

BOLETÍN DE ACLARACIONES NRO. 1

SOLUCIÓN DE DETECCIÓN Y RESPUESTA DE AMENAZAS DE CIBERSEGURIDAD

CÓDIGO: EC-L1253-P00075

PREGUNTA 1.-

El punto 55 y 56 de ANALISIS SANDBOX: los dos cambios eliminan la cantidad de archivos al año o al mes a ser analizados; este es un parámetro importante para el dimensionamiento, caso contrario podríamos como fabricantes colocar un número pequeño de archivos a analizar, que no cumplirían las expectativas o necesidades de la institución. **Adicionalmente, en el archivo Excel que se revisó en febrero de este año se propuso que el texto cambiase a lo siguiente:** “El servicio de sandbox debe permitir el análisis bajo demanda de 100 archivos al mes. Cada archivo para analizar puede ser de hasta 100 MB de tamaño.”, **y no se indicó que se agregaría el texto que ahora aparece en el ítem 56.**

RESPUESTA 1.-

Estimado oferente, los requisitos establecidos en los numerales 55 y 56 ANÁLISIS SANDBOX de la Sección VI. Requisitos de los Bienes y Servicios Conexos, tienen como finalidad definir las capacidades funcionales mínimas que deberá proporcionar la solución de sandbox, diferenciando dos escenarios de uso:

- **Numeral 55:** análisis automático de archivos provenientes de los componentes tecnológicos que formen parte de la solución ofertada y que hagan uso de la funcionalidad de sandbox.
- **Numeral 56:** análisis bajo demanda de archivos cargados manualmente por personal del SRI o del servicio.

No es posible incluir una cantidad específica de archivos por mes o por año que deben ser analizados por el sandbox, esto con el propósito de no restringir la participación de oferentes mediante un dimensionamiento particular que podría estar asociado a una tecnología o modelo comercial específico.

En consecuencia, la solución ofertada deberá incluir todos los recursos, licencias, suscripciones y capacidades necesarias para soportar adecuadamente la operación de la institución respecto de las funcionalidades descritas en los numerales 55 y 56, sin limitaciones que afecten su uso normal.

Por tanto, se mantiene el texto establecido en los numerales 55 y 56 de la Solicitud de Ofertas (SDO).

PREGUNTA 5.-

En observancia de los principios de concurrencia, participación, igualdad de oportunidades y obtención de las mejores condiciones técnicas para la Entidad, se solicita respetuosamente al SRI evaluar la **ampliación del plazo para la presentación de ofertas**

por un período adicional de al menos quince (15) días calendario, contado a partir de la fecha actualmente establecida para su entrega.

RESPUESTA 5.-

Estimado oferente,
No es posible acoger su requerimiento.

PREGUNTA 6.-

Respecto de lo solicitado en el apartado “Calificación del Oferente (IAO 39) - Criterios de Calificación (IAO 39.1) – b) Experiencia Específica”, se solicita considerar como experiencia válida las Actas de Entrega Recepción Parcial correspondientes a contratos de ejecución plurianual, siempre que dichas actas evidencien el cumplimiento de al menos el 90% del valor económico contractual. Esta solicitud se fundamenta en que los contratos relacionados con la experiencia requerida en el presente proceso suelen tener una duración de tres (3) años o más, por lo que, durante su vigencia, las Actas de Entrega Recepción Parcial constituyen documentos fehacientes que acreditan la ejecución efectiva de las obligaciones contractuales y el cumplimiento sustancial del contrato por parte del proveedor. **En tal virtud, se solicita que dichas actas sean aceptadas como medio de verificación de la experiencia específica requerida para efectos de la calificación de los oferentes.**

RESPUESTA 6.-

Estimado oferente, no se acepta su requerimiento.

PREGUNTAS 7.-

Respecto de lo establecido en el literal “CGC 17.1 FORMA Y CONDICIONES DE PAGO – 1. Licenciamiento e Implementación”, se solicita considera la reformulación de la modalidad de pago, estableciendo de manera diferenciada los componentes de licenciamiento e implementación, dado que las licencias deben ser adquiridas y canceladas al fabricante contra entrega para su correspondiente activación a nombre del Servicio de Rentas Internas (SRI). Mantener la estructura actual de pagos implicaría asumir costos financieros adicionales durante el período de implementación, definido en 90 días. **En este sentido, se solicita considerar el pago correspondiente al licenciamiento contra entrega de las licencias y previo al inicio de la etapa de implementación.**

RESPUESTA 7.-

Estimado oferente,

No se acepta su solicitud, el pago se realizará según lo que se encuentra estipulado en CGC 17.1 FORMA Y CONDICIONES DE PAGO de la Sección VIII. Condiciones Especiales de Contrato (CEC).

PREGUNTA 8.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE - NETWORK DETECTION AND RESPONSE (NDR) - 27. La función NDR debe desplegarse en los dos centros de cómputo del SRI (“on-premise”), mediante la instalación de equipos de propósito específico.”. Un NDR de propósito específico es una plataforma dedicada al análisis pasivo del tráfico de red, que opera normalmente fuera de banda mediante TAP o SPAN para detectar e investigar amenazas sin afectar el flujo del tráfico. Su capacidad de detección se basa en analítica avanzada (IA, Machine Learning, análisis de comportamiento y detección de anomalías) y, cuando ejecuta acciones de respuesta, normalmente lo hace mediante la integración con otras plataformas de seguridad, como firewalls, EDR/XDR, agentes de punto final o SOAR. El numeral 26 del pliego establece expresamente que: *“La función NDR puede operar en modo SaaS (“Software-as-a-Service”) o localmente (“on-premises”)”*. Por lo tanto, el propio pliego reconoce que la función NDR puede implementarse mediante una arquitectura distribuida, donde la analítica no necesariamente reside en el equipo instalado en sitio. En este contexto, se solicita confirmar que el requisito se considerará cumplido siempre que el oferente implemente en ambos centros de cómputo equipos físicos dedicados para la captura, inspección profunda y generación de telemetría enriquecida del tráfico de red, pudiendo hacerlo mediante un sensor Next Generation Firewall (NGFW) del mismo fabricante de toda solución a proponer, desplegado de forma pasiva mediante TAP o SPAN, cuya única función dentro de la arquitectura a proponer es la adquisición e inspección profunda del tráfico de red. El sensor NGFW realizará la identificación de aplicaciones (App-ID), la inspección de amenazas (Threat Prevention), el análisis de malware (WildFire), la inspección DNS (DNS Security), el descifrado SSL (cuando corresponda) y la generación de telemetría enriquecida, sin intervenir en el flujo de producción; posteriormente, los componentes de inteligencia y respuesta unificada (a proponer) operando bajo el modelo SaaS permitido por el numeral 26, consumirán dicha telemetría para ejecutar las funciones analíticas propias de un NDR, incluyendo analítica basada en IA y Machine Learning, detección de anomalías, correlación de eventos, análisis de comportamiento (UEBA), detección de movimiento lateral y respuesta automatizada. **Por favor, se solicita al SRI confirmar la aceptación de la arquitectura de seguridad propuesta, en concordancia con el modelo de operación expresamente permitido en el pliego.**

RESPUESTA 8.-

Estimado oferente, no se acepta la solicitud planteada.

Si bien el numeral 26 establece que la función NDR puede operar bajo un esquema SaaS ("Software as a Service") o local ("on-premises"), este requisito debe interpretarse de manera integral con el numeral 27, el cual establece expresamente que la función NDR debe desplegarse en los dos centros de cómputo del SRI mediante **la instalación de equipos de propósito específico**.

En virtud de lo expuesto, y considerando que el requisito del numeral 27 responde a una necesidad técnica institucional orientada a garantizar la adecuada prestación del servicio requerido, el SRI se ratifica en mantener el requerimiento técnico, debiendo los oferentes ajustarse a lo establecido en las especificaciones técnicas del proceso.

