Informe de Estudios Previos
Para la Adquisición del Derecho de Uso Herramienta de SIEM y SOC

A fin de preparar los procedimientos de contrataciones públicas con la información precisa y suficiente que justifique la necesidad de la contratación y la modalidad de selección del proveedor, es necesario que todo procedimiento de contratación se encuentre sustentado en estudios previos, de conformidad con las disposiciones del artículo 87 de la Ley 47-25 de Contrataciones Públicas así como su Reglamento de aplicación aprobado mediante el Decreto 52-26 y las políticas, manuales, guías u orientaciones normativas dictadas por la Dirección General de Contrataciones Públicas o las regulaciones especiales aplicables al objeto contractual, por lo que la Tesorería de la Seguridad Social (TSS), como parte de la etapa precontractual ha realizado el presente informe de estudios previos con la finalidad garantizar la correcta selección de los procedimientos, un mejor aprovechamiento de los recursos y una mayor eficiencia en la ejecución de los contratos.

El objetivo del presente informe es presentar los resultados de los estudios previos, que serán el punto de partida para el diseño del procedimiento a realizar para la adquisición del Derecho De Uso de la Herramienta de SIEM y SOC en cumplimiento con lo establecido en la Ley 47-25 y su Reglamento de aplicación aprobado mediante el Decreto No. 52-26.

En este sentido, luego de varias gestiones de levantamiento de información y consultas de las informaciones disponibles, del análisis de procesos históricos y de la validación de las condiciones de disponibilidad de dichos productos en el mercado, así como del análisis de la necesidad que se pretende satisfacer, se establecen a continuación los siguientes resultados.

Identificación de la necesidad y justificación del proceso

La Tesorería de la Seguridad Social (TSS) desempeña un papel fundamental en la gestión eficiente de los procesos de recaudo, distribución y pago de las cotizaciones del Sistema Dominicano de Seguridad Social (SDSS), así como el Sistema Único de Información y Recaudo (SUIR), por lo que, en el Plan Anual de Contrataciones (PAC), ha consignado para el año 2026 la adquisición del Derecho de Uso de la Herramienta de SIEM y SOC en el marco de su Plan Estratégico Institucional (PEI) para el periodo 2025-2028.

Este servicio permitirá a la institución fortalecer sus capacidades de detección, monitoreo y respuesta ante incidentes de ciberseguridad mediante la implementación de una herramienta de SIEM y un servicio de SOC que facilite la identificación temprana de amenazas, el análisis centralizado de eventos de seguridad y la atención oportuna de incidentes.

Especificaciones técnicas

Para la adquisición del Derecho de Uso de la Herramienta de SIEM y SOC Tercerizado se requiere que los servicios contengan las siguientes especificaciones técnicas:

Ítem	Rubro	Cantidad	Descripción	Especificaciones
1	81112501	1	Adquisición del Derecho de Uso Herramienta de SIEM y SOC	*Ver especificaciones debajo.

Plataforma SIEM

Atributo	Requerimiento mínimo
Modalidad de entrega	SaaS
Capacidad de procesamiento	Mínimo 22 GB/dia sostenidos.
Retención en analítica	Mínimo 3 meses de logs en caliente.
Disponibilidad de la plataforma	Igual o mayor a 99.99%.
Almacenamiento histórico	Capacidad de ampliación bajo demanda (retención fría).
Compatibilidad	Integración nativa con MITRE ATT&CK, UEBA, IoC e IoA.
Correlación	Análisis y detección en tiempo real con casos de uso adaptables al nivel de madurez del Cliente.
Visualización	Dashboards configurables y vistas ejecutivas y operativas.
API	Disponibilidad de API REST para integración con sistemas del Cliente.
Inteligencia de amenazas	Integración con feeds de Threat Intelligence del proveedor o de fabricantes reconocidos.

