**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 1

Fecha: 25 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 trece (13) páginas.

Atentamente,

**Yerina Reyes Carrazana**
Gerente de Compras

22 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.**

22 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:**
• En las especificaciones técnicas, punto 5
- Detallar el listado de equipos que formaran parte del monitoreo (cantidad, marca, modelo).

**Respuesta 6:**

| Marca | Modelo | Cantidad |
|---|---|---|
| UTM - Fortigate | 1100E | 2 |
| UTM - Fortigate | 500E | 2 |
| UTM - Fortigate | 300E | 1 |
| Servidor - DELL | XC730XD | 4 |
| Servidor - HP | ProLiant DL380 Gen10 | 6 |
| Máquinas virtuales | HYPER - V | 85 |
| Total general | | 100 |

**Pregunta 7:**
- En las especificaciones técnicas, punto 6
- Indicar marca y modelo del SIEM con el que cuenta el Consejo del Poder Judicial.

**Respuesta 7:**
Fortinet / FortiSIEM.

**Pregunta 8:**
Indicar si requieren servicio de Threat Intelligence.

**Respuesta 8:**
Sí, es requerido el servicio de Inteligencia de Amenazas (Threat Intelligence), ver especificaciones técnicas en su numeral 4.

**Pregunta 9:**
Indicar paquetes de Casos de Uso requeridos.

**Respuesta 9:**
**Los casos de uso son los siguientes:**
a. Creación, eliminación y modificación de objetos en el Directorio Activo.
b. Delegación de permisos en el Active Directory.

22 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.

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.

**Ver enmienda.**

**Pregunta 10:**
¿Cuántos ataques conocen que les hayan realizado por phishing o malware? Tienen alguna estadística anual?

**Respuesta 10:**
Durante el último año fueron registradas **529** amenazas de phishing.

**Pregunta 11:**
Suministrar lista de dominios y subdominios oficiales:

**Respuesta 11:**
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
ix. observatoriojusticiaygenero.poderjudicial.gob.do
x. sistemadegestiondecasos.poderjudicial.gob.do

22 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 12:**
Suministrar lista de marcas comerciales (propias de la FGS)

**Respuesta 12:**
En la siguiente tabla encontrara las marcas propias del proceso de monitoreo.

| Marca | Modelo | Cantidad |
|---|---|---|
| UTM - Fortigate | 1100E | 2 |
| UTM - Fortigate | 500E | 2 |
| UTM - Fortigate | 300E | 1 |
| Servidor - DELL | XC730XD | 4 |
| Servidor - HP | ProLiant DL380 Gen10 | 6 |
| Máquinas virtuales | HYPER - V | 85 |
| Total general | | 100 |

**Pregunta 13:**
Suministrar Aplicaciones móviles: (cantidad y enlaces de descarga por plataforma)

**Respuesta 13:**
En este momento no contamos con aplicaciones móviles.

**Pregunta 14:**
Suministrar Nº de redes sociales y nombre: (p.ej. Facebook, Twitter, etc correspondientes a la FGS)

**Respuesta 14:**

| No. | Red social | Nombre |
|---|---|---|
| 1 | Facebook | @PoderJudicialRD |
| 2 | Twitter | @poderjudicialrd |
| 3 | Instagram | @PoderJudicialRD |
| 4 | Youtube | PoderJudicialRD |
| 5 | Flickr | PoderJudicialRD |

**Pregunta 15:**
Mencionar los países donde opera:

**Respuesta 15:**
República Dominicana.

22 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 16:**
¿Estarían interesados en el Monitoreo de perfiles VIP (VPs, gerentes, directores, etc)?

**Respuesta 16:**
En las especificaciones técnicas contemplamos el robo de credenciales y la fuga de datos en la Deep Web. Sin embargo, no estamos requiriendo el monitoreo de perfiles VIP de manera particular.

