

BOLETÍN DE ACLARACIONES NRO. 2

SOLUCIÓN DE DETECCIÓN Y RESPUESTA DE AMENAZAS DE CIBERSEGURIDAD

CÓDIGO: EC-L1253-P00075

PREGUNTA 2.-

El punto 31 de GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD debe ser eliminado, ya que no fue parte del estudio de mercado previo y está enfocado en un aplicativo móvil de un fabricante en específico. **Adicionalmente, en el archivo Excel que se revisó en febrero de este año no existía este ítem en el documento.**

RESPUESTA 2.-

Estimado oferente por favor refiérase a la enmienda 1 del Boletín de Enmiendas Nro. 1

PREGUNTA 3.-

Solicitamos que el punto 31 del apartado GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD sea opcional, ya que le mismo solicita una aplicación móvil la cual solo se puede cumplir incluyendo el FortiSOAR Mobile Application, el cual es del fabricante Fortinet, marca que nosotros no comercializamos.

RESPUESTA 3.-

Estimado oferente por favor refiérase a la enmienda 1 del Boletín de Enmiendas Nro. 1

PREGUNTA 4.-

Respecto del requerimiento que establece que la aplicación móvil y el portal web deben permitir la visualización de la categorización de incidentes por técnicas y tácticas de MITRE ATT&CK, así como indicadores de ROSI —retorno de la inversión en seguridad—, solicitamos respetuosamente a la Entidad considerar estas funcionalidades como opcionales o deseables, y no como requisitos obligatorios de cumplimiento. Esto debido a que la información de MITRE ATT&CK puede ser proporcionada por la plataforma SIEM contemplada en el proyecto, mientras que el cálculo de ROSI depende de metodologías y variables financieras propias de cada organización. Mantener ambos puntos como obligatorios podría limitar la participación de oferentes o direccionar el proceso hacia fabricantes específicos.

RESPUESTA 4.-

Estimado oferente por favor refiérase a la enmienda 1 del Boletín de Enmiendas Nro. 1

PREGUNTA 27.-

Respecto de lo solicitado en el apartado Sección VIII. Condiciones Especiales de Contrato (CEC) - CGC 29.5 - ACUERDO DE NIVEL DE SERVICIO – 4. La tabla a continuación establece

los niveles de prioridad del ACUERDO DE NIVEL DE SERVICIO. Estos niveles, en cantidad y definición, pueden ser modificados durante la ejecución del contrato previa notificación por parte del Administrador de Contrato.”, el pliego permite modificar los niveles de prioridad en cantidad y definición durante la ejecución, mediante notificación del administrador del contrato. **Se solicita al SRI considerar que, si una modificación amplía el alcance o endurezca los umbrales, se debería tramitar como control de cambios con revisión económica, por modificar el alcance.**

RESPUESTA 27.-

Estimado oferente por favor refiérase a las enmiendas 2 y 3 del Boletín de Enmiendas Nro. 1

PREGUNTA 35.-

En el documento de licitación Sección VI "Requisitos de los Bienes y Servicios Conexos"(Lista de Servicios Conexos), el Ítem 7 aparece identificado como "Implementación y transferencia de conocimientos" con cantidad 1, lo que sugiere que debe ser cotizado con un valor económico. Sin embargo, en la Sección VIII "Condiciones Especiales del Contrato", en la tabla de precios CGC 16.1, se incluye la siguiente nota: "Los costos asociados a la transferencia de conocimiento deberán entenderse como parte de los costos indirectos incluidos en la oferta global de los servicios. Por lo tanto, no deberán ser cotizados de forma separada ni desglosada." Se solicita aclarar esta aparente contradicción: ¿el Ítem 7 de la tabla de precios debe cotizarse con un valor global que incluya tanto la implementación como la transferencia de conocimiento? ¿O la transferencia de conocimiento no tiene valor económico propio y el Ítem 7 corresponde únicamente al servicio de implementación? Una definición clara es necesaria para garantizar que todos los oferentes presenten sus precios bajo las mismas condiciones y la evaluación económica sea comparable

RESPUESTA 35.-

Estimado Oferente, el Ítem 7 debe ser considerado como un único servicio integral, cuyo valor económico corresponde al de la implementación, mientras que la transferencia de conocimientos se entiende incluida en dicho servicio y no constituye un rubro independiente de cotización.

Adicionalmente, estimado oferente por favor refiérase a la enmienda 4 del Boletín de Enmiendas Nro. 1

PREGUNTA 38.-

En el documento de licitación Sección IX "Formularios del Contrato", en la tabla de precios (CGC 16.1), los Ítems 1 al 5 (componentes de software: EDR, NDR, Gestión de amenazas de identidad, Inteligencia unificada de ciberdefensa y Respuesta unificada de ciberdefensa)

tiene asignada la cantidad "3" en la columna de cantidad. La Sección VI establece que el licenciamiento de cada componente tiene una vigencia de 3 años (1.092 días), pero es entregado como un único lote. Se solicita aclarar el significado de la cantidad "3" en la tablade precios: ¿corresponde a los 3 años de vigencia del licenciamiento, de modo que el precio unitario debe cotizarse como el costo anual por cada componente de software y el valor total corresponde a los 3 años? ¿O existe otra interpretación para esta cantidad? Esta aclaración es esencial para que todos los oferentes estructuren sus precios de manera uniforme y la evaluación económica sea consistente y comparable.

