14 de octubre 2020
DTI-CS-169-2020

Lic. Erick Agüero Vargas
Jefe, Unidad de Compras y Contrataciones
Fundación Omar Dengo

Estimado Lic. Agüero
En respuesta a las aclaraciones solicitadas para el proceso de contratación:

PROCESO DE CONTRATACIÓN 2020PPI-000001-PROV-FOD
"CONTRATACIÓN DE UNA EMPRESA QUE PROVEA EL SERVICIO LLAVE EN MANO, BAJO LA MODALIDAD CONSUMO SEGÚN DEMANDA PARA LA IMPLEMENTACIÓN DE LA RED EDUCATIVA DEL BICENTENARIO EN CENTROS EDUCATIVOS DEL MINISTERIO DE EDUCACIÓN PÚBLICA, UBICADOS EN DIFERENTES ZONAS GEOGRÁFICAS DEL PAÍS.

Me permito indicarle lo siguiente:

Solicitud de aclaraciones SONDA

Aclaración #1:

4. Flujo de la Operación del NOC

Para el Centro de Operaciones de Red en el proyecto de la Red Educativa del Bicentenario al menos debe considerar los siguientes lineamientos de respuesta a monitoreo, colección de datos, contabilidad, planeación de capacidad, disponibilidad SLA's, tendencias, detección de problemas, corrección de problemas, perfeccionamiento, control de cambios y sistema de tiquetes.

Aclaración: Favor aclarar qué se espera por contabilidad, ¿Es solamente indicar la cantidad de casos generados o algo diferente?

Respuesta de la administración

La palabra "contabilidad" no aplica en el contexto del Flujo de Operación el NOC.

Aclaración #2:

6.4 Métricas de Seguimiento
Para la adecuada ejecución de la gestión de Niveles de Servicio es indispensable, implementar, generar y revisar periódicamente las siguientes métricas:

6.4.1. Número de interrupciones del negocio debidas a incidentes en el servicio de TI.
6.4.2 Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados.
6.4.3 Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados.
6.4.4 Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión.
6.4.5 Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información.
6.4.6 Relación o cantidad de decisiones de negocio erróneas en las que la falta de información o la información errónea ha sido la principal causa.
6.4.7 Número de procesos de negocio con acuerdos de servicio sin definir.
6.4.8 Porcentaje de servicio TI activos cubiertos por acuerdos de servicio.
6.4.9 Porcentaje de clientes satisfechos porque el servicio cumple los niveles acordados.
6.4.10 Número y severidad de incumplimientos del servicio.
6.4.11 Porcentaje de servicios monitorizados para cumplir los acuerdos. Porcentaje de servicios que alcanzan su objetivo.

Aclaración: Favor aclarar la fórmula y/o mecanismo esperado para medir cada una de las métricas de la sección 6.4

Respuesta de la administración

Para cada uno de ellos, existe un KPI asignado, favor referirse a ellos para establecer los valores de medición. Los datos de estas mediciones, serán obtenidos de los paneles de administración solicitados en el cartel y del sistema de gestión de incidentes. Para cada incidente generado, se deberá enviar una encuesta de satisfacción del servicio, de forma que se puedan generar las mediciones indicadas en este punto.

Aclaración #3:

Sección 12: Elementos requeridos:

- Monitoreo de la red educativa.
  Se debe contar con una herramienta de monitoreo y personal dedicado a la revisión de red educativa.

Aclaración: ¿Tienen estadísticas de casos de monitoreo actual y casos que hay que atender en sitio por cada zona? Esto para poder proyectar el uso de recursos dedicados.

Respuesta de la administración

Se le indica al posible oferente, que la administración no cuenta con estadística como la requerida dado que es un servicio nuevo en sus características, y los servicios actuales no cuentan con esa trazabilidad.

Aclaración #4:

2.4 Requerimientos de los ingenieros del NOC Nivel 2

2.4.1 Formación

2.4.1.1 Grado de Licenciatura o Maestría en Ingeniería Telemática, Eléctrica, Electrónica para lo cual deberá presentar copia del título que lo acredite. b. Conocimientos técnicos en redes de telecomunicaciones.

