. Este comportamiento requiere mantener el seguimiento sobre las fuentes integradas, las reglas de correlación y los umbrales configurados, con el fin de determinar si la variación corresponde a condiciones operativas, cambios en la ingesta o situaciones que requieran acciones de afinamiento Como parte del proceso de mejora continua, se avanzó en el afinamiento de reglas de correlación, actualización de indicadores de compromiso (IOC) y optimización de casos de uso. Adicionalmente, se realizaron mesas de trabajo con los especialistas de las diferentes áreas para analizar el comportamiento de los dispositivos y las tendencias de los eventos, con el fin de reducir falsas alarmas, optimizar la generación de alertas y fortalecer la eficiencia operativa del Centro de Operaciones de Seguridad (SOC). Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: FortiSiem - Evidencia licenciamiento FortiSiem.pdf - Carpeta: Reportes FortiSiem Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 10	Verificado por el Supervisor

Ejecutar los análisis de vulnerabilidades solicitados por el DNP, entregar el informe de resultados, cumplir con las especificaciones dadas en el anexo técnico, presentar acciones de mitigación de las vulnerabilidades reportadas, y se deben seguir las recomendaciones e indicaciones dadas por la supervisión.	Para el mes de julio de 2026 se realizaron un total de 7 escaneos de vulnerabilidades por demanda, ejecutados mediante la herramienta Nessus, distribuidos de acuerdo con los requerimientos realizados por la Entidad y orientados a la identificación temprana de vulnerabilidades en activos tecnológicos específicos. De cada uno de estos escaneos se generó un informe técnico en formato HTML, el cual contiene el detalle de las vulnerabilidades identificadas, evidencias, niveles de severidad y recomendaciones preliminares de mitigación. Adicionalmente, se elaboró un archivo consolidado en formato Excel que integra los resultados de todos los escaneos realizados durante el periodo, permitiendo una visión global del estado de seguridad, priorización de hallazgos y seguimiento a las acciones de remediación. Los escaneos realizados con Nessus permitieron identificar oportunamente vulnerabilidades conocidas (CVE), configuraciones inseguras y oportunidades de mejora en la postura de seguridad de los activos evaluados, contribuyendo al fortalecimiento continuo de los controles de ciberseguridad de la Entidad. Evidencias: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Analisis de Vulnerabilidades Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 11	Verificado por el Supervisor

Ejecutar los análisis de vulnerabilidades solicitados por el DNP, entregar el informe de resultados, cumplir con las especificaciones dadas en el anexo técnico, presentar acciones de mitigación de las vulnerabilidades reportadas, y se deben seguir las recomendaciones e indicaciones dadas por la supervisión.	Para el mes de julio de 2026 se realizaron un total de 7 escaneos de vulnerabilidades por demanda, ejecutados mediante la herramienta Nessus, distribuidos de acuerdo con los requerimientos realizados por la Entidad y orientados a la identificación temprana de vulnerabilidades en activos tecnológicos específicos. De cada uno de estos escaneos se generó un informe técnico en formato HTML, el cual contiene el detalle de las vulnerabilidades identificadas, evidencias, niveles de severidad y recomendaciones preliminares de mitigación. Adicionalmente, se elaboró un archivo consolidado en formato Excel que integra los resultados de todos los escaneos realizados durante el periodo, permitiendo una visión global del estado de seguridad, priorización de hallazgos y seguimiento a las acciones de remediación. Los escaneos realizados con Nessus permitieron identificar oportunamente vulnerabilidades conocidas (CVE), configuraciones inseguras y oportunidades de mejora en la postura de seguridad de los activos evaluados, contribuyendo al fortalecimiento continuo de los controles de ciberseguridad de la Entidad. Evidencias: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Analisis de Vulnerabilidades Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 11	Verificado por el Supervisor