Plataforma SOAR

Atributo	Requerimiento mínimo
Inclusión	SOAR básico incluido en la suscripción MSSP del SOCaaS, sin costo adicional.
Playbooks	Capacidad de ejecutar playbooks de respuesta automatizada y semi-automatizada.
Orquestación	Integración con la plataforma SIEM y con sistemas de boletinería/ticketing.
Casos de uso	Implementación de casos de uso documentados y mantenibles.

Soporte técnico

- Atención técnica 24x7x365 por parte del oferente.
- Idiomas: español e inglés.
- Múltiples canales: portal web, correo electrónico y teléfono.
- Tiempos de respuesta y atención conforme a lolos niveles de servicios establecidos en este documento

Servicios administrados requeridos

Procesos operativos

- Gestión de incidentes de ciberseguridad y atención de solicitudes de cambio (RFCs).
- Capacitación y mejora continua del personal asignado y de los casos de uso.

- Evaluación periódica de desempeño con base en los niveles de servicios establecidos en este documento.
- Documentación operativa, gestión de conocimiento y registro de lecciones aprendidas.

Funciones del SOC

- Monitoreo continuo y correlación de eventos.
- Análisis y clasificación (triage) de alertas de seguridad.
- Detección de actividades sospechosas o anómalas.
- Notificación y escalamiento a los equipos resolutores del Cliente.
- Mantenimiento preventivo del SIEM/SOAR y de los casos de uso.
- Identificación de fuentes ruidosas y recomendaciones de afinamiento.
- Generación y mantenimiento de playbooks de respuesta.

Cumplimiento normativo y marcos de referencia

Los procesos operativos de ciberseguridad ofrecidos deberán encontrarse certificados y/o alineados a los siguientes marcos de referencia, lo cual deberá acreditarse documentalmente como parte de la propuesta:

- NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover).
- ISO/IEC 27001 — Sistema de Gestión de Seguridad de la Información (vigente).
- ISO/IEC 20000-1 — Gestión de Servicios de TI (vigente).
- ITIL como marco de referencia para gestión de servicios.

Respuesta a incidentes y CSIRT

- El oferente deberá contar con un CSIRT (Computer Security Incident Response Team) propio reconocido por FIRST (Forum of Incident Response and Security Teams) — la membresía deberá acreditarse documentalmente.
- El servicio incluirá la atención a 1 (un) evento de respuesta a incidentes durante la vigencia, con un esfuerzo de hasta 40 horas hombre.
- Disponibilidad de boletines informativos de inteligencia de amenazas, generados por el laboratorio interno del proveedor.

Niveles de servicio (SLA)

El oferente deberá comprometerse, como mínimo, a los siguientes niveles de servicio. Niveles de servicio inferiores a los aquí descritos serán motivo de descalificación; niveles superiores serán evaluados positivamente.

1. Atención y detección de incidentes

Severidad	Tiempo máximo de atención
Alto	10 minutos
Medio	15 minutos
Bajo	30 minutos
Informativo	60 minutos

2. Escalamiento de incidentes de ciberseguridad

Severidad	Tiempo máximo de escalamiento
Alto	45 minutos
Medio	90 minutos
Bajo	120 minutos
Informativo	120 minutos

Periodicidad de medición: mensual. Nivel objetivo de cumplimiento: 99% para eventos críticos.

3. Análisis y clasificación de eventos (triage)

Severidad	Tiempo máximo de atención
Alto	30 minutos
Medio	60 minutos
Bajo	90 minutos
Informativo	120 minutos

Periodicidad: mensual. Nivel objetivo: 99% para eventos críticos y altos.

4. Atención de requerimientos (RFC)

Severidad	Tiempo máximo de atención
Alto	≤ 8 horas
Medio	≤ 12 horas
Bajo	≤ 24 horas
Informativo	≤ 48 horas

Distribución de Indicadores de compromiso: nivel objetivo 99%.