**Pregunta 17:**
Enlistar los Bienes a monitorear (en caso de requerir)

**Respuesta 17:**
No nos queda clara su pregunta.

**Pregunta 18:**
¿Qué herramientas de seguridad tienen?

**Respuesta 18:**
En las especificaciones técnicas, en su numeral 6 citamos: Tomar en consideración que el Poder Judicial cuenta con su propia infraestructura SIEM, Directorio Activo, antivirus, cifrado y cortafuegos.

**Pregunta 19:**
¿Qué SIEM tienen?

**Respuesta 19:**
Fortinet / FortiSIEM.

**Pregunta 20:**
¿Su SIEM tiene funcionalidades de SOAR o XDR?

**Respuesta 20:**
No, no posee funcionalidades de SOAR o XDR.

22 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 21:**
¿Cuál es la ingesta de GB al día?

**Respuesta 21:**
Actualmente la solución SIEM esta en proceso de implementación por lo que no es posible brindarle esta información.

**Pregunta 22:**
¿Qué versión y antivirus tienen?

**Respuesta 22:**
TrendMicro - Apex One.

**Pregunta 23:**
¿Qué firewall posee la institución?

**Respuesta 23:**

| Marca | Modelo | Cantidad |
|---|---|---|
| UTM - Fortigate | 1100E | 2 |
| UTM - Fortigate | 500E | 2 |
| UTM - Fortigate | 300E | 1 |

**Pregunta 24:**
¿Poseen EDR?

**Respuesta 24:**
No, no poseemos EDR.

**Pregunta 25:**
¿En cuanto a Ciberinteligencia en la dark web necesitaran monitorear usuarios en especificos?

**Respuesta 25:**
Todos los usuarios del dominio @poderjudicial.gob.do.

**Pregunta 26:**
¿Qué cantidad de usuario con este requerimiento de monitoreo en la darkweb ?

**Respuesta 26:**
Todos los usuarios del dominio @poderjudicial.gob.do. Aproximadamente 6,000.

22 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 27:**
**Acápite 25: Condiciones de Pagos.**
**La forma de pago puede ser** bajo modalidad de renta mensual, donde se cargue un costo inicial de instalación y el resto en pagos mensuales. Si esto es factible, podemos hacerlo con opciones de 24 meses, o de 12 meses?

**Respuesta 27:**
Los términos de referencia en el numeral 25 especifican que la "***Forma de pago propuesta es del 100%, a crédito de treinta (30) días, luego de emitida la certificación de recepción conforme por parte de la Dirección de Tecnologías de la Información y la Comunicación".***

**Pregunta 28:**
**Acápite 7.1.6 Especificaciones Técnicas:**

- ¿Poder Judicial tiene contemplado el proceso para integración entre SOC y su infraestructura? (Accesos y credenciales plataforma de monitoreo SIEM)
- ¿Marca o tipo de Directorio Activo, antivirus, cifrado y cortafuegos?
- ¿Poder Judicial tiene definido matriz de seguimiento y escalamiento para validar los soportes con respectos a los incidentes generados por el SIEM)?

**Respuesta 28:**

a) El Poder Judicial tienen contemplada la configuración de enlaces VPN para establecer la comunicación segura entre el SOC y nuestra infraestructura, también serán entregados los niveles de acceso y credenciales necesarias.
b) Actualmente utilizamos Microsoft Active Directory, en sus versiones en premisa y en la nube (Azure). Nuestros cortafuegos son de la marca Fortinet y la solución de protección de puntos finales es de Trend Micro.
c) La matriz de escalamiento de incidentes será suministrada durante el proceso de implementación al oferente que resulte adjudicatario.

**Pregunta 29:**
Los servicios web publicados en la nube, que tecnología utilizan? (apache, IIS, algún proveedor de hospedaje?)

**Respuesta 29:**
Los servicios web publicados se encuentran alojados en nuestra nube híbrida mediante la tecnología de IIS.