PREGUNTA 9.-

Respecto de lo solicitado en el apartado "Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE - NETWORK DETECTION AND RESPONSE (NDR) – 28. La función NDR debe desplegarse de tal forma que su falla de operación, avería física o sobrecarga no afecte el flujo normal del tráfico inspeccionado.", se entiende que el objetivo técnico del requerimiento es garantizar que la solución NDR opere de manera independiente al flujo de producción, de forma que cualquier falla, indisponibilidad, avería física o condición de sobrecarga de sus componentes no genere impacto sobre el tráfico de red inspeccionado. En este contexto, la solución a proponer contempla la implementación de la función NDR mediante equipos NGFW desplegados en modo pasivo a través de TAP o SPAN, operando fuera del camino del tráfico (Out-of-Band). Bajo esta arquitectura, los equipos utilizados para la captura e inspección de tráfico y la plataforma analítica asociada reciben copias del tráfico de red sin intervenir en su encaminamiento o procesamiento, por lo que cualquier falla operativa, avería física o condición de sobrecarga de dichos componentes no afecta la disponibilidad ni el flujo normal del tráfico de producción. **Se solicita al SRI confirmar que una arquitectura NDR desplegada en modo pasivo mediante equipos NGFW conectados a través de TAP o SPAN y operando Out-of-Band, que garantice que la falla o indisponibilidad de sus componentes no impacte el tráfico de producción, cumple con lo requerido y en consecuencia confirmar que el SRI puede entregar copia del tráfico en el modo pasivo mencionado.**

RESPUESTA 9.-

Estimado oferente, no se acepta la solicitud planteada.

En particular, el numeral 27 establece expresamente que la función NDR debe desplegarse en los dos centros de cómputo del SRI mediante la instalación de equipos de

propósito específico, requisito que responde a una necesidad técnica institucional y que se mantiene sin modificación.

PREGUNTA 10.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE - NETWORK DETECTION AND RESPONSE (NDR) – 29. La función NDR debe tener la capacidad de monitorear al menos 3.949 dispositivos (ver tabla 6).”, se entiende que el objetivo técnico del requerimiento es garantizar que la solución disponga de la capacidad necesaria para procesar y analizar el tráfico generado por la cantidad de dispositivos indicada en el pliego. En este contexto, la solución a proponer contempla la implementación de la función NDR mediante equipos NGFW utilizados como sensores de captura e inspección de tráfico, el modelo a ofertar soporta hasta 2.990.000 sesiones concurrentes de capa 7 (L7); considerando un escenario de dimensionamiento de 500 sesiones concurrentes por dispositivo, la capacidad resultante corresponde aproximadamente a 5.980 dispositivos monitoreados simultáneamente, superando la capacidad mínima requerida de 3.949 dispositivos. **Dado que la capacidad de monitoreo requerida se encuentra ampliamente cubierta por la capacidad de sesiones concurrentes soportada por la solución a proponer, se solicita al SRI confirmar si se acepta y cumple el requerimiento con lo indicado.**

RESPUESTA 10.-

Estimado oferente, no se acepta la solicitud planteada.

En particular, el numeral 27 establece expresamente que la función NDR debe desplegarse en los dos centros de cómputo del SRI mediante la instalación de equipos de propósito específico, requisito que responde a una necesidad técnica institucional y que se mantiene sin modificación.

PREGUNTA 11.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE - NETWORK DETECTION AND RESPONSE (NDR) - 35. El componente de hardware de la solución NDR debe ser desplegado de manera que al menos tenga visibilidad del tráfico que circula por los segmentos de los centros de datos que se indican a continuación. Para este efecto deben considerarse los datos de la tabla 8 de la INFRAESTRUCTURA ACTUAL. El tráfico de ingreso y de egreso de la DMZ de servicios externos, El tráfico de ingreso y de egreso de la DMZ de servicios internos, El tráfico de ingreso y de egreso de la red de acceso a Internet, El tráfico intercambiado entre cada centro de datos y las agencias, El tráfico intercambiado entre los dos centros de datos.”, **se solicita a SRI por favor confirmar que se podrá**

obtener copia del tráfico indicado en la Tabla 8 en modo pasivo a través de TAP o SPAN y que físicamente los sensores se puedan conectar en el mismo punto.

RESPUESTA 11.-

Estimado oferente, no se acepta la solicitud planteada.

El numeral 35 establece el requisito de que el componente de hardware de la solución NDR disponga de visibilidad sobre los segmentos de red especificados, con base en la infraestructura descrita en la Solicitud de Ofertas (SDO). Sin embargo, la forma específica de obtención del tráfico, así como los mecanismos de integración y conectividad requeridos para la implementación de la solución, forman parte del diseño detallado que deberá definirse en función de la solución ofertada y de las condiciones técnicas de la infraestructura institucional.

Corresponde a los oferentes presentar una solución que garantice el cumplimiento de los requisitos funcionales y de visibilidad establecidos en el numeral 35 y en los demás numerales correspondientes a NDR, considerando para ello las características de la infraestructura detalladas en la Solicitud de Ofertas (SDO).

PREGUNTA 12.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE - NETWORK DETECTION AND RESPONSE (NDR) – 35. El componente de hardware de la solución NDR debe ser desplegado de manera que al menos tenga visibilidad del tráfico que circula por los segmentos de los centros de datos que se indican a continuación. Para este efecto deben considerarse los datos de la tabla 8 de la INFRAESTRUCTURA ACTUAL. El tráfico de ingreso y de egreso de la DMZ de servicios externos, El tráfico de ingreso y de egreso de la DMZ de servicios internos, El tráfico de ingreso y de egreso de la red de acceso a Internet, El tráfico intercambiado entre cada centro de datos y las agencias, El tráfico intercambiado entre los dos centros de datos.”. Respecto del requisito de capacidad establecido en el presente numeral, se ha realizado el análisis de dimensionamiento tomando como base los volúmenes de tráfico indicados en la Tabla 8, cuya suma corresponde a 13,337 Gbps por centro de datos. Considerando el crecimiento compuesto del 5 % anual durante el período de vigencia previsto para la solución, el tráfico proyectado a cinco (5) años asciende a aproximadamente 17,022 Gbps por centro de datos. En este contexto, la solución propuesta contempla la implementación de un equipo NGFW en cada centro de datos, con una capacidad oficial de 20 Gbps de Threat Prevention. **Considerando que se ofertará un equipo NGFW por cada centro de datos, y que la capacidad de procesamiento de cada equipo es superior al tráfico máximo proyectado para el horizonte de diseño considerado, se solicita al SRI confirmar que con los equipos ofertados se cumple con el requerimiento de capacidad establecido en el presente numeral.**

RESPUESTA 12.-

Estimado oferente:

La Tabla 8 tiene por finalidad proporcionar una referencia del volumen de tráfico de los segmentos de red que deberán ser monitoreados por la solución NDR, considerando además las proyecciones de crecimiento definidas por la entidad.

Sin embargo, el cumplimiento de este requisito no se determina únicamente por la capacidad nominal de procesamiento o inspección de tráfico de un equipo específico, ni por los cálculos de dimensionamiento efectuados sobre un dispositivo particular de la arquitectura propuesta.

El SRI requiere, conforme lo establecido en el numeral 27, que la función NDR sea desplegada en los dos centros de cómputo mediante la instalación de **equipos de propósito específico para NDR**, requisito que responde a una necesidad técnica institucional y que se mantiene sin modificación.

La entidad evaluará la capacidad de la solución propuesta de manera integral, considerando el cumplimiento de todos los requisitos establecidos en la Solicitud de Ofertas (SDO).

PREGUNTA 13.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE - NETWORK DETECTION AND RESPONSE (NDR) – 18.43 La función NDR debe poder monitorear y analizar al menos las siguientes actividades u operaciones de los dispositivos: volumen de tráfico, descarga de software inusual, uso de herramientas de ataque y reconocimiento, ejecución de comandos remotos, ejecución de operaciones de lectura y escritura de SMB, acceso a sitios web (ej. URL, IP, dominio) sospechosos.”, **se solicita confirmar al SRI si se acepta que el presente requerimiento pueda ser cumplido mediante la información generada por los sensores NGFW de la función NDR y correlacionada por el Componente de Respuesta Unificada de Ciberdefensa, los cuales están incluidos en la oferta.**

RESPUESTA 13.-

Estimado oferente, no se acepta la solicitud planteada.

El SRI requiere, conforme lo establecido en el numeral 27, que la función NDR sea desplegada en los dos centros de cómputo mediante la instalación de **equipos de propósito específico para NDR**, requisito que responde a una necesidad técnica institucional y que se mantiene sin modificación.