5. Disponibilidad de la plataforma

Indicador	Compromiso mínimo
Disponibilidad mensual de la plataforma SaaS	99.99%
Disponibilidad del servicio SOC (atención humana)	24x7x365 sin ventanas de mantenimiento programadas que afecten la operación

Entregables del servicio

Como parte del servicio, el oferente deberá entregar al menos los siguientes reportes:

Entregable	Formato	Frecuencia estándar
Resumen de incidentes de seguridad identificados y escalados.	Reporte ejecutivo	A definir en transición
Resumen de amenazas e indicadores de compromiso (IoC) identificados y reportados.	Reporte ejecutivo	A definir en transición
Resumen de detección en SIEM, por reglas y casos de uso configurados.	Reporte ejecutivo	A definir en transición
Resumen de alertas y notificaciones realizadas a equipos resolutores.	Reporte ejecutivo	A definir en transición
Identificación de fuentes ruidosas y recomendaciones para su atención.	Reporte ejecutivo	Mensual
Análisis de los casos de uso y playbooks implementados.	Reporte ejecutivo	Mensual
Reporte de eventos, usuarios, activos y amenazas; tendencias para toma de decisiones.	Reporte ejecutivo	Semanal o bajo demanda

Adicionalmente, el proveedor entregará los reportes formales que se acuerden durante la transición, así como los reportes ad-hoc requeridos por investigaciones o auditorías.

Arquitectura conceptual y elementos técnicos

Modelo de despliegue

La arquitectura propuesta deberá considerar los siguientes elementos como mínimo:

- Plataforma SIEM/SOAR del oferente entregada como SaaS.
- Integración con plataformas de inteligencia de amenazas (Threat Intelligence) y motores de correlación.
- Acceso seguro del personal del SOC del oferente a la plataforma de gestión a través de mecanismos de autenticación robusta.

Inventario base fuentes de datos

Se presenta el inventario inicial de fuentes de datos a integrar a la plataforma SIEM. El inventario podrá ajustarse durante la transición sin afectar el alcance económico, siempre que el volumen total se mantenga dentro del límite de 22 GB/día contratado.

Fuente	Cantidad	Notas
Firewalls perimetrales	5	Dispositivos NGFW perimetrales en el sitio principal.
Plataforma de gestión/analítica de firewalls	1	Consola/analizador centralizado de los firewalls.
Servidores de alta utilización	10	Servidores críticos del Cliente.
Endpoints protegidos por antivirus/EDR	350	250 estaciones de usuario y 100 servidores.
Licencias de productividad con módulos de seguridad	350	Suite de productividad en la nube con módulos de seguridad avanzados (telemetría de identidad, correo y endpoint).

Volumen estimado de eventos: hasta 22 GB/día. Cualquier excedente sostenido será motivo de revisión contractual de capacidad.

Requisitos del oferente

El oferente deberá acreditar documentalmente todos los siguientes requisitos. La falta de cualquiera de estos requisitos será motivo de descalificación.

Requisitos legales y operativos

- Persona moral legalmente constituida con al menos 5 años de operación demostrable como Managed Security Services Provider (MSSP).
- Operación de SOC propio (no subcontratado).
- Capacidad de operación 24x7x365 con respaldo
- Acreditación de la póliza de ciber ataque
- Acuerdo de confidencialidad
- Informe SOC 2 Tipo 2

Certificaciones corporativas obligatorias

El proveedor deberá contar con las siguientes certificaciones vigentes a nombre de la persona moral o del grupo corporativo al que pertenezca, presentando copia de los certificados emitidos por organismos acreditados (ENAC, EMA, IAF o equivalentes):

Certificación	Alcance requerido
ISO/IEC 27001:2022	Seguridad de la Información — alcance que incluya SOC.
ISO/IEC 22301:2019	Continuidad del Negocio — alcance que incluya servicios de SOC.
ISO 9001:2015	Gestión de la Calidad.
ISO/IEC 20000-1:2018	Gestión de Servicios de TI — alcance que incluya SOC.
ISO 37001:2016	Sistema de Gestión Antisoborno.
SOC 2 Type 2	Criterios de servicios de confianza (seguridad, disponibilidad, integridad del procesamiento, confidencialidad, privacidad)

Acreditaciones técnicas y CSIRT

- Membresía vigente en FIRST (Forum of Incident Response and Security Teams) acreditada documentalmente.
- CSIRT propio con laboratorio de inteligencia de amenazas que emita boletines informativos.
- Cuando la propuesta incluya infraestructura propia de Data Center, el proveedor deberá contar con al menos una certificación de tercero independiente (ICREA, ANSI/TIA-942 o equivalente) sobre el sitio.

