ESPECIFICACIONES TÉCNICAS

RENOVACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNETICOS

SANTO DOMINGO, R.D.
19 DE ENERO DEL 2026

CONTENIDO

NOMBRE DEL PROCESO

Renovación de Servicios de Monitoreo y Respuesta a Incidentes Cibernéticos para el Poder Judicial.

OBJETIVO GENERAL

Renovar el contrato de prestación de servicios de SOC (Centro de Operaciones de Seguridad) para el monitoreo del ciberespacio y la respuesta ante incidentes cibernéticos relacionados con la infraestructura tecnológica que soporta los sistemas de información críticos del Poder Judicial.

INTRODUCCION

En fecha 11 de octubre del 2022 el Comité de Compras y Licitaciones del Consejo del Poder Judicial decidió adjudicar mediante el Acta núm. 007 el proceso de referencia CP-CPJ-BS-12-2022 al Consorcio INCIBER, los servicios de monitoreo y respuesta a incidentes cibernéticos para el Poder Judicial.

A partir de esta adjudicación, el Poder Judicial cuenta con un Centro de Operaciones de Seguridad (SOC) cuya actividad se mantiene las 24 horas del día, los siete días de la semana. En el marco de este servicio tenemos el monitoreo en tiempo real de la infraestructura crítica del Poder Judicial, el análisis diario de bitácoras y comportamientos anómalos, la gestión de incidentes cibernéticos y los servicios de Inteligencia de Amenazas y Cacería de Amenazas (Threat Hunting).

El 02 de julio del 2025 fue adjudicado a la empresa Consorcio INCIBER, S.R.L. el proceso para la contratación de los servicios de monitoreo y respuesta a incidentes cibernéticos del Poder Judicial de referencia número: PEPU-CPJ-04-2025. A través de este proceso fueron adquiridos los servicios mencionados, para mantener un monitoreo de la infraestructura critica del Poder Judicial, (24/7/365) por un año.

Es importante destacar, que el enfoque principal de este servicio de monitoreo y respuesta a incidentes cibernéticos son los servicios tecnológicos críticos del Poder Judicial, tales como el portal de Acceso Judicial, el Sistema de Gestión de Casos, la plataforma de firma electrónica, entre otros. En ese sentido, y tomando en consideración los siguientes aspectos, solicitamos la renovación del contrato de prestación de servicios de SOC con el proveedor Consorcio INCIBER, quien en los últimos años ha consolidado su centro de operaciones de seguridad, tomando así mismo en consideración los siguientes aspectos:

- Este proceso de implementación tomó aproximadamente ocho (8) meses. En caso de adjudicarse el proceso a otra empresa, sería necesario iniciar nuevamente la implementación de este servicio e implicaría unos costos mayores para la institución. En consecuencia, las plataformas críticas del Poder Judicial no estarán siendo monitoreadas durante este periodo de tiempo.
- Los procesos de monitoreo y respuesta a incidentes fueron establecidos y recibimos notificaciones e informes de actividad cibernética de manera periódica.
- Este consorcio cuenta con experiencia en materia de ciberseguridad y ya está familiarizado con el entorno cibernético del Poder Judicial, lo que facilita la detección y respuesta.
- El nivel de madurez del centro de operaciones de seguridad ha aumentado en los últimos años evidenciándose a través de las siguientes certificaciones:
    - Seguridad de la información ISO/IEC 27001
    - Gestión de Servicios de TI ISO/IEC 20000-1

Por consiguiente, tenemos a bien solicitar y recomendar al Comité de Compras y Contrataciones del Consejo del Poder Judicial la selección del proveedor Consorcio INCIBER SRL. bajo una modalidad que permita que este sea el único proveedor.

DE LOS BIENES Y SERVICIOS A ADQUIRIRSE

Servicios de SOC:

a) Monitoreo
b) Respuesta a incidentes cibernéticos
c) Inteligencia de amenazas

HITOS

El siguiente hito será factor clave para medir el avance del proceso y liberar el pago:

a. Hito No. 1 – 100% Renovación de servicios de monitoreo.