PREGUNTA 14.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE – RESPUESTA UNIFICADA DE CIBERDEFENSA - 149. La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes controles de ciberseguridad institucionales: Check Point VSX, Proofpoint Core Email protection, Broadcom/Symantec ProxySG, Otros controles de ciberseguridad existentes con los que el servicio requiera integrarse para realizar acciones de contención. NOTAS: Es responsabilidad del contratista incluir en la función central de respuesta unificada de ciberdefensa las integraciones y las acciones de respuesta necesarias para lograr una respuesta efectiva y oportuna ante amenazas de ciberseguridad en el entorno institucional. El alcance de cada integración puede variar a medida que los fabricantes involucrados liberen nuevas versiones.”, **se consulta al SRI si la responsabilidad del contratista se considerará cumplida mediante la implementación de las integraciones requeridas para habilitar las acciones automatizadas de respuesta y contención, siempre que las plataformas de terceros identificadas por el SRI dispongan de interfaces, APIs, conectores, webhooks o mecanismos estándar técnicamente compatibles que permitan su integración y operación. Lo anterior considerando que la solución propuesta soporta múltiples mecanismos de integración y que el alcance y funcionalidades disponibles dependen de las capacidades expuestas por cada fabricante en sus respectivas plataformas y versiones.**

RESPUESTA 14.-

Estimado oferente,

De conformidad con el numeral 149 y sus notas asociadas, es responsabilidad del contratista implementar las integraciones y acciones de respuesta necesarias para que la función central de Respuesta Unificada de Ciberdefensa pueda ejecutar acciones automatizadas de contención sobre los controles de ciberseguridad institucionales indicados y sobre aquellos componentes tecnológicos “complementarios” que por la arquitectura de la solución propuesta se requieran integrar para una respuesta efectiva y oportuna ante amenazas de ciberseguridad.

La implementación de dichas integraciones podrá realizarse utilizando los mecanismos **técnicos disponibles y soportados por las plataformas involucradas**, tales como APIs, conectores, webhooks u otros mecanismos estándar de integración proporcionados por los respectivos fabricantes.

Se debe considerar que no se está solicitando que la integración sea nativa, es decir se podrá desarrollar las integraciones necesarias para dar cumplimiento con el requisito.

PREGUNTA 15.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE – RESPUESTA UNIFICADA DE CIBERDEFENSA - 149. La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes controles de ciberseguridad institucionales: Check Point VSX, Proofpoint Core Email protection, Broadcom/Symantec ProxySG, Otros controles de ciberseguridad existentes con los que el servicio requiera integrarse para realizar acciones de contención. NOTAS: Es responsabilidad del contratista incluir en la función central de respuesta unificada de ciberdefensa las integraciones y las acciones de respuesta necesarias para lograr una respuesta efectiva y oportuna ante amenazas de ciberseguridad en el entorno institucional. El alcance de cada integración puede variar a medida que los fabricantes involucrados liberen nuevas versiones.”, **se consulta al SRI si se aceptaría como cumplimiento, una carta de compromiso del oferente que garantice la creación y ejecución de las tareas automáticas de los controles de ciberseguridad institucionales que no están implementados a la fecha, considerando que el alcance y funcionalidades disponibles dependen de las capacidades expuestas por cada fabricante en sus respectivas plataformas y versiones.**

RESPUESTA 15.-

Estimado oferente,

Se aclara que de conformidad con el numeral 149 donde se establece:

“Otros controles de ciberseguridad existentes con los que el servicio requiera integrarse para realizar acciones de contención.”

Esto corresponde a aquellos componentes tecnológicos “complementarios” que por la arquitectura de la solución propuesta se requieran integrar para una respuesta efectiva y oportuna ante amenazas de ciberseguridad.

Adicionalmente, se aceptará una carta de compromiso por parte del oferente únicamente para aquellas integraciones en las que no se cuentan con mecanismos nativos de los fabricantes involucrados y que en consecuencia requieren un desarrollo o componentes complementarios.

PREGUNTA 16.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE – RESPUESTA UNIFICADA DE CIBERDEFENSA - 150. La función central de respuesta unificada de ciberdefensa debe

ser capaz de realizar al menos las siguientes tareas automáticas sobre la solución de Check Point VSX del SRI: Bloquear comunicaciones relacionadas con IOCs específicos; Bloquear una dirección IP de origen o destino específica.”, **se consulta al SRI si se aceptaría como cumplimiento, una carta de compromiso del oferente que garantice la creación y ejecución de las tareas automáticas sobre la solución de Check Point VSX que no están implementadas a la fecha, considerando que el alcance y funcionalidades disponibles dependen de las capacidades expuestas por cada fabricante en sus respectivas plataformas y versiones, así como, de la disponibilidad de los interfaces o mecanismos de integración técnicamente compatibles que permitan implementar dichas acciones mediante automatizaciones en la solución ofertada.**

RESPUESTA 16.-

Estimado oferente,

Se aceptará una carta de compromiso por parte del oferente únicamente para aquellas integraciones en las que no se cuentan con mecanismos nativos de los fabricantes involucrados y que en consecuencia requieren un desarrollo o componentes complementarios.

PREGUNTA 17.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE – RESPUESTA UNIFICADA DE CIBERDEFENSA – 151. La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar al menos las siguientes tareas automáticas sobre la solución de Proofpoint Core Email Protection del SRI: Bloquear dominios y direcciones IP de remitentes; Bloquear direcciones URL maliciosas en mensajes entregados.”, **se consulta al SRI si se aceptaría como cumplimiento, una carta de compromiso del oferente que garantice la creación y ejecución de las tareas automáticas sobre la solución de Proofpoint Core Email Protection que no están implementadas a la fecha, considerando que el alcance y funcionalidades disponibles dependen de las capacidades expuestas por cada fabricante en sus respectivas plataformas y versiones, así como, de la disponibilidad de los interfaces o mecanismos de integración técnicamente compatibles que permitan implementar dichas acciones mediante automatizaciones en la solución ofertada.**

RESPUESTA 17.-

Estimado oferente,

Se aceptará una carta de compromiso por parte del oferente únicamente para aquellas integraciones en las que no se cuentan con mecanismos nativos de los fabricantes

involucrados y que en consecuencia requieren un desarrollo o componentes complementarios.

PREGUNTA 18.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE – RESPUESTA UNIFICADA DE CIBERDEFENSA – 152. La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar al menos las siguientes tareas automáticas sobre la solución de Broadcom/Symantec ProxySG del SRI: Bloquear en función de direcciones URL; Bloquear en función de usuarios; Bloquear en función de la ubicación geográfica.”, **se consulta al SRI si se aceptaría como cumplimiento, una carta de compromiso del oferente que garantice la creación y ejecución de las tareas automáticas sobre la solución de Broadcom/Symantec ProxySG que no están implementadas a la fecha, considerando que el alcance y funcionalidades disponibles dependen de las capacidades expuestas por cada fabricante en sus respectivas plataformas y versiones, así como, de la disponibilidad de los interfaces o mecanismos de integración técnicamente compatibles que permitan implementar dichas acciones mediante automatizaciones en la solución ofertada.**

RESPUESTA 18.-

Estimado oferente,

Se aceptará una carta de compromiso por parte del oferente únicamente para aquellas integraciones en las que no se cuentan con mecanismos nativos de los fabricantes involucrados y que en consecuencia requieren un desarrollo o componentes complementarios.

PREGUNTA 19.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE – RESPUESTA UNIFICADA DE CIBERDEFENSA – 153. La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes componentes tecnológicos institucionales: Microsoft Exchange (local y online), Palo Alto Networks ION SDWAN, IBM Verify Identity Governance, VMware vCenter/vSphere, Otros componentes tecnológicos existentes con los que el servicio requiera integrarse para realizar acciones de contención.”, **se consulta al SRI si se aceptaría como cumplimiento, una carta de compromiso del oferente que garantice la creación y ejecución de las tareas automáticas de los componentes tecnológicos institucionales (indicados) que no están implementadas a la fecha, siempre que estos dispongan de interfaces o mecanismos de**

integración técnicamente compatibles que permitan implementar dichas acciones mediante automatizaciones en la solución ofertada.

RESPUESTA 19.-

Estimado oferente,

Se aceptará una carta de compromiso por parte del oferente únicamente para aquellas integraciones en las que no se cuentan con mecanismos nativos de los fabricantes involucrados y que en consecuencia requieren un desarrollo o componentes complementarios.

PREGUNTA 20.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE – RESPUESTA UNIFICADA DE CIBERDEFENSA – 155. La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar al menos las siguientes tareas automáticas sobre el sistema Palo Alto Networks ION SDWAN del SRI (ver INFRAESTRUCTURA ACTUAL): Aislar automáticamente segmentos comprometidos o dispositivos infectados del resto de la red; Ajustar prioridades de tráfico para controlar propagación de malware; Restringir comunicaciones con regiones geográficas identificadas como fuentes de amenazas; Bloquear comunicaciones con servidores C&C a través de toda la infraestructura SD-WAN.” **se consulta al SRI si se aceptaría como cumplimiento, una carta de compromiso del oferente que garantice la creación y ejecución de las tareas automáticas de los controles de ciberseguridad institucionales que no están implementados e integrados a la fecha, siempre que las operaciones específicas requeridas se encuentren disponibles y soportadas por las APIs o los mecanismos de integración habilitados en Prisma SD-WAN ION o se consideren las buenas prácticas del mercado respecto de la integración de plataformas de networking en soluciones y/o servicios de Ciberseguridad.**

RESPUESTA 20.-

Estimado oferente,

Se aceptará una carta de compromiso por parte del oferente únicamente para aquellas integraciones en las que no se cuentan con mecanismos nativos de los fabricantes involucrados y que en consecuencia requieren un desarrollo o componentes complementarios.