Realizar el ejercicio de Ethical hacking, entregar el informe de resultados, cumplir con las especificaciones dadas en el anexo técnico, y se deben seguir las recomendaciones e indicaciones dadas por la supervisión.	Este mes NO hubo necesidad de realizar este elemento.Durante el mes de julio de 2026 se complementaron las pruebas de Ethical Hacking a los siguientes aplicativos web: https://datalogo.dnp.gov.co/, https://dialogosregionales.dnp.gov.co/, https://finanzasdelclima.dnp.gov.co/Paginas/index.aspx, https://gesproysgr.dnp.gov.co/jsgr/, https://habitantesdecalle.sisben.gov.co, https://mapainversiones.dnp.gov.co, https://masclima.dnp.gov.co/#/ y https://mgaweb.dnp.gov.co. Estos portales cuentan con su informe técnico de hallazgos alojados en los en el Entrega de consolidado de vulnerabilidades identificadas en portales web - 1. De igualmente se realizaron pruebas de Ethical Hacking sobre los portales: https://www.dnp.gov.co/, http://ae.dnp.gov.co, https://orfeo.dnp.gov.co/login.php, https://www.sgr.gov.co, https://registrosocial.dnp.gov.co/, https://siiat.sgr.gov.co, https://sinergia20app.dnp.gov.co y https://mgaayuda.dnp.gov.co/IndexChatSUAIAVOZ.html. Cada uno de los hallazgos identificados en este ejercicio se encuentran debidamente documentados en su informe técnico alojado en el Entrega de consolidado de vulnerabilidades identificadas en portales web 2. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Ethical Hacking Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 12	Verificado por el Supervisor

Realizar el ejercicio de Ethical hacking, entregar el informe de resultados, cumplir con las especificaciones dadas en el anexo técnico, y se deben seguir las recomendaciones e indicaciones dadas por la supervisión.	Este mes NO hubo necesidad de realizar este elemento.Durante el mes de julio de 2026 se complementaron las pruebas de Ethical Hacking a los siguientes aplicativos web: https://datalogo.dnp.gov.co/, https://dialogosregionales.dnp.gov.co/, https://finanzasdelclima.dnp.gov.co/Paginas/index.aspx, https://gesproysgr.dnp.gov.co/jsgr/, https://habitantesdecalle.sisben.gov.co, https://mapainversiones.dnp.gov.co, https://masclima.dnp.gov.co/#/ y https://mgaweb.dnp.gov.co. Estos portales cuentan con su informe técnico de hallazgos alojados en los en el Entrega de consolidado de vulnerabilidades identificadas en portales web - 1. De igualmente se realizaron pruebas de Ethical Hacking sobre los portales: https://www.dnp.gov.co/, http://ae.dnp.gov.co, https://orfeo.dnp.gov.co/login.php, https://www.sgr.gov.co, https://registrosocial.dnp.gov.co/, https://siiat.sgr.gov.co, https://sinergia20app.dnp.gov.co y https://mgaayuda.dnp.gov.co/IndexChatSUAIAVOZ.html. Cada uno de los hallazgos identificados en este ejercicio se encuentran debidamente documentados en su informe técnico alojado en el Entrega de consolidado de vulnerabilidades identificadas en portales web 2. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Ethical Hacking Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 12	Verificado por el Supervisor

Realizar el ejercicio de ingeniería social, entregar el informe de resultados, cumplir con las especificaciones dadas en el anexo técnico, se deben seguir las recomendaciones e indicaciones dadas por la supervisión	Se adelantan el plan de actividades para el ejercicio de ingeniería social, el cual se planea para ser ejecutado durante le mes de octubre de 2026 El objetivo de este ejercicio es evaluar el nivel de concientización y resiliencia de los usuarios frente a posibles ataques de ingeniería social, tales como phishing, suplantación de identidad y manipulación de información. Asimismo, permitirá identificar posibles brechas en los controles de seguridad asociados al factor humano, considerado uno de los principales vectores de riesgo en la seguridad de la información. Para el desarrollo de esta actividad se ha adelantado la elaboración de una presentación (PPT) en la que se propone el alcance del ejercicio y las plantillas de campaña definidas para su ejecución. Considerando la volumetría de usuarios que hacen parte de la Entidad, se propone ejecutar el ejercicio en dos bloques: en el primero se seleccionará una cantidad determinada de usuarios, sobre los cuales se aplicará la primera plantilla (Temu); en el segundo se incluirán los usuarios restantes, empleando la segunda plantilla propuesta (Copilot). El objetivo de esta distribución es evaluar el comportamiento de los usuarios frente a dos escenarios de naturaleza distinta: uno de origen externo a la Entidad y otro asociado a una herramienta de uso corporativo, lo que permitirá comparar la reacción de los usuarios en cada caso y obtener una medición más representativa del nivel de concientización. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Ingeniería Social Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 13	Verificado por el Supervisor