RESPUESTA 38.-

Estimado oferente por favor refiérase a la enmienda 4 del Boletín de Enmiendas Nro. 1

PREGUNTA 39.-

En la página 143.- ACUERDO DE NIVEL DE SERVICIO se indica que los niveles en cantidad y definición pueden ser modificados durante la ejecución del contrato previa notificación por parte del Administrador del Contrato. Considerando que los planes de soporte se basan en tiempo de respuesta y solución, es de nuestro entendimiento que dicha modificación será aceptada en mutuo acuerdo. Confirmar si es correcto nuestro entendimiento.

RESPUESTA 39.-

Estimado oferente por favor refiérase a las enmiendas 2 y 3 del Boletín de Enmiendas Nro. 1

PREGUNTA 101.-

En el documento "DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios", sección "BIENES REQUERIDOS" componente "RESPUESTA UNIFICADA DE CIBERDEFENSA" en el numeral 148 se solicita. "La función central de respuesta unificada de ciberdefensa debe incluir un tablero ("dashboard") que muestre el tiempo ahorrado por la ejecución automática de playbooks proveyendo así una métrica clara sobre el retorno de la inversión (ROI) de la automatización"

Según nuestro entendimiento por tiempo ahorrado, al no existir un parámetro que determine cuanto debe tomar la respuesta a un incidente ya que esto a su vez depende del tipo de incidente, se admitirá que se incluya en la plataforma el tiempo consumido y el tiempo ahorrado sea parte de los reportes periódicos entregados. Por favor indicar si es

correcto nuestro entendimiento o aclarar.

RESPUESTA 101.-

Estimado oferente por favor refiérase a la enmienda 5 del Boletín de Enmiendas Nro. 1

PREGUNTA 108.-

En la sección VIII. Condiciones Especiales de Contrato (CEC), CGC 16.1, tabla de precios, páginas 189 y 190, los ítems 1 al 5, correspondientes a los componentes de software Endpoint Detection and Response (EDR), Network Detection and Response (NDR), Gestión de amenazas de identidad, Inteligencia unificada de ciberdefensa y Respuesta unificada de ciberdefensa, tienen asignada la cantidad “3” en la columna CANTIDAD. Sin embargo, en la sección V. Formularios de la Oferta, formulario PRECIO Y CRONOGRAMA DE CUMPLIMIENTO: SERVICIOS / SERVICIOS CONEXOS, páginas 85 y 86, que es el formulario que el oferente debe completar y suscribir, los mismos ítems 1 al 5 tienen asignada la cantidad “1” con la indicación “Vigencia de 3 años”; e igual cantidad “1” consta en la sección VI. Requisitos de los Bienes y Servicios Conexos, subsección 1. LISTA DE SERVICIOS Y CRONOGRAMA DE ENTREGAS, páginas 99 a 101. La sección VI establece que el licenciamiento de cada componente tiene una vigencia de tres (3) años, equivalente a 1.092 días, y que es entregado como un único lote. La discrepancia entre la cantidad consignada en el formulario de oferta y la consignada en la tabla de precios del contrato implica que un mismo precio unitario produciría dos valores totales distintos según el documento que se aplique, con una diferencia de tres veces el valor ofertado. Se solicita aclarar el significado de la cantidad “3” en la tabla de precios de la CGC 16.1: ¿corresponde a los tres años de vigencia del licenciamiento, de modo que el precio unitario debe cotizarse como el costo anual por cada componente de software y el valor total corresponde a los tres años? ¿O existe otra interpretación para esta cantidad? ¿Se emitirá la enmienda que armonice la cantidad consignada en el formulario de la sección V y en la subsección 1 de la sección VI con la de la tabla de precios de la CGC 16?1? Esta aclaración es esencial para que todos los oferentes estructuren sus precios de manera uniforme y para que la evaluación económica sea consistente y comparable.

RESPUESTA 108.-

Estimado oferente por favor refiérase a la enmienda 4 del Boletín de Enmiendas Nro. 1

PREGUNTA 119.-

Contratos en ejecución

Solicitamos confirmar si se aceptará experiencia proveniente de contratos actualmente en ejecución cuando existan actas parciales, certificados de cumplimiento o documentos emitidos por el cliente que acrediten el monto efectivamente ejecutado y recibido.

RESPUESTA 119.-

Estimado oferente por favor refiérase a la enmienda 6 del Boletín de Enmiendas Nro. 1

PREGUNTA 127.-

Modificación unilateral de niveles de prioridad

El SRI puede modificar la cantidad y definición de los niveles de prioridad mediante

notificación del administrador.

Solicitamos confirmar que cualquier modificación de los niveles de prioridad o del SLA deberá contar con aceptación de ambas partes y que no podrá incrementar las obligaciones, recursos o costos del contratista sin el correspondiente instrumento modificatorio.

