PROCEDIMIENTO DE COMPARACIÓN DE PRECIOS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNÉTICOS PARA EL PODER JUDICIAL
Referencia: CP-CPJ-BS-12-2022.

CIRCULAR NÚMERO 2

Fecha: 29 de agosto de 2022

El Poder Judicial de la República Dominicana, en el marco del procedimiento de la comparación de precios, llevada a cabo para la **contratación de los servicios de monitoreo y respuesta a incidentes cibernéticos para el Poder Judicial**, referencia número **CP-CPJ-BS-12-2022**, y actuando de conformidad con lo establecido en el numeral 12 de los términos de referencia, tiene a bien responder las preguntas por parte de los oferentes interesados, recibidas de manera oportuna y en tiempo hábil, según el plazo establecido en el cronograma de actividades (copiadas textualmente de la manera en que fueron recibidas).

SECCIÓN I- PREGUNTAS DE CARÁCTER TÉCNICO.

Las preguntas de carácter técnico respondidas por los peritos se encuentran anexas al presente documento, el cual consta de siete (7) páginas.

Atentamente,

Yerina Reyes Carrazana
Gerente de Compras

PODER JUDICIAL | REPÚBLICA DOMINICANA
Yerina Reyes Carrazana

26 de agosto del 2022

PREGUNTAS Y RESPUESTAS

PROCEDIMIENTO DE COMPARACIÓN DE PRECIOS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNÉTICOS PARA EL PODER JUDICIAL
Referencia: CP-CPJ-BS-12-2022.

Pregunta 1:
El monitoreo de todos los componentes de la infraestructura mencionada, debe hacerse desde una misma herramienta?.

Respuesta 1:
Esto dependerá de la herramienta o solución utilizada por cada oferente.

Pregunta 2:
Que solución de SIEM, Antivirus y Firewall utilizan actualmente?

Respuesta 2:
Actualmente utilizamos FortiSIEM, Trend Micro y Fortinet.

Pregunta 3:
¿Para el componente de Servicios de Asesoría y contención de riesgo identificados se limitan al alcance de los componentes monitoreados?

Respuesta 3:
Los requerimientos detallados en las especificaciones técnicas del proceso tienen como alcance la infraestructura a ser monitoreada.

Pregunta 4:
¿A cuántos empleados se requiere capacitar en el uso de las soluciones?

Respuesta 4:
Se debe contemplar la capacitación necesaria para 10 especialistas técnicos del Poder Judicial. **Ver enmienda.**

Pregunta 5:
¿Qué niveles de soporte a la operación se requieren? (primer, segundo o tercer nivel)

Respuesta 5:
Son requeridos el primer y el segundo nivel de soporte. **Ver enmienda.**

26 de agosto del 2022

PREGUNTAS Y RESPUESTAS

PROCEDIMIENTO DE COMPARACIÓN DE PRECIOS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNÉTICOS PARA EL PODER JUDICIAL
Referencia: CP-CPJ-BS-12-2022.

Pregunta 6:
Los servicios web publicados en la nube, que tecnología utilizan? (apache, IIS, especificar proveedor de hospedaje o servicio web)

Respuesta 6:
Los servicios web publicados se encuentran alojados en nuestra nube híbrida mediante la tecnología de IIS.

Pregunta 7:
Características de los 100 dispositivos alojados en nube hibrida (Modelo, Sistema Operativo, rol, etc)

Respuesta 7:

Marca	Modelo	Sistema Operativo	Cantidad
UTM - Fortigate	1100E	FortiOS	2
UTM - Fortigate	500E	FortiOS	2
UTM - Fortigate	300E	FortiOS	1
Servidor web	Virtualizados	Microsoft Windows Server 2012, 2016 y 2019	15
Servidor de aplicaciones	Virtualizados	Microsoft Windows Server 2012, 2016 y 2019	35
Servidor de base de datos	Virtualizados	Microsoft Windows Server 2012, 2016 y 2019	25
Servidor de dominio	Virtualizados	Microsoft Windows Server 2012, 2016 y 2019	10
Servidor - DELL	XC730XD	Microsoft Windows Server 2019 (Hipervisor Hyper-V)	4
Servidor - HP	ProLiant DL380 Gen10	Microsoft Windows Server 2019 (Hipervisor Hyper-V)	6
Total general			100

Pregunta 8:
¿Los 100 dispositivos alojados en la nube está enviando datos de logs o tienen integración con el SIEM?