Realizar el ejercicio de ingeniería social, entregar el informe de resultados, cumplir con las especificaciones dadas en el anexo técnico, se deben seguir las recomendaciones e indicaciones dadas por la supervisión	Se adelantan el plan de actividades para el ejercicio de ingeniería social, el cual se planea para ser ejecutado durante le mes de octubre de 2026 El objetivo de este ejercicio es evaluar el nivel de concientización y resiliencia de los usuarios frente a posibles ataques de ingeniería social, tales como phishing, suplantación de identidad y manipulación de información. Asimismo, permitirá identificar posibles brechas en los controles de seguridad asociados al factor humano, considerado uno de los principales vectores de riesgo en la seguridad de la información. Para el desarrollo de esta actividad se ha adelantado la elaboración de una presentación (PPT) en la que se propone el alcance del ejercicio y las plantillas de campaña definidas para su ejecución. Considerando la volumetría de usuarios que hacen parte de la Entidad, se propone ejecutar el ejercicio en dos bloques: en el primero se seleccionará una cantidad determinada de usuarios, sobre los cuales se aplicará la primera plantilla (Temu); en el segundo se incluirán los usuarios restantes, empleando la segunda plantilla propuesta (Copilot). El objetivo de esta distribución es evaluar el comportamiento de los usuarios frente a dos escenarios de naturaleza distinta: uno de origen externo a la Entidad y otro asociado a una herramienta de uso corporativo, lo que permitirá comparar la reacción de los usuarios en cada caso y obtener una medición más representativa del nivel de concientización. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Ingeniería Social Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 13	Verificado por el Supervisor

Implementación de la solución de inteligencia de amenazas, realizar monitorización continua de amenazas, entregar el informe de resultados, cumplir con las especificaciones dadas en el anexo técnico, se deben seguir las recomendaciones e indicaciones dadas por la supervisión.	Durante el periodo se realizó una investigación en fuentes abiertas y plataformas de inteligencia de amenazas con el propósito de identificar indicadores de compromiso relacionados con el incidente de seguridad reportado por Ecopetrol. Durante la revisión se analizaron posibles direcciones IP, dominios, URL, archivos, hashes y artefactos asociados con operaciones de Ransomware y con el grupo de amenaza mencionado en fuentes externas. Como resultado, se identificaron algunos indicadores técnicos relacionados de manera general con el Ransomware The Gentlemen; sin embargo, no se encontró evidencia pública que permitiera atribuirlos directamente al incidente de Ecopetrol. Asimismo, las direcciones IP difundidas inicialmente correspondían a rangos TEST-NET reservados para documentación, por lo que fueron descartadas al no constituir infraestructura maliciosa real. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Inteligencia de amenazas Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 14	Verificado por el Supervisor
Implementación de la solución de inteligencia de amenazas, realizar monitorización continua de amenazas, entregar el informe de resultados, cumplir con las especificaciones dadas en el anexo técnico, se deben seguir las recomendaciones e indicaciones dadas por la supervisión.	Durante el periodo se realizó una investigación en fuentes abiertas y plataformas de inteligencia de amenazas con el propósito de identificar indicadores de compromiso relacionados con el incidente de seguridad reportado por Ecopetrol. Durante la revisión se analizaron posibles direcciones IP, dominios, URL, archivos, hashes y artefactos asociados con operaciones de Ransomware y con el grupo de amenaza mencionado en fuentes externas. Como resultado, se identificaron algunos indicadores técnicos relacionados de manera general con el Ransomware The Gentlemen; sin embargo, no se encontró evidencia pública que permitiera atribuirlos directamente al incidente de Ecopetrol. Asimismo, las direcciones IP difundidas inicialmente correspondían a rangos TEST-NET reservados para documentación, por lo que fueron descartadas al no constituir infraestructura maliciosa real. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: Inteligencia de amenazas Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 14	Verificado por el Supervisor