Recursos humanos

- Plantilla mínima de analistas SOC L1, L2 y L3 con turnos rotativos para cobertura 24x7x365.

- Personal con dominio de español e inglés para comunicación y reportes.
- Capacidad demostrable de respuesta a incidentes con personal dedicado al CSIRT.

Vigencia, transición e implementación

- Vigencia del servicio: 12 (doce) meses.
- Periodo de transición e implementación: hasta 30 (treinta) días hábiles contados a partir de la certificación del contrato ante la Contraloría General de la República.
- Durante la transición, el oferente deberá:
    a) Levantar el inventario detallado de fuentes
    b) Desplegar el colector.
    c) Configurar casos de uso iniciales.
    d) Acordar los reportes y el canal de comunicación con los equipos resolutores.
    e) Ejecutar pruebas de extremo a extremo.
    f) Entregar acta de cierre de transición.

Para la adquisición de Servicio Herramienta de SIEM y SOC, los oferentes deben demostrar que poseen las calificaciones profesionales, técnicas y financieras que aseguren su competencia, los recursos financieros y el bien solicitado para cumplir con el objeto contractual.

Resultados o Productos Esperados

Para la contratación del Derecho de Uso de la Herramienta de SIEM y SOC se requiere el siguiente resultado: Un (1) año de soporte y actualizaciones.

Análisis de las particularidades del mercado, en cuanto a cómo y en cuáles plazos se ofrece ese bien, se presta el servicio o se ejecuta la obra.

Plazo y Lugar de ejecución del objeto del proceso

El lugar de ejecución de los servicios será en el domicilio Tesorería de la Seguridad Social (TSS), ubicado en la Avenida Tiradentes No. 33, Torre de la Seguridad Social, Ensanche Naco, Santo Domingo, Distrito Nacional.

Tiempo de ejecución del servicio

El tiempo de ejecución del servicio será por el periodo de **1 año**. El plazo mencionado supone un ritmo de labor con jornadas y horarios que el oferente deberá expresar en su propuesta, para que la institución contratante realice los controles que le competen. Los aumentos de horario que disponga el proveedor no originarán mayores erogaciones para la institución contratante y serán asumidas exclusivamente por éste.

El plazo para la ejecución del servicio propuesto por el proveedor adjudicatario se convertirá en el plazo contractual, siempre y cuanto se ajuste al estimado propuesto por la institución contratante.

Modalidad del procedimiento aplicable, tipo de contrato y resultados esperados

Conforme el costo estimado de la contratación se ha determinado, tomando en cuenta la Resolución Núm. PNP-03-2026 que establece los umbrales topes para la determinación de la modalidad de selección de los procedimientos de contratación pública, correspondientes al año dos mil veintiséis (2026) y la naturaleza de lo requerido, que la modalidad de la contratación será a través de un procedimiento de **Contratación Simplificada** y la adjudicación será a un **único proveedor.**

El Contrato que resulte de este procedimiento de selección será mediante un contrato de **servicios**, para el cual se requiere la presentación de garantía de seriedad de la oferta y fiel cumplimiento de contrato conforme a las disposiciones y porcentajes establecidos a partir del artículo 162 de la Ley 47-25.

El plazo de entrega de los servicios objeto del presente contrato será no más de Veinte (20) días hábiles, luego de la recepción de la certificación del contrato por la Contraloría General de la República. En cumplimiento con lo establecido en el Párrafo III del Artículo 134 de la Ley No. 47-25 de Contrataciones Públicas.