PREGUNTA 21.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE – RESPUESTA UNIFICADA DE CIBERDEFENSA – 156. La función central de respuesta unificada de ciberdefensa debe

ser capaz de realizar al menos las siguientes tareas automáticas sobre el sistema IBM Verify Identity Governance del SRI: Desactivar usuario.”, **se consulta al SRI si se aceptaría como cumplimiento, una carta de compromiso del oferente que garantice la creación y ejecución de la tarea automática sobre el sistema IBM Verify Identity Governance que no está implementada a la fecha, siempre que la operación de desactivación de usuarios se encuentre disponible y soportada en la API o en los mecanismos de integración habilitados por IBM Verify Identity Governance.**

RESPUESTA 21.-

Estimado oferente,

Se aceptará una carta de compromiso por parte del oferente únicamente para aquellas integraciones en las que no se cuentan con mecanismos nativos de los fabricantes involucrados y que en consecuencia requieren un desarrollo o componentes complementarios.

PREGUNTA 22.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - BIENES REQUERIDOS - COMPONENTE DE SOFTWARE – RESPUESTA UNIFICADA DE CIBERDEFENSA – 157. La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar al menos las siguientes tareas automáticas sobre el sistema VMware vCenter/vSphere del SRI (ver INFRAESTRUCTURA ACTUAL): Apagar o reiniciar forzosamente máquinas virtuales; Aislar máquinas virtuales de la red.”, **se consulta al SRI si se aceptaría como cumplimiento, una carta de compromiso del oferente que garantice la creación y ejecución de las tareas automáticas sobre el sistema VMware vCenter/vSphere que no están implementadas a la fecha, siempre que las operaciones de apagado, reinicio forzado y aislamiento de máquinas virtuales se encuentren disponibles y soportadas por las APIs o los mecanismos de integración habilitados en VMware vCenter/vSphere.**

RESPUESTA 22.-

Estimado oferente,

Se aceptará una carta de compromiso por parte del oferente únicamente para aquellas integraciones en las que no se cuentan con mecanismos nativos de los fabricantes involucrados y que en consecuencia requieren un desarrollo o componentes complementarios.

PREGUNTA 23.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - B. PRESTACIONES DEL SERVICIO DE GESTIÓN DE CIBERDEFENSA - SERVICIOS

CONEXOS REQUERIDOS – 1. 1. La gestión de ciberdefensa incluida debe ser realizada por el equipo de Managed Detection and Response (MDR) del fabricante, el cual debe colaborar con el personal local.”. y considerando que diversos fabricantes autorizan la prestación de estos servicios tanto de manera directa como a través de partners certificados, bajo modelos de prestación como Extended MDR, **se consulta al SRI si será aceptable que el servicio MDR sea ejecutado por un partner certificado y autorizado por el fabricante, en colaboración con el personal local, siempre que dicho partner disponga de personal certificado, acceso a los procesos oficiales de soporte y escalamiento del fabricante, y garantice el cumplimiento integral de los niveles de servicio y requerimientos establecidos en el proceso.**

RESPUESTA 23.-

Estimado oferente, no se acepta la solicitud planteada.

El numeral 1 de la Sección VI establece expresamente que la gestión de ciberdefensa incluida en el servicio debe ser realizada por el **equipo de Managed Detection and Response (MDR) del fabricante**, el cual deberá colaborar con el personal local.

En este sentido, el requerimiento define que la responsabilidad de la operación MDR corresponde directamente al equipo especializado del fabricante, por lo que la prestación del servicio únicamente mediante un partner certificado o autorizado no se considera equivalente al cumplimiento de la condición establecida.

PREGUNTA 24.-

Con el fin de optimizar la operación, visibilidad y capacidades de respuesta ante incidentes, y considerando que la solución propuesta contempla una arquitectura integrada de ciberdefensa, **se consulta al SRI si se acepta que los componentes de inteligencia y respuesta unificada consoliden y correlacionen las funcionalidades de EDR, NDR y Gestión de Amenazas de Identidad, manteniendo el cumplimiento de todos los requisitos técnicos y niveles definidos en el proceso.**

RESPUESTA 24.-

Estimado oferente, no se acepta la solicitud planteada.

A diferencia de NDR y Gestión de Amenazas de Identidad, cuyos numerales 25 y 58 permiten expresamente su implementación *"como componente independiente o como funcionalidad de uno o varios de los componentes tecnológicos incluidos en la solución"*, el componente EDR no cuenta con este requisito.

PREGUNTA 25.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - SERVICIO DE GESTIÓN DE CIBERDEFENSA – 4. Si la gestión de eventos o

incidentes requiere la intervención directa de los componentes tecnológicos o los controles de seguridad institucionales, el personal del servicio debe ingresar el requerimiento en la herramienta de gestión tecnológica (ITSM) del SRI para que así pueda realizar el seguimiento de la realización de las actividades y también para que el personal del SRI pueda realizar la asignación interna de tareas.” **Por favor indicar cuál es la herramienta de gestión tecnológica (ITSM) del SRI y qué mecanismo de integración expone, debido a que el documento de licitación obliga a registrar en ella los requerimientos que involucren intervención del personal institucional.**

RESPUESTA 25.-

El Servicio de Rentas Internas (SRI) dispone de la plataforma **BMC Helix ITSM** para la gestión tecnológica ITSM.

Para el cumplimiento del requerimiento señalado, no se establece como condición obligatoria la implementación de una integración automática mediante API, web services u otros mecanismos de interoperabilidad entre la plataforma del contratista y BMC Helix ITSM.

El contratista podrá realizar el registro de los requerimientos de manera manual en la herramienta BMC Helix ITSM, utilizando los mecanismos de acceso sean proporcionados o habilitados por el SRI, siempre que se garantice la trazabilidad y el seguimiento de las actividades requeridas.

En caso de que el contratista disponga de mecanismos de integración compatibles con la plataforma ITSM que tiene el SRI, estos podrán ser utilizados, previa coordinación y autorización del SRI, sin que su implementación constituya un requisito obligatorio para el cumplimiento de este requerimiento.

PREGUNTA 26.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - SERVICIO DE GESTIÓN DE CIBERDEFENSA – 4. Si la gestión de eventos o incidentes requiere la intervención directa de los componentes tecnológicos o los controles de seguridad institucionales, el personal del servicio debe ingresar el requerimiento en la herramienta de gestión tecnológica (ITSM) del SRI para que así pueda realizar el seguimiento de la realización de las actividades y también para que el personal del SRI pueda realizar la asignación interna de tareas.”, los tiempos de la tabla de respuesta miden el inicio del análisis técnico por lo cual se consulta si **el SRI acepta el registro de la herramienta de gestión del contratista como evidencia del inicio, o exige el registro en el ITSM institucional.**

RESPUESTA 26.-

Estimado oferente:

El inicio del análisis técnico deberá contar con evidencia verificable y auditable que permita determinar la fecha y hora en la que el personal especializado del servicio inició las actividades de análisis, investigación o gestión correspondientes.

Para tal efecto, será responsabilidad del contratista mantener una bitácora o registro de las actividades realizadas, la cual deberá contener la información y los respaldos, documentos, registros, evidencias técnicas o cualquier otro material pertinente que permita verificar y acreditar de manera objetiva las actividades ejecutadas, así como el cumplimiento de los tiempos establecidos en la tabla de niveles de servicio.

