Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

INF-1035/26

INFORME SOLICITUD DE ASISTENCIA

TESORERÍA DE LA SEGURIDAD SOCIAL

TSS

SEPTIEMBRE 22, 2026.-

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Informe

Luego de un cordial saludo, sirva la presente para exponer consideraciones de la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), respecto al proceso de compra para la **contratación del derecho de uso herramienta de siem y soc,** el cual se nos ha presentado como dirección ejecutiva del gabinete de innovación y desarrollo digital.

Observaciones:

- Se adjunta carta de solicitud
- Se adjunta justificación de compra
- Se adjunta especificaciones técnicas

A groso modo se solicita:

- **1 Contratación del Derecho de Uso Herramienta de SIEM y SOC.**
  - 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.
  - APIDisponibilidad 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
    - Inclusión SOAR básico incluido en la suscripción MSSP del SOCaaS, sin costo adicional.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

  - 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.[EJ1.1][MG1.2]
  - 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

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- 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
  - 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)
  - 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.
- Atención y detección de incidentes
  - Severidad Tiempo máximo de atención
  - Alto 10 minutos
  - Medio 15 minutos
  - Bajo 30 minutos
  - Informativo 60 minutos
- Escalamiento de incidentes de ciberseguridad
  - Severidad Tiempo máximo de escalamiento
  - Alto 45 minutos

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Medio 90 minutos
- Bajo 120 minutos
- Informativo 120 minutos
- Periodicidad de medición: mensual. Nivel objetivo de cumplimiento: 99% para eventos críticos.

- 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.
- 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%.
- 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 escalado
    - Reporte ejecutivo A definir en transición
    - Resumen de amenazas e indicadores de compromiso (IoC) identificados y reportados. Reporte ejecutivo A definir en transición

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- 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.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

  - 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.
- Certificaciones corporativas obligatorias
  - 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.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

  - 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. [EJ2.1]
  - Durante la transición, el oferente deberá:
    - Levantar el inventario detallado de fuentes
    - Desplegar el colector.
    - Configurar casos de uso iniciales.
    - Acordar los reportes y el canal de comunicación con los equipos resolutores.
    - Ejecutar pruebas de extremo a extremo.
    - Entregar acta de cierre de transición.

Conclusión:

Luego de revisar la documentación aportada, verificar la solicitud y sus soportes, evaluamos las especificaciones técnicas y consideramos que cumplen con todos los aspectos necesarios requeridos y no solapan ningún proyecto que haya de ejecutarse desde la Agenda Digital 2030, esta aprobación tiene vigencia hasta el 31 de diciembre 2026.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Mario Adames

Encargado departamento Asistencia Técnica Especializada

Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC)

MF/ma

Oficina Gubernamental de Tecnologías de la Información y Comunicación
Manuel Mayrele - Director de Servicios Digitales Institucionales (23/09/2026 09:17 AST)
Mario Adames - Encargado/a de Departamento de Asistencia Técnica Especializada (23/09/2026 09:44 AST)
Edgar Batista Carrasco - Director General (23/09/2026 12:52 AST)
Documento firmado digitalmente, para validar en medio electrónico:
https://buzon.firmagob.gob.do/inbox/app/ogtic/v/6e3a06d6-ec37-4696-afae-c1a378d9c4b5

GOBIERNO DE LA REPÚBLICA DOMINICANA
ADMINISTRACIÓN PÚBLICA