Análisis de oferta y demanda y riesgos previsibles involucrados en la contratación de los servicios requeridos:

En el proceso de selección de proveedores para **la Adquisición del Derecho de Uso de la Herramienta SIEM & SOC** se ha identificado un número considerable de proveedores a nivel nacional, considerando los aspectos de oferta y demanda, así como las cláusulas jurídicas, económicas, técnicas y administrativas, de naturaleza reglamentaria, en tal sentido, es necesario que los oferentes cumplan con los requisitos para garantizar la calidad y el respaldo de los servicios.

Por la naturaleza del proceso, no se requiere presentar muestras, sino que en la propuesta técnica el oferente debe demostrar el cumplimiento de las especificaciones técnicas descritas en este informe de estudios previos.

Los riesgos de esta contratación han sido identificados y establecido en la matriz de riesgos que se anexa al presente informe la cual abarca desde la planificación hasta la adjudicación, liquidación del contrato, vencimiento de garantías de calidad del objeto del contrato.

Supervisor del contrato

La Tesorería de la Seguridad Social ha designado como supervisor o responsable del contrato **a la Dirección de Gestión de Normas, Cumplimiento y Ciberseguridad**, bajo la responsabilidad de **José Alberto Luna Peña, asesor de la Dirección de Gestión de Normas, Cumplimiento y Ciberseguridad.**

Condiciones de pago

La Tesorería de la Seguridad Social (TSS), realizará dos pagos de la siguiente manera:

- **Un primer pago del veinte por ciento (20%)** cuya gestión se iniciará una vez sea certificado el Contrato ante la Contraloría General de la Republica y se inicie el periodo de transición e implementación, con el recibido conforme por **José Alberto Luna Peña, asesor de la Dirección de Gestión de Normas, Cumplimiento y Ciberseguridad**, o quien este designe en su

representación. El proveedor que resulte adjudicado deberá emitir una factura con Número de Comprobante Gubernamental.

- **Un segundo pago del ochenta por ciento (80%)** cuya gestión se iniciará una vez sea finalizado el periodo de transición e implementación con el acta de cierre de transición recibido conforme por **José Alberto Luna Peña, asesor de la Dirección de Gestión de Normas, Cumplimiento y Ciberseguridad**, o quien este designe en su representación. El proveedor que resulte adjudicado deberá emitir una factura con Número de Comprobante Gubernamental.

- Los pagos se realizarán dentro de los treinta (30) días hábiles siguientes a la fecha de recepción de la factura.

- Si una MIPYME resulta adjudicada, se hará un anticipo del 30% del valor del contrato en un plazo no mayor a treinta (30) días hábiles desde la certificación del contrato, contra presentación de una Póliza de Seguro. El 70% restante se pagará una vez sea finalizado el periodo de transición e implementación con el acta de cierre de transición recibido conforme por José Alberto Luna Peña, asesor de la Dirección de Gestión de Normas, Cumplimiento y Ciberseguridad, o quien este designe en su representación, en un plazo no mayor a treinta (30) días hábiles.

- Conforme establece el artículo 225 del reglamento de aplicación de la ley 47-25 aprobado con el decreto 52-26, el desembolso del pago realizado a una MIPYME por concepto de anticipo debe ser registrado obligatoriamente en el Sistema Electrónico de Contrataciones Públicas, así como la constancia de su aplicación en la ejecución contractual.

- En cada factura podrán ser solicitadas certificaciones de la DGII y TSS a los fines de gestionar el pago, según corresponda.

- El proveedor adjudicataria deberá mantenerse en todo momento al día con sus obligaciones fiscales y de seguridad social, según corresponda, para poder recibir el pago correspondiente. En ese sentido, si por el no cumplimiento de estas obligaciones por parte del adjudicatario la Tesorería se ve imposibilitada de recibir los servicios objeto de la presente contratación, el contrato podrá ser rescindido dando pie a la adjudicación del proveedor que haya quedado en segundo lugar o a un nuevo proceso según corresponda.