FORMA DE PAGO

100% pago total, aceptación conforme de certificación de recepción validado por la Dirección de TIC.

ESPECIFICACIONES TÉCNICAS

Ítem	Cant.	UDM	Descripción	No.	Especificación técnica
1	1	Servicio	Servicios de SOC	1	Monitoreo en tiempo real de la infraestructura crítica del Poder Judicial.
				2	Análisis diario de bitácoras y comportamientos anómalos.
				3	Gestión de incidentes cibernéticos.
				4	Servicios de Inteligencia de Amenazas y Cacería de Amenazas (Threat Hunting).
				5	La siguiente infraestructura debe ser monitoreada: a) 10 servicios web publicados en internet. b) 100 dispositivos alojados en una infraestructura de nube híbrida. c) Nombres de dominios adquiridos parecidos. d) Certificados digitales adquiridos parecidos. e) Correos fraudulentos haciéndose pasar por la institución. f) Robo de credenciales. g) Búsqueda de sitios falsos parecidos a los sitios del Poder Judicial. h) Fuga de datos en la Deep Web.
				6	Tomar en consideración que el Poder Judicial cuenta con su propia infraestructura SIEM, Directorio Activo, antivirus, cifrado y cortafuegos.
				7	Servicios de asesoría y apoyo en la contención de riesgos identificados.
				8	Apoyo técnico remoto y/o presencial ante incidencias de seguridad que lo ameriten.
				9	El Poder Judicial debe tener acceso a los tableros (dashboards) en tiempo real de cada fuente de información monitoreada.
				10	Reportes de incidencias y postura de seguridad de los servicios críticos con periodicidad mensual y en demanda. También se deben generar reportes posteriores a una falla o incidente crítico de ciberseguridad.

				11	Reportes de cumplimiento con normativas de la familia ISO 27000.
				12	Suscripción del servicio de SOC 24/7 por un (1) año.
				13	Contemplar dentro del servicio la realización de pruebas de penetración a la infraestructura crítica.

TIEMPO DE ENTREGA

La renovación será efectiva a partir de vencimiento del contrato actual, el cual concluye el 11 de junio de 2026, garantizando así la continuidad ininterrumpida de los servicios.

LUGAR DE ENTREGA

La entrega debe ser realizada en los portales de administración del Poder Judicial.

CRITERIOS DE EVALUACIÓN.

Los bienes requeridos y los otros requerimientos serán evaluados bajo el método de **Cumple / No Cumple**, utilizando el siguiente cuadro:

Item	Bienes Requeridos	No.	Detalles	Cumplimiento
x	Servicio Requerido	1	Especificación técnica	Cumple/ No Cumple
		2	…	

CRITERIOS DE ADJUDICACIÓN

La adjudicación será decidida a favor de un ÚNICO oferente cuya propuesta: 1) haya sido calificada como CUMPLE en las propuestas técnicas y económicas por reunir las condiciones legales, técnicas y económicas requeridas en los presentes Pliegos de Condiciones.

El oferente que resulte adjudicatario deberá firmar un Acuerdo de Confidencialidad.

Aseguramos que los criterios utilizados para la elaboración de este documento están basados en los principios éticos, de transparencia, de imparcialidad y de procurar proteger los intereses del Poder Judicial.

Este documento sustituye, deroga y deja sin efecto cualquier otro relativo a las especificaciones técnicas para la Renovación de Servicios de Monitoreo y Respuesta a Incidentes Cibernéticos para el Poder Judicial.

Equipo de peritos:

Bernardo Barreiro
Coordinador de Seguridad y Monitoreo TIC

Adderli de la Rosa
Gerente de Seguridad de Información

Luis A. Vargas De La Cruz
Coordinador de Seguridad de Infraestructura

Revisado por:

Emmanuel E. Tejada
Subdirector de Seguridad de la Información y Servicios TIC