INFORME DE JUSTIFICACIÓN

CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNÉTICOS

SANTO DOMINGO, R.D.
22 DE ENERO DEL 2024

TABLA DE CONTENIDO

1. Objetivo 3

2. Antecedentes 3

3. Justificación técnica 3

1. Objetivo

Presentar la justificación técnica para la renovación del 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.

2. Antecedentes

El 17 de octubre de 2022, El Pleno de la Suprema Corte de Justicia (SCJ) aprobó el Reglamento de aplicación de la Ley núm. 339-22 que habilita el Uso de Medios Digitales en el Poder Judicial, normativa que tiene por objeto la implementación y regulación de las herramientas tecnológicas en los procesos judiciales y administrativos de cara a las competencias de los tribunales.

En ese sentido, para la implementación de dicha ley, a través de su reglamento de aplicación, fue necesaria la contratación de los siguientes servicios orientados a la ciberseguridad:

a. Servicios de auditoría a la calidad del software y pruebas de penetración, con el fin de identificar y solventar cualquier vulnerabilidad que presenten los activos que soportan el Sistema de Gestión de Casos y el Acceso Digital.
b. Herramienta para el registro de usuarios (servicios de Onboarding digital), que facilitará el registro de los ciudadanos y la verificación de su identidad para el acceso al portal de Acceso Digital, donde podrán realizar sus trámites.
c. **Centro de Operaciones de Seguridad (SOC), facilitando el monitoreo de la infraestructura tecnológica critica 24/7 y la respuesta a incidentes cibernéticos a través de un primer nivel de soporte y su oportuna escalación a los especialistas de ciberseguridad del Poder Judicial cuando esto sea necesario.**
d. Solución de monitoreo y respuesta a incidentes cibernéticos basada en Inteligencia Artificial. Sistema que permite responder a cualquier actividad sospechosa de manera proactiva, aplicando controles de seguridad específicos para cada caso. Este sistema aprende los patrones de comportamiento de la red institucional para mantener los servicios e infraestructura tecnológicas que son accedidos a través de internet protegidos ante amenazas.

3. Justificación técnica

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, la institución ha establecido un Centro de Operaciones de Seguridad (SOC) el cual opera las 24 horas del día, los siete días de la semana. En el marco de este servicio, llevamos a cabo el monitoreo en tiempo real de la infraestructura crítica del Poder Judicial, realizamos

el análisis diario de bitácoras y comportamientos anómalos, gestionamos incidentes cibernéticos y proporcionamos servicios de Inteligencia de Amenazas y Cacería de Amenazas (Threat Hunting).

Es crucial destacar, que el enfoque principal de este servicio de monitoreo y respuesta a incidentes cibernéticos se centra en 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 este sentido, y considerando los siguientes aspectos, solicitamos la renovación del contrato de prestación de servicios de SOC con el proveedor Consorcio INCIBER, según lo descrito en las especificaciones técnicas:

- Este proceso de implementación tomó aproximadamente ocho (8) meses. En caso de que el proceso sea adjudicado a otra empresa, sería necesario iniciar nuevamente la implementación de este servicio, lo que conllevaría 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 de la Institución, lo que facilita la detección y respuesta.

En consecuencia, tenemos a bien solicitar y recomendar al Comité de Compras y Contrataciones del Consejo del Poder Judicial, que el proceso se realice bajo la modalidad que permita de Excepción Proveedor Único. Emitimos este informe para sus consideraciones.

Este documento sustituye, deroga y deja sin efecto cualquier otro relativo al Informe de Justificación para la renovación del contrato de prestación de servicios de monitoreo y respuesta a incidentes cibernéticos para el Poder Judicial.

Elaborado por:

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