Cambio:

Solicitar si para el grado académico se puede dejar como Grado mínimo de Bachillerato en Informática o Computación

Respuesta de la administración

Este requerimiento ya ha sido actualizado en previos oficios del presente proceso licitatorio. Favor referirse a esta documentación.

Aclaración #5:

E. Requerimientos del Componente de Centro de Seguridad de la red SOC

Como parte de los requerimientos, se deben considerar los recursos y actividades para la protección de los activos del Ministerio de Educación Pública y reducir la probabilidad y el impacto de riesgos de seguridad contra las plataformas tecnológicas de los más de 2139 nodos en los Centros Educativos del MEP.

Pregunta: Solicitamos a la entidad por favor aclarar a qué tipo de recursos y actividades se refieren, si son de gestión, de mantenimiento, de soporte o todas las anteriores.

Respuesta de la administración

Se aclara que el punto hace referencia todos los recursos requeridos, sean humanos o técnicos que sean requeridos para brindar el servicio y asegurar la red. Es responsabilidad del oferente garantizar la seguridad de la red, de los estudiantes y de la información dentro de esta.

Aclaración #4:

4.1. Defensa Perimetral

En el perímetro pueden existir diferentes tecnologías que se pueden utilizar. El perímetro es donde su organización pone en alto y detiene el control y la administración de los proveedores de servicios, socios comerciales o de conexiones no confiables. El propósito de la defensa perimetral es evitar el ingreso no autorizado a la red tanto como sea posible y detectar todo lo que pueda si no puede detenerse específicamente.

Pregunta: Para poder calcular los equipos de defensa perimetral es necesario conocer el troughpunt y cantidad de conexiones simultáneas por cada sede.

Pregunta: Por favor aclarar si los equipos de defensa perimetral son puestos por el cliente o por el servicio de SOC.

Respuesta de la administración

Tal cual se indica en la Sección VI punto A.3.2, se establece un periodo de monitoreo durante el cual se determinará la utilización de los servicios de forma que se puedan establecer parámetos como los solicitados

(ancho de banda requerido, utilización de los enlaces, cantidad de conexiones, thruput, etc). Al ser este un servicio nuevo, no se cuenta con esta estadística.

Todos los equipos para brindar los servicios requeridos en este cartel, son responsabilidad del oferente.

Aclaración #5:

4.1. Defensa de Red:

Observación: En nuestro entender los equipos de defensa de red ya existen sobre la red y lo que se requiere es que monitoreemos esos equipos desde el SOC, Por favor confirmar si nuestro entender es correcto

Respuesta de la administración

Se aclara que es responsabilidad del oferente, asegurar que la oferta incluya todos los equipos necesarios para brindar los servicios requeridos en el cartel. No es correcto asumir que existen equipos previos instalados en los centros educativos.

Aclaración #6:

4.3. SIEM y Log Management

Pregunta: Cuanto es el tiempo de retención de logs. En frio y en caliente.
Con la intención de tener datos históricos y estadísticos, se solicita almacenar la información del SIEM al menos por 5 años. Todos los eventos de la WAN deben ser contemplados en esta solución.

Respuesta de la administración

Se aclara que, para lo referente a los Logs de los equipos, estos deberán de mantenerse disponibles por 3 meses en caliente, pasado este tiempo, se deberán mover a una ubicación segura y accesible a la administración por un tiempo no menor a 1 año.

Los datos de incidentes de soporte y atención de usuarios, deberán mantenerse almacenados y accesibles a la administración por un tiempo no menor a 5 años.

Aclaración #7:

5.4. Gestión de Parches y Vulnerabilidades

Solicitud: Para poder dimensionar el esfuerzo se debe saber la cantidad de dispositivos objeto de este ejercicio y la periodicidad de la ejecución de los ejercicios.