PREGUNTA 28.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - SERVICIO DE GESTIÓN DE CIBERDEFENSA – 2. Si la gestión de eventos o incidentes requiere la intervención directa de los componentes tecnológicos o los controles de seguridad institucionales, el personal del servicio debe coordinar las acciones correctivas, de remediación o de respuesta presencialmente en las oficinas de la Dirección Nacional de Tecnología.”, **se solicita al SRI una estimación de frecuencia y franja horaria de acuerdo con el historial que maneje el SRI al respecto.**

RESPUESTA 28.-

Los incidentes o eventos no son predecibles por lo que no es factible establecer una frecuencia o franja horaria. Por este motivo se solicitó el servicio debe estar disponible y activo las 24 horas del día, los 7 días de la semana, de acuerdo con lo que se establece en el numeral 2 del apartado “B. PRESTACIONES DEL SERVICIO DE GESTIÓN DE CIBERDEFENSA”

PREGUNTA 29.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - SERVICIO DE GESTIÓN DE CIBERDEFENSA – 7. Es responsabilidad del contratista realizar el mantenimiento periódico de los componentes tecnológicos incluidos en la solución contratada para garantizar su correcto funcionamiento y la entrega del servicio.”, **se solicita al SRI definir la frecuencia esperada de dicho mantenimiento.**

RESPUESTA 29.-

Estimado oferente,

La frecuencia del mantenimiento periódico de los componentes tecnológicos incluidos en la solución ofertada **deberá ejecutarse conforme a las recomendaciones y mejores**

prácticas definidas por los fabricantes, considerando la naturaleza de cada componente, su criticidad, estado operativo, actualizaciones disponibles, vulnerabilidades identificadas, entre otras.

En función de lo expuesto, corresponde al contratista establecer la frecuencia, alcance y actividades asociadas al mantenimiento dentro del plan de implementación de acuerdo con las recomendaciones y mejores prácticas de los fabricantes involucrados en la solución ofertada, el cual deberá ser presentado para revisión y aprobación del Administrador del Contrato, considerando que los componentes forman parte de un servicio y no serían propiedad del SRI.

PREGUNTA 30.-

Respecto de lo solicitado en el apartado “Sección VI. Requisitos de los Bienes y Servicios Conexos - ACUERDO DE NIVEL DE SERVICIO – 2. El tiempo de contención de ciberamenazas se define como el intervalo comprendido entre la materialización de una ciberamenaza – según los registros de los sistemas y controles involucrados– y el momento en que se logra detener su avance o propagación. La tabla 2 aplica únicamente a los casos en los que la contención se efectúa sin requerir intervención sobre los sistemas institucionales.”, **se solicita al SRI indicar ¿Cómo se acredita que un caso no requería intervención de los sistemas institucionales?, debido a que esta es la condición que activa el umbral de tiempo del SLA, por lo cual su verificación debe ser objetiva para ambas partes.**

RESPUESTA 30.-

Estimado oferente:

De conformidad con lo establecido en el numeral 2 del apartado “ACUERDO DE NIVEL DE SERVICIO”, el tiempo de contención de ciberamenazas aplica únicamente para aquellos casos en los que las acciones de contención puedan ejecutarse sin requerir intervención directa sobre los sistemas o controles de seguridad institucionales del SRI.

La determinación de si un caso requiere o no intervención sobre sistemas institucionales deberá realizarse durante el proceso de análisis técnico del evento o incidente, considerando la información disponible, el alcance de la amenaza identificada, los activos involucrados y las capacidades de respuesta disponibles mediante los componentes tecnológicos incluidos en la solución contratada.

La acreditación de dicha condición deberá sustentarse mediante los registros de gestión del caso generados durante la atención, incluyendo, según corresponda, la descripción de la amenaza, los activos afectados o potencialmente afectados, las acciones de contención

ejecutadas, los componentes tecnológicos utilizados y la justificación técnica respecto a si fue necesaria o no la intervención sobre sistemas institucionales.

En los casos en los que la contención pueda ejecutarse mediante las capacidades propias de la solución contratada (por ejemplo, mediante automatizaciones, playbooks, acciones sobre los componentes incluidos en el servicio u otros mecanismos disponibles), sin requerir cambios, accesos o acciones directas sobre infraestructura tecnológica del SRI, aplicará el tiempo de contención establecido en la Tabla 2 del Acuerdo de Nivel de Servicio.

Cuando la contención requiera intervención directa del personal del SRI, accesos administrativos, ejecución de actividades sobre sistemas institucionales o participación de terceros responsables de dichos componentes, dicha condición deberá quedar documentada en el registro del incidente y se gestionará conforme a las actividades de coordinación y atención definidas para estos casos.

La validación de la clasificación del caso y de la aplicabilidad del umbral correspondiente será realizada con base en la evidencia técnica registrada durante la gestión del evento o incidente.

PREGUNTA 31.-

Respecto de lo solicitado en el apartado CGC 28.1 – PENALIDADES – SERVICIO DE GESTIÓN DE CIBERDEFENSA, **se solicita al SRI confirmar si a penalidad por cada hora de exceso en la resolución de incidentes, ¿tiene un tope máximo por periodo, o es acumulativa sin límite?**

RESPUESTA 31.-

Estimado oferente,

El documento de licitación no establece un tope máximo por periodo para la aplicación de esta penalidad, ni establece una condición diferente para su acumulación. En consecuencia, la multa se aplicará conforme al número de horas o fracciones de hora de retraso que se verifiquen respecto del tiempo máximo de resolución definido en el Acuerdo de Nivel de Servicio (SLA) para cada incidente de ciberseguridad.

PREGUNTA 32.-

En la sección VI. Requisitos de los Bienes y Servicios Conexos, subsección 2. LISTA DE SERVICIOS / SERVICIOS CONEXOS Y CRONOGRAMA DE CUMPLIMIENTO en el apartado de ACUERDO DE NIVEL DE SERVICIO, página 142 indica el "tiempo de atención" inicia cuando comienza el análisis técnico humano y no la notificación automática. ¿Cómo se validará y certificará ese inicio para efectos de auditoría del cumplimiento del SLA (ticket bitácora, sello de tiempo del SOC, etc.)?

RESPUESTA 32.-

Estimado oferente:

El inicio del análisis técnico deberá contar con evidencia verificable y auditable que permita determinar la fecha y hora en la que el personal especializado del servicio inició las actividades de análisis, investigación o gestión correspondientes.

Para tal efecto, será responsabilidad del contratista mantener una bitácora o registro de las actividades realizadas, la cual deberá contener la información y los respaldos, documentos, registros, evidencias técnicas o cualquier otro material pertinente que permita verificar y acreditar de manera objetiva las actividades ejecutadas, así como el cumplimiento de los tiempos establecidos en la tabla de niveles de servicio.

PREGUNTA 33.-

En la sección VI. Requisitos de los Bienes y Servicios Conexos, subsección 2. LISTA DE SERVICIOS / SERVICIOS CONEXOS Y CRONOGRAMA DE CUMPLIMIENTO en el apartado de ACUERDO DE NIVEL DE SERVICIO, en Tabla 2 página 143 ¿Por favor definir a qué se considera "hora hábil" para el cómputo del SLA (rango horario específico) y qué calendario de días hábiles y feriados aplica?

RESPUESTA 33.-

Se considera "hora hábil" al intervalo comprendido entre las 08:00 y las 17:00 horas, tomando como referencia el calendario oficial de días laborables y feriados de la República del Ecuador.

PREGUNTA 34.-

En la sección VII. Condiciones Generales del Contrato (CGC), ítem 36.Terminación subítem 36.1 Terminación por Incumplimiento, página 177 ¿Existe un techo máximo de multas acumuladas, mensual o total del contrato, antes de configurar causal de terminación anticipada por incumplimiento?

RESPUESTA 34.-

De conformidad con lo previsto en la cláusula CGC 10.1, el contrato se regirá por las leyes de la República del Ecuador. En este marco normativo, resulta aplicable la Ley Orgánica del Sistema Nacional de Contratación Pública y su Reglamento General, los cuales establecen que procede la terminación unilateral del contrato por incumplimiento cuando el monto acumulado de las multas impuestas exceda el valor de la garantía de fiel cumplimiento.

PREGUNTA 36.-

En el documento de licitación Sección VIII "Condiciones Especiales del Contrato", CGC 17.1

"FORMA Y CONDICIONES DE PAGO", se indica que "El 100% de ambos rubros [licenciamiento e implementación] se pagará al finalizar la Implementación, previa presentación de la planilla de pago y suscripción del acta de entrega-recepción." Esto implica que el proveedor adjudicado no recibirá ningún pago durante un período aproximado de 105 días calendario (15 días de activación de licenciamiento + 90 días de implementación), período en el cual debe costear la adquisición e importación del hardware NDR, la activación de licencias de todos los componentes y la ejecución completa de la implementación. Se solicita a la entidad considerar la viabilidad de establecer un esquema de pago en al menos dos tramos, por ejemplo: un porcentaje al momento de la entrega activación del licenciamiento, y el saldo al momento de la suscripción del acta de entrega-recepción de la implementación. En caso de mantener el esquema de pago único, se solicita confirmar que el presupuesto referencial incorpora el costo financiero asociado a este flujo diferido de pago.