Implementar y operar la solución de orquestación, automatización y remediación, se debe presentar la licencia de la solución implementada, cumplir con las especificaciones dadas en el anexo técnico, se deben seguir las recomendaciones e indicaciones dadas por la supervisión.	Durante el mes de julio de 2026 se continuó con el desarrollo y la puesta a punto de la instancia de FortiSoar dedicada al cliente DNP, avanzando en la construcción de PlayBooks de respuesta automatizada a incidentes. El trabajo se concentró en dos frentes principales: el bloqueo automático de IPs maliciosas detectadas por FortiSiem en los firewalls FortiGate, y la respuesta integral a incidentes de phishing con extracción de indicadores desde Exchange y validación mediante VirusTotal. Es importante resaltar que el desarrollo de PlayBooks en una plataforma SOAR no se limita al diseño de la lógica de automatización: requiere un ciclo considerable de pruebas y simulaciones controladas antes de habilitar cualquier flujo en producción. Durante julio se invirtieron aproximadamente 130 horas en pruebas y simulaciones orientadas a validar el correcto funcionamiento de los PlayBooks desarrollados, cifra que refleja el esfuerzo de depuración necesario para garantizar que las acciones automatizadas (bloqueos, notificaciones, extracción de indicadores) se ejecuten de forma confiable y sin efectos no deseados sobre el entorno del cliente. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: FortiSoar Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 15	Verificado por el Supervisor

Implementar y operar la solución de orquestación, automatización y remediación, se debe presentar la licencia de la solución implementada, cumplir con las especificaciones dadas en el anexo técnico, se deben seguir las recomendaciones e indicaciones dadas por la supervisión.	Durante el mes de julio de 2026 se continuó con el desarrollo y la puesta a punto de la instancia de FortiSoar dedicada al cliente DNP, avanzando en la construcción de PlayBooks de respuesta automatizada a incidentes. El trabajo se concentró en dos frentes principales: el bloqueo automático de IPs maliciosas detectadas por FortiSiem en los firewalls FortiGate, y la respuesta integral a incidentes de phishing con extracción de indicadores desde Exchange y validación mediante VirusTotal. Es importante resaltar que el desarrollo de PlayBooks en una plataforma SOAR no se limita al diseño de la lógica de automatización: requiere un ciclo considerable de pruebas y simulaciones controladas antes de habilitar cualquier flujo en producción. Durante julio se invirtieron aproximadamente 130 horas en pruebas y simulaciones orientadas a validar el correcto funcionamiento de los PlayBooks desarrollados, cifra que refleja el esfuerzo de depuración necesario para garantizar que las acciones automatizadas (bloqueos, notificaciones, extracción de indicadores) se ejecuten de forma confiable y sin efectos no deseados sobre el entorno del cliente. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capítulo: FortiSoar Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 15	Verificado por el Supervisor

Implementar y operar la solución de emulación de adversarios, se debe presentar la licencia de la solución implementada, cumplir con las especificaciones dadas en el anexo técnico, se deben seguir las recomendaciones e indicaciones dadas por la supervisión.	Basados en el RFC_1030 que se ejecutó durante julio de 2026 un ejercicio de emulación de adversarios sobre la plataforma Reveald Epiphany (Epiphany Validation Engine EVE), orientado a validar la efectividad real de los controles de seguridad de la Entidad frente a técnicas de ataque empleadas por atacantes reales. A continuación, se presenta el estado general del ejercicio, los principales hallazgos derivados de su análisis y los riesgos emergentes identificados. Durante el mes de julio de 2026, como resultado del RFC_1030, se efectuaron diferentes pruebas con la finalidad de evaluar los controles de seguridad de la Entidad, en particular el comportamiento del antivirus Trellix (EDR), frente a técnicas de ataque reales del catálogo MITRE ATTCK. El ejercicio se desarrolló bajo el enfoque assume breach, en un entorno de pruebas aislado, utilizando como objetivo el servidor Windows Server 2019 VSAPPRREVEALD, el cual replica las políticas, roles y configuraciones de los servidores de producción. Se generó un snapshot previo del servidor y las muestras no fueron ejecutadas dentro del mismo: únicamente se evaluó su transferencia, almacenamiento y detección, sin acciones destructivas ni afectación de la operación. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capitulo: Reveald (Epiphany) Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 16	Verificado por el Supervisor