Respuesta de la administración

Se aclara que la cantidad de dispositivos a monitorear será aquella que el oferente indique en su oferta. No se debe monitorear ni serán parte de este proceso, los equipos instalados en la LAN. En caso de que el despliegue de un parche para atender una vulnerabilidad requiera de instalación en los equipos de usuario final, esto deberá ser informado a la administración para coordinar los esfuerzos requeridos.

La gestión de parches y vulnerabilidades es un proceso de monitoreo diario propio del SOC y no obedece a un calendario programado con anterioridad, sino a la necesidad de mantener la red segura. El SOC debe monitorear constantemente los equipos y la red de forma que pueda determinar posibles amenazas y de forma proactiva, indicar a la administración del riesgo y su respectiva mitigación.

Aclaración #8:

5.5.8. Realizar Implementación Automatizada de Parches:

Pregunta: Se requiere saber los sistemas operativos de los servidores de la red para conocer que elemento de automatización de gestión de parches que se debe integrar al servicio.

Respuesta de la administración

Se aclara que los sistemas operativos de los servidores son responsabilidad del oferente y del diseño que vaya a aplicar para responder a los requerimientos del cartel.

Aclaración #9:

C. Organización del SOC
1. Descripción general del servicio

El oferente debe entregar al órgano fiscalizador, los procedimientos detallados de reporte de vulnerabilidades, atención de problemas y cualquier otro procedimiento de operación del SOC.

Observación: Bajo nuestro modelo de Gestión de seguridad, la información de los procedimientos del SOC es información confidencial la cual no puede ser compartida con terceros, ya que se corre el riesgo que sea luego utilizada para implementar SOC propios, y además porque en esos procedimientos se consigna el conocimiento adquirido por SONDA para ejercer este tipo de servicios, por lo que no es posible entregar procedimientos detallados, se podrán entregar procedimientos de alto nivel de la operación del SOC pero no detallados.

Pregunta: ¿El servicio de SOC se ofrece de forma remota para todos los clientes con recursos compartidos, por lo que queremos aclarar si bajo este esquema estaríamos en cumplimiento de la organización del SOC?

Respuesta de la administración

Se aclara que el requerimiento del cartel en este punto, este tener claro cuáles serán los procesos de trabajo del SOC con respecto a la red objeto de este cartel. No se solicita información confidencial de operación de la organización, pero se debe tener claro cómo operará el SOC y cómo velará por la seguridad de la red. El

procedimiento deberá ser lo suficientemente detallado para atender el punto sin revelar información que el oferente estime como confidencial. Estos procedimientos serán evaluados por la administración para determinar el cumplimiento del punto y el oferente se compromete a modificarlos para atender el requerimiento del cartel a satisfacción de la administración.

El servicio de SOC puede ser un servicio compartido, en el tanto se cumplan los requerimientos del cartel y se garantice el cumplimiento de los SLAs solicitados en el cartel. Tal cual se solicita, el oferente debe estar en capacidad de estimar el costo de este servicio por centro educativo y detallarlo en su oferta.

Aclaración #10:

11.5 Tiempos de atención y resolución

Pregunta: ¿Las horas de resolución de los incidentes que se atienden en horario 12x6 son horas que también serán contabilizadas sobre el mismo horario? Es decir, si una incidencia alta que se reportó el sábado a las 11pm, la cual tiene 8 horas de resolución, se debería resolver el domingo o se esperaría hasta el lunes que vuelve a empezar el horario del servicio.

Respuesta de la administración

Tal cual se indica en el cartel, los tiempos de atención han sido previamente definidos. Aunque el monitore de la solución deberá ser constante, se entiende que el horario de atención en sitio será únicamente en días hábiles de acuerdo a los horarios indicados en el cartel.

Sin más por el momento, quedo atento

Saludos

MINOR ALFARO CUBERO (FIRMA)

Digitally signed by MINOR ALFARO CUBERO (FIRMA)
Date: 2020.10.14 08:00:00 -06'00'

Ing. Minor Alfaro Cubero
Director de Tecnología
Fundación Omar Dengo