RESPUESTA 36.-

Estimado oferente,

No se acepta su solicitud, el pago se realizará según lo que se encuentra estipulado en CGC 17.1 FORMA Y CONDICIONES DE PAGO de la Sección VIII. Condiciones Especiales de Contrato (CEC).

PREGUNTA 37.-

En el documento de licitación Sección VI "Requisitos de los Bienes y Servicios Conexos", en las especificaciones técnicas del componente NDR, se establece que las acciones de contención del NDR deben incluir "acciones de bloqueo mediante integración con la infraestructura de SDN del SRI (ver INFRAESTRUCTURA ACTUAL)", siendo esta integración calificada como obligatoria. La Tabla 4 del documento detalla que la infraestructura SDN del SRI es Cisco ACI con controladores APIC en versión 5.2(8g), tanto en el centro de datos principal como en el alterno. Se solicita a la entidad confirmar: (a) ¿El controlador APIC

de Cisco ACI tiene habilitadas las APIs REST necesarias para la integración con soluciones

NDR de terceros fabricantes? (b) ¿Existe alguna restricción de licenciamiento en

la infraestructura Cisco ACI (versión del software, módulos adicionales requeridos)

que pudiera limitar o condicionar la integración con soluciones NDR? Esta información es esencial para que los oferentes evalúen la viabilidad técnica de la integración obligatoria con la infraestructura SDN del SRI antes de presentar su oferta.

RESPUESTA 37.-

Estimado oferente, el numeral 50 de la Sección VI, establece que la función NDR debe realizar acciones de contención mediante al menos dos de las siguientes formas:

- acciones autónomas de bloqueo (ej. TCP RESET),

- acciones de bloqueo mediante integración con la infraestructura de SDN del SRI (ver **INFRAESTRUCTURA ACTUAL**),
- acciones de bloqueo mediante integración con el sistema de firewall del SRI (ver **INFRAESTRUCTURA ACTUAL**) [*obligatoria*].

Siendo esta última la única calificada expresamente como obligatoria, es decir, la integración con la infraestructura SDN (Cisco ACI) constituye una de las alternativas posibles y no la única vía obligatoria de contención.

El controlador Cisco APIC expone de forma nativa y habilitada por defecto una API REST northbound (sobre HTTPS, con respuestas en JSON/XML), que constituye la interfaz primaria de gestión y programabilidad del fabric ACI. Esta API está disponible y permite a soluciones de terceros (incluidas plataformas NDR) obtener contexto de red (topología, endpoints, EPGs, tenants, inventario, fallas y health scores). Para la captura de tráfico propia de un NDR, el fabric ACI soporta adicionalmente SPAN, ERSPAN y telemetría, configurables a través de la misma API REST.

Para la integración vía API REST y para la captura de tráfico mediante SPAN/ERSPAN no existe restricción de licenciamiento adicional: estas capacidades están cubiertas por la suscripción básica (Essentials), que incluye las funciones de gestión del fabric ACI a través del APIC. Solo aplicaría un condicionante si la solución NDR requiriera telemetría avanzada o Network Insights (también conocido como Day-2 Operations Suite), en cuyo caso se necesitaría el licenciamiento Premier o el add-on Day-2 Operations.

PREGUNTA 40.-

En la página 146 en relación a la Tabla 3.- Descripción de los niveles de prioridad. Por favor confirmar ¿si el SRI cuenta con la clasificación de los activos y servicios de IMPACTO: crítico alto, medio y bajo?

RESPUESTA 40.-

El SRI dispone de la categorización y clasificación de sus activos tecnológicos, la cual será compartida con el contratista durante la etapa correspondiente.

PREGUNTA 41.-

En la página 140 sección: Sección VI – Requisitos de los Bienes y Servicios Conexos, Apartado: GESTIÓN DE INCIDENTES, Teniendo en cuenta que existen incidentes de ciberseguridad cuya solución puede considerarse a largo plazo por varias situaciones, ¿estos podrían cerrarse y ser tratados como problemas, sin afectación al SLA?

RESPUESTA 41.-

Estimado oferente,

En la Solicitud de Oferta (SDO) no se contempla la posibilidad de cerrar un incidente de

ciberseguridad y tratarlo posteriormente como un problema.

La gestión de los incidentes de ciberseguridad deberá realizarse conforme a lo establecido en el apartado "GESTIÓN DE INCIDENTES", cubriendo las etapas de análisis, contención, erradicación y acciones posteriores, así como la elaboración de los informes de avance y de cierre que correspondan.

El cumplimiento de los Acuerdos de Nivel de Servicio (SLA) será evaluado conforme a las condiciones y tiempos establecidos en la SDO.

PREGUNTA 42.-

En la página 131, punto 34 relacionado con B. PRESTACIONES DEL SERVICIO DE GESTIÓN DE CIBERDEFENSA, es de nuestro entendimiento que la fase de CONTENCIÓN estará relacionada única y exclusivamente con las acciones automatizadas en la solución tecnológica propuesta. Por favor confirmar si es correcto nuestro entendimiento.

RESPUESTA 42.-

Estimado oferente, no es correcto su entendimiento. El numeral 34 del apartado GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD, establece que en la etapa de contención el servicio debe incluir, entre otras actividades: *"Ejecutar playbooks o acciones automatizadas para la contención automatizada de los incidentes"*, pero también *"Convocar al equipo CSIRT del servicio"*, *"Definir las acciones necesarias para contener el ataque"*, *"Elaborar la estrategia y la táctica de contención"*, *"Colaborar con el CERT conformado por el SRI"* y *"Participar en las actividades de contención del incidente coordinadas por el SRI"*.

En consecuencia, la fase de contención no se limita exclusivamente a las acciones automatizadas ejecutadas por la solución tecnológica propuesta, sino que comprende todas las actividades previstas en el numeral citado.

PREGUNTA 43.-

En el documento de licitación Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE EVENTOS DE CIBERSEGURIDAD", se indica que "La gestión de los eventos de ciberseguridad debe incluir su remediación mediante la aplicación de las acciones necesarias para eliminar su ocurrencia o reducirla significativamente" y que "Las acciones de remediación se deben aplicar directamente en los controles de ciberseguridad incluidos en la solución contratada o indirectamente en los controles de ciberseguridad institucionales integrados con el servicio." Se solicita aclarar el alcance de las acciones de remediación a cargo del proveedor contratado: Es de nuestro entendimiento que la remediación sobre los componentes tecnológicos institucionales del SRI (aquellos que no forman parte de la solución contratada) se limitará a la elaboración y entrega de recomendaciones técnicas, planes de migración y lineamientos operativos, siendo el personal de TI y los administradores de infraestructura del SRI los únicos responsables de ejecutar, configurar y aplicar dichos cambios en el entorno de producción institucionales. Confirmar si es correcto nuestro entendimiento.

RESPUESTA 43.-

Estimado oferente:

No es correcto su entendimiento.

De conformidad con los numerales 13 y 14 del apartado “GESTIÓN DE EVENTOS DE CIBERSEGURIDAD”, la gestión de los eventos de ciberseguridad debe incluir su remediación mediante la aplicación de las acciones necesarias para eliminar su ocurrencia o reducirla significativamente. Asimismo, dichas acciones de remediación deberán aplicarse directamente en los controles de ciberseguridad incluidos en la solución contratada o indirectamente en los controles de ciberseguridad institucionales integrados con el servicio, según corresponda.

Adicionalmente, cuando la gestión de eventos o incidentes requiera la intervención directa de componentes tecnológicos o controles de seguridad institucionales, serán aplicables las disposiciones establecidas en el apartado “SERVICIO DE GESTIÓN DE CIBERDEFENSA”, que contemplan la coordinación con el personal del SRI, la ejecución presencial cuando corresponda y el registro del requerimiento en la herramienta ITSM institucional.

En consecuencia, el alcance de las obligaciones del contratista será el establecido en la SDO, sin limitarse únicamente a la elaboración de recomendaciones técnicas sobre los componentes tecnológicos institucionales.

PREGUNTA 44.-

En el documento en la página en la página 131 de licitación Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE EVENTOS DE CIBERSEGURIDAD", se indica que "El servicio debe revisar periódicamente que los flujos de trabajo ('playbooks') estén operando adecuadamente y debe agregar o configurar nuevos en función del análisis de los eventos detectados o de los requerimientos del SRI." Se solicita aclarar la situación actual de los playbooks institucionales: ¿El SRI cuenta actualmente con playbooks de respuesta a incidentes previamente implementados y en operación sobre los cuales el equipo consultor deberá realizar revisiones periódicas de eficacia? ¿O los playbooks

deberán ser diseñados, configurados e implementados desde cero por el proveedor como parte del contrato? En caso de que ya existan playbooks, ¿se pondrán a disposición del oferente durante el proceso de licitación para que este pueda estimar correctamente el esfuerzo requerido?