Implementar y operar la solución de emulación de adversarios, se debe presentar la licencia de la solución implementada, cumplir con las especificaciones dadas en el anexo técnico, se deben seguir las recomendaciones e indicaciones dadas por la supervisión.	Basados en el RFC_1030 que se ejecutó durante julio de 2026 un ejercicio de emulación de adversarios sobre la plataforma Reveald Epiphany (Epiphany Validation Engine EVE), orientado a validar la efectividad real de los controles de seguridad de la Entidad frente a técnicas de ataque empleadas por atacantes reales. A continuación, se presenta el estado general del ejercicio, los principales hallazgos derivados de su análisis y los riesgos emergentes identificados. Durante el mes de julio de 2026, como resultado del RFC_1030, se efectuaron diferentes pruebas con la finalidad de evaluar los controles de seguridad de la Entidad, en particular el comportamiento del antivirus Trellix (EDR), frente a técnicas de ataque reales del catálogo MITRE ATTCK. El ejercicio se desarrolló bajo el enfoque assume breach, en un entorno de pruebas aislado, utilizando como objetivo el servidor Windows Server 2019 VSAPPRREVEALD, el cual replica las políticas, roles y configuraciones de los servidores de producción. Se generó un snapshot previo del servidor y las muestras no fueron ejecutadas dentro del mismo: únicamente se evaluó su transferencia, almacenamiento y detección, sin acciones destructivas ni afectación de la operación. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capitulo: Reveald (Epiphany) Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 16	Verificado por el Supervisor
Realizar los mantenimientos preventivos acordados y los mantenimientos correctivos solicitados por el DNP, cumpliendo con las especificaciones dadas en el anexo técnico, se debe presentar aprobación de los planes de mantenimiento preventivo y ordenes aprobadas de mantenimiento correctivo, evidencia de los acompañamientos de mantenimientos realizados por terceros, realizar la actualización de la CMDB y atender los requerimientos realizados por la supervisión.	Durante el mes de julio de 2026 no se realizaron mantenimientos preventivos. De acuerdo con el cronograma del proyecto se estima iniciar en el mes de septiembre de 2026. Evidencia: - Plan de mantenimiento preventivo DNP - V1.0.pdf Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 17	Verificado por el Supervisor

Realizar los mantenimientos preventivos acordados y los mantenimientos correctivos solicitados por el DNP, cumpliendo con las especificaciones dadas en el anexo técnico, se debe presentar aprobación de los planes de mantenimiento preventivo y ordenes aprobadas de mantenimiento correctivo, evidencia de los acompañamientos de mantenimientos realizados por terceros, realizar la actualización de la CMDB y atender los requerimientos realizados por la supervisión.	Durante el mes de julio de 2026 no se realizaron mantenimientos preventivos. De acuerdo con el cronograma del proyecto se estima iniciar en el mes de septiembre de 2026. Evidencia: - Plan de mantenimiento preventivo DNP - V1.0.pdf Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 17	Verificado por el Supervisor
Realizar el suministro y gestión de la bolsa de recursos TIC conforme a las necesidades establecidas por la entidad y a lo especificado en el anexo técnico, entregar las aprobaciones de ejecución de recursos y las evidencias de su ejecución.	En el mes de julio de 2026 se realizó una compra de una memoria Micro SD, por un valor de $37.128 IVA incluido. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capitulo: Bolsa de repuestos TIC Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 18	Verificado por el Supervisor
Realizar el suministro y gestión de la bolsa de recursos TIC conforme a las necesidades establecidas por la entidad y a lo especificado en el anexo técnico, entregar las aprobaciones de ejecución de recursos y las evidencias de su ejecución.	En el mes de julio de 2026 se realizó una compra de una memoria Micro SD, por un valor de $37.128 IVA incluido. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capitulo: Bolsa de repuestos TIC Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 18	Verificado por el Supervisor
Se deben realizar reuniones mensuales para: socializar el estado de la operación de los servicios y ejecución de actividades del contrato, y realizar otras reuniones entre los pares técnicos de especialista de la Oficina de Tecnología y Sistemas de Información (OTSI), para verificar la operación, monitoreo y soporte de la infraestructura tecnológica del DNP.	Durante el mes de julio de 2026 se realizaron reuniones de acuerdo al plan de comunicaciones: Seguimmiento Operativo, Seguimiento de Líneas de Servicio, Seguimiento internas de la UT, entre otras. Dentro de la ruta de evidencia se encuentran las actas y los adjuntos o soportes que apoyan cada reunión si aplica. El prefijo de los documentos indica la línea de servicios que realizó la reunión. Evidencia: - Carpeta: Reuniones Julio 2026 Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 18\Reuniones Julio 2026	Verificado por el Supervisor