22 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 30:**
Características de los 100 dispositivos alojados en nube hibrida

**Respuesta 30:**

| Marca | Modelo | Cantidad |
|---|---|---|
| UTM - Fortigate | 1100E | 2 |
| UTM - Fortigate | 500E | 2 |
| UTM - Fortigate | 300E | 1 |
| Servidor web | Virtualizados | 15 |
| Servidor de aplicaciones | Virtualizados | 35 |
| Servidor de base de datos | Virtualizados | 25 |
| Servidor de dominio | Virtualizados | 10 |
| Servidor - DELL | XC730XD | 4 |
| Servidor - HP | ProLiant DL380 Gen10 | 6 |
| Total general | | 100 |

**Pregunta 31:**
¿Los 100 dispositivos alojados en la nube está enviando datos de logs o tienen integración con el SIEM?

**Respuesta 31:**
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.

**Pregunta 32:**
¿Que tecnología SIEM poseen?

**Respuesta 32:**
Fortinet / FortiSIEM.

22 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 33:**
¿El SIEM con el que cuentan esta siendo utilizado en producción, tienen analistas?, tienen procesos definidos para la gestión de incidentes?

**Respuesta 33:**
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 34:**
¿Los servicios de SOC lo deberíamos hacer administrando el SIEM que poseen?

**Respuesta 34:**
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 35:**
¿Cantidad de firewalls que poseen?

**Respuesta 35:**
Cinco (5) firewalls a monitorear.

**Pregunta 36:**
¿Cantidad de consolas de Antivirus que poseen?

**Respuesta 36:**
Poseemos una consola de antivirus.

**Pregunta 37:**
¿Cantidad de dominios de AD que poseen?

**Respuesta 37:**
Un (1) dominio de Active Directory.

**Pregunta 38:**
¿Posee un proceso de Monitoreo de Seguridad?

**Respuesta 38:**
Los procesos de Monitoreo de Seguridad se encuentran en proceso de documentación.

22 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 39:**
¿Posee proceso de Gestión de Incidentes? En base a que normativa o marco de trabajo esta desarrollado?

**Respuesta 39:**
El proceso de Respuesta a Incidentes cibernéticos está en proceso de documentación.

**Pregunta 40:**
¿El cliente cuenta con un documento del plan para la respuesta ante incidentes de seguridad de la información?

**Respuesta 40:**
El proceso de Respuesta a Incidentes cibernéticos está en proceso de documentación.

**Pregunta 41:**
¿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 41:**
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 42:**
¿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 42:**
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 á la siguiente tecnología:

- ✓ Virtualización con HyperV y Kubernetes.
- ✓ IIS
- ✓ SQL Server
- ✓ Microsoft Active Directory / Azure AD.

22 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.

- ✓ Fortinet
- ✓ Trend Micro.

**Pregunta 43:**
Por favor indicar para el dimensionamiento, la cantidad promedio mensual de incidentes de seguridad (SOC) que se presentan en la organización

**Respuesta 43:**
La solución SIEM está en proceso de implementación por lo que esta información aún no está disponible.

**Pregunta 44:**
¿Posee la categorización de incidentes de su plataforma, por tipo, plataforma y criticidad?

**Respuesta 44:**
En este momento no contamos con esta información, sin embargo, estará siendo documentada durante el proceso de incorporación del SOC.

**Pregunta 45:**
¿Posee la organización grupos resolutorios para cada uno de los incidentes categorizados en su plataforma?

**Respuesta 45:**
Existen grupos resolutorios para los tipos de incidentes, sin embargo, la plataforma esta en proceso de implementación. Esta información será suministrada durante el proceso de incorporación del SOC.

**Pregunta 46:**
¿Cuenta con matriz de escalamiento clara y detallada para la notificación de eventos en horario 5x8 y 7x24?

**Respuesta 46:**
La matriz de escalamiento de incidentes será suministrada durante el proceso de implementación al oferente que resulte adjudicatario.

22 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 47:**
¿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 47:**
Los procesos de Monitoreo y Respuesta a Incidentes de seguridad se encuentran en proceso de documentación.

**Pregunta 48:**
¿Posee Casos de Uso de Monitoreo definido por sistema o plataforma?

**Respuesta 48:**
**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 49:**
¿cuántos dominios externos (FQDN) desea monitorear y proteger para prevencion de usurpación de identidad via correo y DNS?

**Respuesta 49:**

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

22 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