- Los pagos se harán por transferencia bancaria a la cuenta que el proveedor tenga registrada en la DGCP, por lo que para recibir los pagos el suplidor debe encontrarse registrado como beneficiario en la Dirección General de Contrataciones Públicas y tener cuenta registrada. Esta cuenta debe ser en pesos dominicanos.

- La Tesorería de la Seguridad Social realiza retención del Impuesto Sobre la Renta de acuerdo con las Normas Legales Vigentes de la Dirección General de Impuestos Internos.

El costo estimado del bien, obra o servicio a contratar, que determine el presupuesto de la contratación e identifique la partida presupuestaria a afectar.

El costo estimado para **la Adquisición del Derecho de Uso de la Herramienta de SIEM & SOC** es de **Cinco Millones Trescientos Cincuenta Mil Pesos Dominicanos con 00/100 (RD$ 5,350,000.00), Exento de ITBIS.** El precio puede estar sujeto a cambios debido a:

- **La variación en la tasa del dólar:** Muchos productos se importan o contienen componentes importados que están afectados por la tasa de cambio del dólar estadounidense. Si la tasa de cambio del dólar sube en relación con la moneda local, los productos importados pueden volverse más caros, lo que podría aumentar el precio final para los consumidores.
- **La falta de abastecimiento en el mercado local:** Escasez de un producto en el mercado local debido a factores como problemas de producción, interrupciones en la cadena de suministro o una demanda inesperadamente alta, los precios tienen a subir. La oferta limitada en comparación con la demanda puede conducir a un aumento en los precios.
- **Políticas del fabricante sobre tiempos de renovación o adquisición del producto:** los fabricantes pueden tener políticas que influyen en el precio final de un producto, como establecer precios según la demanda o introducir nuevas versiones o modelos que afectan la percepción del valor anterior. Además, los programas de renovación o adquisición pueden influir en el precio si incluyen descuentos, incentivos u otros términos que afecten el costo para el consumidor.

El costo estimado para la adquisición de los servicios se hace en base a las informaciones disponibles en el SECP, en los catálogos de bienes y servicios y en el Sistema de Información de Precios, administrados por la Dirección General de Contrataciones Públicas. Además, se tomó en cuenta las diferentes variaciones que pueden afectar el precio final.

Los criterios sociales, ambientales y económicos asociados a la contratación, con el propósito de generar los mayores beneficios posibles, con los recursos disponibles.

Por la naturaleza de la contratación, se pudieran considerar criterios sociales que fomenten la inclusión de proveedores identificados como Mipymes o que se demuestre a través de buenas prácticas la inclusión social a través de la contratación de personas con discapacidad certificadas por el CONADIS o el fomento de políticas de responsabilidad ambiental en las empresas. Todo esto será determinado al momento de la elaboración del Pliego de Condiciones pudiéndose utilizar estos criterios como mecanismos de desempate.

Regulaciones aplicables a los bienes, servicios u obras.

El Decreto 71-21 y la Comunicación MINPRE-DMI-2022 del 01/02/2022 establecen la necesidad de que la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) emita informes y peritajes técnicos para los bienes y servicios que se adquieran y/o renuevan para las instituciones públicas en el marco de los procesos de compras y contrataciones relacionadas con Gobierno Digital.

Esto implica que la OGTIC tiene la responsabilidad de evaluar la idoneidad, eficiencia y seguridad de las soluciones tecnológicas que se pretenden adquirir y/o renovar para su uso en las instituciones públicas.

Sus informes y peritajes técnicos ayudarán a garantizar que las adquisiciones y/o renovaciones cumplan con los estándares requeridos en materia de tecnología de la información y comunicación, así como con los objetivos de Gobierno Digital establecidos por el gobierno.

En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, Capital de la República Dominicana, a los veinte (20) días del mes de junio del año dos mil veintiséis (2026).

Jose Alberto Luna Peña
Responsable Técnico

Elisa Cristina Jaquez Diaz
Responsable Legal

Darlin Antonio Martinez Diaz
Responsable Financiero