Se deben realizar reuniones mensuales para: socializar el estado de la operación de los servicios y ejecución de actividades del contrato, y realizar otras reuniones entre los pares técnicos de especialista de la Oficina de Tecnología y Sistemas de Información (OTSI), para verificar la operación, monitoreo y soporte de la infraestructura tecnológica del DNP.	Durante el mes de julio de 2026 se realizaron reuniones de acuerdo al plan de comunicaciones: Seguimmiento Operativo, Seguimiento de Líneas de Servicio, Seguimiento internas de la UT, entre otras. Dentro de la ruta de evidencia se encuentran las actas y los adjuntos o soportes que apoyan cada reunión si aplica. El prefijo de los documentos indica la línea de servicios que realizó la reunión. Evidencia: - Carpeta: Reuniones Julio 2026 Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 18\Reuniones Julio 2026	Verificado por el Supervisor
Entregar las licencias de los softwares requeridos por el DNP, cumpliendo con las cantidades y tiempo de vigencia de la licencia que fueron requeridos en los numerales 9 y 11 del Anexo Técnico.	Se realizó la gestión para la adquisición del licenciamiento solicitado en los capítulos 9 y 11 del Anexo Técnico. ShareGate: Se gestionó la compra de ShareGate por un año. El compromiso indica que la renovación sera por el plazo de la ejecución del contrato (del 09/04/2026 al 28/12/2026). Sin embargo al no poder tener la licencia desde el día 1, se adquirió por doce meses a partir de la fecha de adquisición. ADManager Plus: El licenciamiento actual esta hasta el 31/08/2026. Se renovará en el mes de agosto. Blancco: La licencia se encuentra hasta el 25/01/2026. No se puede volver a renovar el uso de las licencias. Se utilizará hasta consumir las licencias activas. Eviencia: - Evidencia licencia ShareGate hasta 12052027.pdf - Evidencia licencia ADManager Plus DNP hasta 31082026.pdf - Evidencia licencia Blancco hasta 25022027.pdf Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 20	Verificado por el Supervisor

Entregar las licencias de los softwares requeridos por el DNP, cumpliendo con las cantidades y tiempo de vigencia de la licencia que fueron requeridos en los numerales 9 y 11 del Anexo Técnico.	Se realizó la gestión para la adquisición del licenciamiento solicitado en los capítulos 9 y 11 del Anexo Técnico. ShareGate: Se gestionó la compra de ShareGate por un año. El compromiso indica que la renovación sera por el plazo de la ejecución del contrato (del 09/04/2026 al 28/12/2026). Sin embargo al no poder tener la licencia desde el día 1, se adquirió por doce meses a partir de la fecha de adquisición. ADManager Plus: El licenciamiento actual esta hasta el 31/08/2026. Se renovará en el mes de agosto. Blancco: La licencia se encuentra hasta el 25/01/2026. No se puede volver a renovar el uso de las licencias. Se utilizará hasta consumir las licencias activas. Eviencia: - Evidencia licencia ShareGate hasta 12052027.pdf - Evidencia licencia ADManager Plus DNP hasta 31082026.pdf - Evidencia licencia Blancco hasta 25022027.pdf Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 20	Verificado por el Supervisor
Cumplir con los Acuerdos de Niveles de Servicio (ANS) según Anexo C ANS Servicios TIC, se debe presentar un análisis de causas cuando se presenten incumplimiento de ANS.	Para el mes de julio de 2026 se dio cumplimiento a los ANS de acuerdo con el Anexo Técnico del contrato. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capitulo: Acuerdos de Niveles de Servicio Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 21	Verificado por el Supervisor
Cumplir con los Acuerdos de Niveles de Servicio (ANS) según Anexo C ANS Servicios TIC, se debe presentar un análisis de causas cuando se presenten incumplimiento de ANS.	Para el mes de julio de 2026 se dio cumplimiento a los ANS de acuerdo con el Anexo Técnico del contrato. Evidencia: - Informe de Gestión - Julio de 2026 - V-1.0.pdf - Capitulo: Acuerdos de Niveles de Servicio Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 21	Verificado por el Supervisor