RESPUESTA 44.-

Estimado oferente,

En el numeral 137 de la sección “RESPUESTA UNIFICADA DE CIBERDEFENSA” se establece que: *“La función central de respuesta unificada de ciberdefensa debe utilizar flujos de trabajo (“playbooks”) para ejecutar automáticamente las acciones de respuesta a los eventos e incidentes de ciberseguridad detectados”*

En el numeral 140 de la misma sección se establece que:

“La función central de respuesta unificada de ciberdefensa debe permitir al Administrador incorporar tareas automáticas, tareas manuales, tareas de colección de datos y tareas condicionadas en la ejecución de los playbooks, si la respuesta a un evento o incidente así lo requiere.”

En función de lo expuesto los *playbooks* a los que hace referencia el apartado **GESTIÓN DE EVENTOS DE CIBERSEGURIDAD** corresponden a los flujos de trabajo de la **función central de respuesta unificada de ciberdefensa** que forme parte de la solución ofertada. En consecuencia, los *playbooks* objeto del contrato corresponden a los implementados sobre la solución ofertada por el contratista. La definición, configuración, implementación, revisión y actualización de dichos *playbooks* deberán realizarse como parte de la ejecución contractual, de conformidad con los requerimientos establecidos en la Solicitud de la Oferta (SDO).

PREGUNTA 45.-

En el documento en la página 131 de licitación Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE EVENTOS DE CIBERSEGURIDAD", se indica que " El servicio debe hacer el seguimiento de las acciones de gestión de eventos de ciberseguridad hasta su remediación." Se solicita aclarar cómo se define el término "seguimiento" en este contexto es de nuestro entendimiento que el seguimiento consiste en el monitoreo y verificación por parte del proveedor de que las acciones correctivas acordadas han sido ejecutadas por el personal de TI del SRI, hasta confirmar la remediación del evento. Por favor confirmar si es correcto nuestro entendimiento.

RESPUESTA 45.-

Estimado oferente, su entendimiento es correcto.

El término **“seguimiento”** hace referencia a la verificación y trazabilidad de las acciones ejecutadas durante la gestión de eventos de ciberseguridad, hasta confirmar que las acciones definidas para su remediación hayan sido aplicadas y que el evento haya sido gestionado conforme corresponda.

PREGUNTA 46.-

En el documento de licitación Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD", se indica que "El servicio debe proveer al personal de Soporte a Usuarios y de Seguridad Informática de un juego de herramientas ('toolkit') portable, incluyendo su medio físico, que les permita reaccionar y colaborar con el servicio en los casos de incidentes de ciberseguridad que afecten las estaciones de trabajo." Es de nuestro entendimiento que el alcance funcional del toolkit portable se restringe a herramientas orientadas exclusivamente a la investigación técnica y al análisis forense digital de estaciones de trabajo afectadas. Confirmar si es correcto

nuestro entendimiento.

RESPUESTA 46.-

Estimado oferente, de acuerdo con lo establecido en el apartado GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD, el servicio debe proveer al personal de Soporte a Usuarios y de Seguridad Informática un juego de herramientas (*toolkit*) portable, incluyendo su medio físico, que permita reaccionar y colaborar con el servicio en los casos de incidentes de ciberseguridad que afecten las estaciones de trabajo.

Por lo tanto, el *toolkit* deberá incluir las herramientas necesarias para apoyar las actividades requeridas durante la atención de incidentes de ciberseguridad en estaciones de trabajo, de acuerdo con las capacidades y procedimientos definidos por la solución contratada. Estas actividades pueden incluir, entre otras que correspondan, la recopilación de información, análisis técnico, apoyo en la investigación y demás acciones necesarias para la respuesta al incidente.

En consecuencia, no se confirma que el alcance del *toolkit* se restrinja exclusivamente a herramientas de investigación técnica y análisis forense digital, debido a que el requerimiento establece como finalidad permitir la reacción y colaboración en la gestión de incidentes de ciberseguridad que afecten estaciones de trabajo.

PREGUNTA 47.-

En el documento en la página 156 de licitación Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD", se indica que "El servicio debe proveer protocolos de respuesta al personal de Soporte a Usuarios y de Seguridad Informática para los casos de incidentes de ciberseguridad que afecten las estaciones de trabajo, de tal manera que ayuden a reaccionar y colaborar con el servicio en la contención y erradicación del ciberataque." Es de nuestro entendimiento que los protocolos de respuesta pueden ser entregados en calidad de material de capacitación estructurado (por ejemplo: manuales de procedimientos, guías de respuesta rápida), orientados a preparar y habilitar al personal de Soporte a Usuarios y de Seguridad Informática para actuar de forma coordinada con el equipo del proveedor ante incidentes en estaciones de trabajo, sin que ello implique que el personal del proveedor deba ejecutar directamente los procedimientos sobre los equipos de usuario final. Confirmar si es correcto nuestro entendimiento.

RESPUESTA 47.-

Estimado oferente,

De acuerdo con lo establecido en el apartado GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD, el servicio debe proveer protocolos de respuesta al personal de Soporte a Usuarios y de Seguridad Informática para los casos de incidentes de ciberseguridad que afecten estaciones de trabajo, con el objetivo de facilitar la reacción y colaboración con el servicio durante las etapas de contención y erradicación del ciberataque.

Dichos protocolos podrán ser entregados mediante documentación estructurada, como guías de actuación, procedimientos o material equivalente que permita al personal del SRI conocer las acciones requeridas para la atención coordinada de incidentes.

Sin embargo, la entrega de estos protocolos no limita las responsabilidades del servicio de gestión de incidentes. Cuando la atención de un incidente requiera la intervención del personal del proveedor, este deberá participar en las actividades de gestión conforme a los requerimientos establecidos en la Solicitud de Ofertas (SDO), incluyendo las actividades de análisis, contención, erradicación y acciones posteriores que correspondan.

PREGUNTA 48.-

17. En el documento en la página 156 de licitación Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD", en las etapas de contención y erradicación se indica que el servicio debe: "Definir las acciones necesarias para contener el ataque", "Elaborar la estrategia y la táctica de contención", "Participar en las actividades de contención del incidente coordinadas por el SRI", "Definir las acciones necesarias para evitar que, de repetirse el ataque, este logre ser exitoso", "Documentar las acciones correctivas aplicables a los controles de seguridad y sistemas informáticos institucionales", y "Hacer seguimiento de la aplicación de las acciones correctivas sobre los controles de seguridad y sistemas informáticos institucionales." Es de

nuestro entendimiento que el rol del proveedor en las etapas de contención y erradicación,

en lo que respecta a los sistemas institucionales del SRI que no forman parte de la solución contratada, consistirá en: (a) definir las estrategias, elaborar los planes de acción, documentar las recomendaciones y hacer el seguimiento de su implementación, y (b) ejecutar directamente las acciones de contención y erradicación únicamente sobre los componentes tecnológicos incluidos en la solución contratada; siendo el departamento de

TI del SRI el responsable de ejecutar los cambios operativos en los sistemas institucionales propios, siguiendo las recomendaciones del proveedor. Confirmar si es correcto nuestro entendimiento.

RESPUESTA 48.-

Estimado oferente, es correcta su afirmación. Los numerales 34 y 35 del apartado GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD, se divide la responsabilidad entre la ejecución directa sobre los controles provistos por el servicio y la recomendación/seguimiento sobre sistemas netamente institucionales.

PREGUNTA 49.-

En el documento en la página 156 de licitación Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD", en las

etapas de erradicación y acciones posteriores, y en la Sección VI "ACUERDO DE NIVEL DE SERVICIO" (Tabla 3 - Descripción de niveles de prioridad), se establecen las obligaciones del proveedor en materia de respuesta a incidentes. Es de nuestro entendimiento los siguientes aspectos: (a) Las acciones de remediación y contención del proveedor sobre los sistemas institucionales del SRI que no forman parte de la solución contratada se limitarán a la entrega de recomendaciones técnicas, planes de mitigación y playbooks, siendo el departamento de TI del SRI el único responsable de ejecutar dichos cambios en el entorno de producción. (b) El SRI se compromete a proveer oportunamente los recursos de diagnóstico necesarios tales como registros de eventos ("logs"), capturas de tráfico de red y accesos a sistemas con el único fin de facilitar el análisis técnico del incidente por parte del proveedor, sin utilizarlos para otros propósitos distintos al establecido en el contrato (c) Con el fin de delimitar el alcance operativo del servicio y garantizar una gestión eficiente de los recursos, confirma la entidad que la intervención activa del equipo del proveedor en la gestión de incidentes estará orientada principalmente a incidentes de severidad Alta y Crítica (Prioridades 1 y 2 según la Tabla 3 del Acuerdo de Nivel de Servicio), mientras que los incidentes de impacto medio, bajo e informativo (Prioridades 3 y 4) serán gestionados y descartados en primera instancia por el equipo de TI y de monitoreo interno del SRI. Confirmar si es correcto nuestro entendimiento.