Respuesta 8:
Actualmente estos logs están disponibles en la nube de Azure. La solución SIEM está en proceso de implementación por lo que esta integración aún no existe.

26 de agosto del 2022

PREGUNTAS Y RESPUESTAS

PROCEDIMIENTO DE COMPARACIÓN DE PRECIOS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNÉTICOS PARA EL PODER JUDICIAL
Referencia: CP-CPJ-BS-12-2022.

Pregunta 9:
¿Que tecnología SIEM poseen?

Respuesta 9:
Fortinet / FortiSIEM.

Pregunta 10:
¿El SIEM con el que cuentan esta siendo utilizado en producción, tienen analistas?, tienen procesos definidos para la gestión de incidentes?

Respuesta 10:
Actualmente la solución SIEM está en proceso de implementación y los procesos aún están siendo documentados. Contamos con un equipo de analistas de seguridad que participará del proceso de respuesta a incidentes.

Pregunta 11:
¿Los servicios de SOC lo deberíamos hacer administrando el SIEM que poseen?

Respuesta 11:
Sí, en las especificaciones técnicas, numeral 6, citamos: Tomar en consideración que el Poder Judicial cuenta con su propia infraestructura SIEM, Directorio Activo, antivirus, cifrado y cortafuegos.

Pregunta 12:
¿Cantidad de firewalls que poseen?

Respuesta 12:
Cinco (5) firewalls a monitorear.

Pregunta 13:
¿Cantidad de consolas de Antivirus que poseen?

Respuesta 13:
Poseemos una consola de antivirus.

Pregunta 14:
¿Cantidad de dominios de AD que poseen?

Respuesta 14:
Un (1) dominio de Active Directory.

26 de agosto del 2022

PREGUNTAS Y RESPUESTAS

PROCEDIMIENTO DE COMPARACIÓN DE PRECIOS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNÉTICOS PARA EL PODER JUDICIAL
Referencia: CP-CPJ-BS-12-2022.

Pregunta 15:
¿Posee un proceso de Monitoreo de Seguridad?

Respuesta 15:
Los procesos de Monitoreo de Seguridad se encuentran en proceso de documentación.

Pregunta 16:
¿Posee proceso de Gestión de Incidentes? En base a que normativa o marco de trabajo esta desarrollado?
Respuesta 16:
El proceso de Respuesta a Incidentes cibernéticos está en proceso de documentación.

Pregunta 17:
¿El cliente cuenta con un documento del plan para la respuesta ante incidentes de seguridad de la información?

Respuesta 17:
El proceso de Respuesta a Incidentes cibernéticos está en proceso de documentación.

Pregunta 18:
¿La responsabilidad de una contención y erradicación de un incidente de seguridad, dependerá del Cliente y sus correspondientes administradores de las plataformas tecnológicas?, Especificar.

Respuesta 18:
Sí, la responsabilidad de una contención y erradicación de un incidente de seguridad dependerá del Poder Judicial y sus correspondientes administradores de las plataformas tecnológicas. Sin embargo, son requeridos los servicios de asesoría y apoyo en caso de ser necesarios.

Pregunta 19:
¿Poseen un listado o inventario de las tecnologías que serán objeto de una respuesta o acción por el oferente y realizar contención a un incidente de seguridad?

Respuesta 19:
La responsabilidad de una contención y erradicación de un incidente de seguridad dependerá del Poder Judicial y sus correspondientes administradores de las plataformas tecnológicas. Sin embargo, son requeridos los servicios de asesoría y apoyo en caso de ser necesarios. En el marco de los servicios de monitoreo a la siguiente tecnología:

- ✓ Virtualización con HyperV y Kubernetes.

26 de agosto del 2022

PREGUNTAS Y RESPUESTAS

PROCEDIMIENTO DE COMPARACIÓN DE PRECIOS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNÉTICOS PARA EL PODER JUDICIAL
Referencia: CP-CPJ-BS-12-2022.