Presentar y ejecutar el plan de entrega de la operación de los servicios, dos meses antes de finalizar el plazo de ejecución del contrato, este plan debe ser acordado con la supervisión y se debe atender los requerimientos e indicaciones dadas por la supervisión.	Este mes NO hubo necesidad de realizar este elemento.	Verificado por el Supervisor
Presentar y ejecutar el plan de entrega de la operación de los servicios, dos meses antes de finalizar el plazo de ejecución del contrato, este plan debe ser acordado con la supervisión y se debe atender los requerimientos e indicaciones dadas por la supervisión.	Este mes NO hubo necesidad de realizar este elemento.	Verificado por el Supervisor
El contratista debe mantener vigente su afiliación en el FIRST durante el plazo total de ejecución del contrato.	Se evidencia que en el mes de Julio de 2026 el certificado de afiliación FIRST esta vigente. Evidencia: - Certificacón FIRST 2026.pdf Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 23	Verificado por el Supervisor
El contratista debe mantener vigente su afiliación en el FIRST durante el plazo total de ejecución del contrato.	Se evidencia que en el mes de Julio de 2026 el certificado de afiliación FIRST esta vigente. Evidencia: - Certificacón FIRST 2026.pdf Ruta: S:\1020 OI Oficina de Informatica\CENTRO DE SERVICIOS \CONTRATO UT CDS DNP-1198-2026 SGR-280-2026\3.- Ejecución\Informes de Gestión\4.- Julio 2026\Obligaciones específicas\Actividad 23	Verificado por el Supervisor

1.1. OBLIGACIONES CUMPLIDAS:

3.3. PRODUCTOS ENTREGADOS Y/O BIENES ENTREGADOS:

DESCRIPCIÓN DEL BIEN	CANTIDAD	FECHA DE ENTREGA	A SATISFACCIÓN

4. OBSERVACIONES A LAS ACTIVIDADES EJECUTADAS, A LAS OBLIGACIONES CUMPLIDAS, Y A LOS PRODUCTOS Y/O BIENES ENTREGADOS.

5. OBSERVACIONES ADICIONALES, SI A ELLO HUBIERE LUGAR.

5.1. ANÁLISIS MATERIALIZACIÓN Y MITIGACIÓN DEL RIESGO:

1. ¿Durante la ejecución se materializó algún riesgo?	NO
2. Tipo de riesgo	N/A
3. ¿Cómo se materializó el riesgo?	N/A
4. ¿Cómo se mitigó el riesgo?	N/A
5. ¿Fue oportuna la mitigación?	N/A
OBSERVACIONES:	

5.2. VERIFICACIÓN de obligaciones frente al SGSST

5.2.1 EXAMEN OCUPACIONAL

En caso de ser afirmativas las anteriores respuestas, por favor diligencie la siguiente información:

5.2.2. CAPACITACION EN EL SISTEMA DE GESTION DE SEGURIDAD Y SALUD EN EL TRABAJO

5.3. PUBLICACION DEL INFORME EN LA PLATAFORMA SECOP II

Se publicó el informe del mes 6 en SECOP: NO

NOTA: este cuadro deberá ser diligenciado a partir del **segundo (2do) informe**.

6. PORCENTAJES DE AVANCE PRESUPUESTAL Y EN EJECUCIÓN DEL CONTRATO.

6.1. AVANCE PRESUPUESTAL EN RAZÓN DE LOS PAGOS REALIZADOS:

Valor del Contrato	Valor a Ejecutar	Valor Ejecutado	Valor Restante
7.847.481.900	7.847.481.900	3.284.078.700	4.563.403.200
		42%	58%

6.2. AVANCE EN EL PORCENTAJE DE EJECUCIÓN DEL CONTRATO RESPECTO DE LOS PRODUCTOS Y/O BIENES ENTREGADOS.

En mi calidad de supervisor del contrato me permito avalar el contenido del informe y el avance en la ejecución del mismo de acuerdo a lo descrito.

El contrato no presenta a la fecha dificultades en su ejecución, ni situaciones exógenas que afecten el normal desarrollo del mismo.

	CLAUDIA ANGELICA BEN-AMY PAEZ	Nelson Fabio Pinzon Barrantes	Orlando Benavides Santacruz