ESPECIFICACIONES TÉCNICAS

CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNETICOS

SANTO DOMINGO, R.D.
22 ENERO DEL 2024

CONTENIDOS

NOMBRE DEL PROCESO

Renovación de la contratación de los 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).

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 del contrato de prestación de servicios.

FORMA DE PAGO

La forma de pago propuesta es:

b. 100% pago final, aceptación conforme del informe de recepción correspondiente al hito 1.

ESPECIFICACIONES TÉCNICAS

Ítem	Descripción	No.	Especificación técnica
1	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 entrega de los servicios deberá ser en cinco (05) días calendario contados a partir de la recepción de la orden de compra.

LUGAR DE ENTREGA

Los servicios deben ser entregados en el edificio del Consejo del Poder Judicial ubicado en la Av. Enrique Jiménez Moya esq. Juan de Dios Ventura Simó, Centro de los Héroes, Santo Domingo, Distrito Nacional.

CRITERIOS DE EVALUACIÓN.

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

Lote	Bienes Requeridos	No.	Detalles	Cumplimiento
x	Bien Requerido	1	Especificación técnica	Cumple/ No Cumple
		2	…	
		3	…	

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, y 2) presente el menor precio.

El oferente que resulte adjudicatario deberá firmar un Acuerdo de Confidencialidad antes de iniciar con la implementación.

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 la Contratación de los 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
Coordinador de Seguridad de Infraestructura

Emmanuel E. Tejada
Gerente de Seguridad y Monitoreo TIC

Revisado por:

Welvis Beltrán
Director de TIC