- ✓ IIS
- ✓ SQL Server
- ✓ Microsoft Active Directory / Azure AD.
- ✓ Fortinet
- ✓ Trend Micro.

Pregunta 20:
Por favor indicar para el dimensionamiento, la cantidad promedio mensual de incidentes de seguridad (SOC) que se presentan en la organización

Respuesta 20:
La solución SIEM está en proceso de implementación por lo que esta información aún no está disponible.

Pregunta 21:
¿Posee la categorización de incidentes de su plataforma, por tipo, plataforma y criticidad?

Respuesta 21:
En este momento no contamos con esta información, sin embargo, estará siendo documentada durante el proceso de incorporación del SOC.

Pregunta 22:
¿Posee la organización grupos resolutorios para cada uno de los incidentes categorizados en su plataforma?

Respuesta 22:
Existen grupos resolutorios para los tipos de incidentes, sin embargo, la plataforma está en proceso de implementación. Esta información será suministrada durante el proceso de incorporación del SOC.

Pregunta 23:
¿Cuenta con matriz de escalamiento clara y detallada para la notificación de eventos en horario 5x8 y 7x24?

Respuesta 23:
La matriz de escalamiento de incidentes será suministrada durante el proceso de implementación al oferente que resulte adjudicatario.

26 de agosto del 2022

PREGUNTAS Y RESPUESTAS

PROCEDIMIENTO DE COMPARACIÓN DE PRECIOS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNÉTICOS PARA EL PODER JUDICIAL
Referencia: CP-CPJ-BS-12-2022.

Pregunta 24:
¿Existen niveles de Acuerdo de Servicio de Notificación para el registro, notificación y respuesta a incidentes durante días y horas hábiles y no hábiles?

Respuesta 24:
Los procesos de Monitoreo y Respuesta a Incidentes de seguridad se encuentran en proceso de documentación.

Pregunta 25:
¿Posee Casos de Uso de Monitoreo definido por sistema o plataforma?

Respuesta 25:
Los casos de uso son los siguientes:

a. Creación, eliminación de objetos en el Directorio Activo.
b. Delegación de permisos en el Active Directory.
c. Usuarios agregados o removidos de grupos de seguridad / distribución.
d. Cambios realizados en las políticas de grupo (GPO).
e. Actividades relacionadas con inicios de sesión sospechosos.
f. Seguimiento a cuentas privilegiadas.
g. Infección de malware.
h. Navegación y comunicaciones maliciosas.
i. Ataques detectados en IPS.

Pregunta 26:
¿cuántos dominios externos (FQDN) desea monitorear y proteger para prevencion de usurpación de identidad via correo y DNS?

Respuesta 26:

i. poderjudicial.gob.do
ii. portal.poderjudicial.gob.do
iii. transparencia.poderjudicial.gob.do
iv. dialogojusticia.poderjudicial.gob.do
v. escalafonjudicial.poderjudicial.gob.do
vi. diadelpoderjudicial.poderjudicial.gob.do
vii. webmail.poderjudicial.gob.do
viii. observatorio.poderjudicial.gob.do

26 de agosto del 2022

PREGUNTAS Y RESPUESTAS

PROCEDIMIENTO DE COMPARACIÓN DE PRECIOS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE MONITOREO Y RESPUESTA A INCIDENTES CIBERNÉTICOS PARA EL PODER JUDICIAL
Referencia: CP-CPJ-BS-12-2022.

ix. observatoriojusticiaygenero.poderjudicial.gob.do
x. sistemadegestiondecasos.poderjudicial.gob.do

Atentamente:

Equipo de peritos:

Luis Joel Mejia
Analista de Continuidad
Consejo del Poder Judicial

Adderli de la Rosa
Coordinador de Seguridad de Infraestructura
Consejo del Poder Judicial

Emmanuel E. Tejada
Gerente de Seguridad y Monitoreo TIC
Consejo del Poder Judicial

Revisado por:

Welvis Beltrán
Director de Tecnología y Comunicaciones
Consejo del Poder Judicial