RESPUESTA 127.-

Estimado oferente por favor refiérase a las enmiendas 2 y 3 del Boletín de Enmiendas Nro. 1

PREGUNTA 135.-

Estimada entidad referente al punto: La función NDR debe permitir realizar una captura de paquetes en tiempo real para ejecutar un análisis exhaustivo de los incidentes detectados en el momento del suceso. La captura debe poderse exportar para ser analizada por otras herramientas en al menos uno de los siguientes formatos: PCAP ("Packet Capture"), JSON o CVE. Por favor confirmar que existe un error de tipeo y que el formato CVE que se solicita más bien se refiere a un formato CSV, ya que CVE no es un formato válido para capturas.

RESPUESTA 135.-

Estimado oferente por favor refiérase a la enmienda 8 del Boletín de Enmiendas Nro. 1

PREGUNTA 143.-

Estimada entidad referente al punto: El servicio debe proveer una aplicación móvil compatible, que soporte iOS y Android y un portal web, de forma que a través de ambos el personal del SRI pueda visualizar la siguiente información: Visualización de indicadores de ROSI (retorno de la inversión sobre la seguridad) en un tiempo específico. Por favor confirmar qué fórmula, variables, costos base y periodo utilizará el SRI para calcular y aceptar los indicadores de retorno de la inversión en seguridad (ROSI)

RESPUESTA 143.-

Estimado oferente por favor refiérase a la enmienda 1 del Boletín de Enmiendas Nro. 1

PREGUNTA 156.-

Estimada entidad, en el punto 9.f de la etapa de transición, en el punto IMPLEMENTACION, se indica que habrá otras actividades que el SRI requiera incluir en esta etapa. Dado que el periodo de implementación es de 90 días, como se manejará el alcance y tiempos de estas actividades adicionales que no están dimensionadas en lo económico ni el tiempo para que el contratista sea sancionado al no cumplir los tiempos estipulados. Por favor acotar que tipo de actividades serán y como se manejará el tiempo adicional requerido para realizarlas.

RESPUESTA 156.-

Estimado oferente por favor refiérase a la enmienda 9 del Boletín de Enmiendas Nro. 1

PREGUNTA 172.-

Estimada Entidad, confirmar si para la validación de cumplimiento del punto PRODUCTOS Y SERVICIOS ESPERADOS, requieren la presentación de documentos técnicos o certificados de los fabricantes de los equipos con los que se brindará el servicio, para así justificar el cumplimiento de las especificaciones técnicas; o solo con que pongamos como oferentes que, , si cumplimos con el servicio, sin ninguna referencia o certificado será aceptado.

RESPUESTA 172.-

Estimado oferente:

De conformidad con lo establecido en la Sección II. Datos de la Licitación (DDL), apartado C. Preparación de las Ofertas, desde la página 45, se detallan los requisitos, documentos y condiciones que deben ser considerados para la presentación de la oferta.

En este sentido, el oferente deberá presentar su propuesta conforme a la documentación solicitada en la Solicitud de Ofertas (SDO) del proceso, incluyendo la información técnica que permita verificar el cumplimiento de las especificaciones.

Adicional, por favor refiérase a la enmienda 7 del Boletín de Enmiendas Nro. 1

PREGUNTA 199.-

Estimada entidad, en el apartado IAO 12.1(j), en el ítem Documentación técnica de sustento solicitan: La documentación que corresponda a fichas técnicas, hojas de especificación, catálogos, manuales o similares de los ítems ofertados debe tener resaltadas las secciones que permiten verificar su cumplimiento de las especificaciones técnicas.... Entendemos que la documentación de sustento técnico se puede presentar en formato digital y no es necesario presentar de forma impresa. Por favor confirmar

RESPUESTA 199.-

Estimado oferente por favor refiérase a la enmienda 10 del Boletín de Enmiendas Nro. 1

PREGUNTA 210.-

Estimada entidad respecto al punto: El servicio debe proveer una aplicación móvil compatible, que soporte iOS y Android y un portal web, de forma que a través de ambos el personal del SRI pueda visualizar la siguiente información: Cantidad de casos abiertos, Cantidad de incidente atendidos en un periodo de tiempo, Priorización de los incidentes,

Categorización de los incidentes por tipo de técnica y táctica según el MITRE ATT&CK, Acceso cercano con los ingenieros especialista asignado a los casos. Visualización del estatus de los incidentes (cerrados, pendiente, resueltos). Visualización de indicadores de ROSI (retorno de la inversión sobre la seguridad) en un tiempo específico. Estimada entidad, entendiendo que el cálculo de los indicadores ROSI depende de metodologías e indicadores financieros propios de la institución, y que la categorización de incidentes según MITRE ATT&CK puede ser proporcionada por la plataforma SIEM incluida en el proyecto, solicitamos que estas características solicitadas sean opcionales.

RESPUESTA 210.-

Estimado oferente por favor refiérase a la enmienda 1 del Boletín de Enmiendas Nro. 1