RESPUESTA 49.-

Estimado oferente,

El proveedor no puede delegar exclusivamente la gestión inicial de prioridades menores (impacto medio y bajo) al personal institucional. El servicio MDR contratado debe gestionar y responder a todos los incidentes categorizados en las 4 prioridades listadas, en colaboración con el personal del SRI según lo estipulado.

PREGUNTA 50.-

En el documento en la página 156 de licitación Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD", se indica que el servicio debe entregar "informes de avance de respuesta a incidente" y "informes de cierre de respuesta a incidente" con los contenidos y los plazos establecidos en la Sección VIII "Condiciones Especiales del Contrato" (CGC 17.1: 4 horas hábiles para informes de avance y 2 días hábiles para informes de cierre). Se solicita confirmar que: (a) La obligación de elaborar y entregar informes de avance y de cierre de respuesta a incidente aplica únicamente ante incidentes de ciberseguridad verificados y confirmados, es decir, situaciones que hayan causado un impacto negativo efectivo en la institución, excluyendo los falsos positivos y las alertas sin impacto real. (b) La obligación de entrega de dichos informes está sujeta al Acuerdo de Nivel de Servicio del contrato y que los plazos establecidos (4 horas hábiles y 2 días hábiles respectivamente) inician a partir del momento en que el incidente ha sido formalmente confirmado y clasificado como tal por el equipo de monitoreo del servicio.

RESPUESTA 50.-

Estimado oferente, se confirma el entendimiento planteado en el literal (a). El apartado CONDICIONES GENERALES, numeral 6.c, página 113, define expresamente al “incidente de ciberseguridad” como “una situación causada por un ciberataque (...) que genera un impacto negativo efectivo en la institución”, en contraposición al “evento de ciberseguridad” (numeral 6.b), que “no genera un impacto negativo efectivo en la institución”. En consecuencia, la obligación de elaborar informes de avance y de cierre de respuesta a incidente, prevista en los numerales 34, 35 y 38 del apartado GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD, aplica exclusivamente a las situaciones formalmente clasificadas como incidentes, con impacto negativo efectivo confirmado, excluyendo los falsos positivos y los eventos sin impacto real, los cuales se rigen por el apartado GESTIÓN DE EVENTOS DE CIBERSEGURIDAD. Respecto del literal (b), el plazo para la entrega de informes de “avance de repuesta a incidente” y de “cierre de respuesta a incidente” será conforme lo estipulado en la Sección VIII. Condiciones Especiales de Contrato (CEC) en el apartado DOCUMENTOS Y ACTIVIDADES.

PREGUNTA 51.-

En la Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE EVENTOS DE CIBERSEGURIDAD", página 131, se establecen las actividades relacionadas con el monitoreo, priorización y gestión de eventos de ciberseguridad. En este contexto, se solicita confirmar si el SRI dispone de una matriz vigente de criticidad de activos y servicios, así como del listado de usuarios VIP, cuentas privilegiadas, cuentas administrativas y cuentas de servicio, y si dicha información será proporcionada al SOC adjudicado para la adecuada configuración de la solución, la priorización de eventos y el monitoreo diferenciado, de conformidad con las políticas institucionales de seguridad de la información.

RESPUESTA 51.-

Estimado oferente, el numeral 9 del apartado B. PRESTACIONES DEL SERVICIO DE GESTIÓN DE CIBERDEFENSA (MONITOREO DE AMENAZAS DE CIBERSEGURIDAD), página 130, establece que *“el servicio debe realizar un monitoreo diferenciado en función de: la criticidad del componente tecnológico para la disponibilidad de la operación, la criticidad del componente tecnológico para la confidencialidad de la información, si se trata de un usuario VIP, si se trata de un usuario con accesos privilegiados”*.

No obstante, corresponderá al contratista realizar el levantamiento, identificación, caracterización y clasificación de los activos, servicios, usuarios VIP, cuentas privilegiadas, cuentas administrativas y cuentas de servicio que sean necesarios para la adecuada prestación del servicio, en coordinación con el SRI.

El contratista deberá contemplar dentro de sus actividades de implementación y operación el levantamiento de la información necesaria para configurar adecuadamente el monitoreo, la priorización y el tratamiento diferenciado de los eventos de ciberseguridad.

PREGUNTA 52.-

En la Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE EVENTOS DE CIBERSEGURIDAD", página 131, se establecen las actividades relacionadas con el monitoreo y gestión de eventos de ciberseguridad. En este contexto, se solicita confirmar si el SRI dispone de un inventario actualizado de las estaciones de trabajo y servidores que serán cubiertos por el servicio, incluyendo información como hostname, dirección IP, sistema operativo, ubicación, responsable y criticidad del activo, y si dicha información será proporcionada al SOC adjudicado para la planificación del despliegue, configuración de la solución, monitoreo y priorización de alertas, conforme a las políticas institucionales de seguridad de la información.

RESPUESTA 52.-

Estimado oferente, el SRI suministrará al proveedor adjudicado la información necesaria para garantizar la planificación en el despliegue del software y un monitoreo adecuado. Además, el proveedor será el único responsable de mantener dicha información actualizada durante la ejecución del proyecto, debiendo notificar y gestionar cualquier cambio, ampliación o ajuste necesario para la correcta operatividad del sistema.

PREGUNTA 53.-

En la Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD", se describen las actividades de respuesta, contención, erradicación y recuperación ante incidentes de ciberseguridad. En este contexto, se solicita especificar las acciones de respuesta que el SOC podrá ejecutar directamente y aquellas que requerirán aprobación previa, diferenciando su aplicación sobre estaciones de trabajo, servidores, cuentas de usuario y activos críticos, así como los responsables autorizados para aprobar dichas acciones, conforme a los procedimientos de gestión de cambios y seguridad de la información del SRI.

RESPUESTA 53.-

Estimado oferente, la Solicitud de Ofertas (SDO) no contienen una matriz diferenciada, activo por activo, de las acciones de respuesta que el servicio podrá ejecutar directamente.

No obstante, el numeral 2 del apartado CONDICIONES GENERALES, establece que *“todas las actividades que impliquen cambios en la configuración, en la operación o en el nivel de seguridad informática de los sistemas o componentes instalados o desplegados que*

representen un impacto o afectación a la operación de los servicios o componentes tecnológicos institucionales deberán ser informadas al administrador del contrato y deberán ser aplicadas de manera controlada en coordinación con el personal del SRI”.

PREGUNTA 54.-

En la Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD", página 156, se establecen las actividades relacionadas con la gestión, seguimiento y registro de incidentes de ciberseguridad. En este contexto, se solicita detallar el procedimiento de contingencia que deberá aplicarse en caso de pérdida o indisponibilidad del acceso a la herramienta ITSM institucional por problemas de red, VPN, autenticación, permisos o fallas de la plataforma, incluyendo los canales alternativos de notificación y registro, los responsables de restablecer el servicio, la disponibilidad del soporte correspondiente y el procedimiento para regularizar posteriormente en la herramienta ITSM los casos gestionados por medios alternativos.

RESPUESTA 54.-

Estimado oferente, la Solicitud de Ofertas (SDO) no contienen un procedimiento de contingencia específico para los casos de indisponibilidad de la herramienta ITSM institucional.

El numeral 4 del apartado MONITOREO Y DETECCIÓN, sí establece que “los eventos e incidentes de seguridad deberán ser reportados por los canales electrónicos de comunicación provistos por el contratista, siendo indispensables el correo electrónico y la vía telefónica”. En escenarios de indisponibilidad de la ITSM, se procederá mediante notificaciones formales vía correo electrónico corporativo u otras herramientas de contingencia que se acuerden (llamadas, canales cifrados) con el administrador del contrato.

PREGUNTA 55.-

En la Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "ACUERDO DE NIVEL DE SERVICIO", páginas 142 y 143, se establecen los tiempos de atención, contención, resolución y los niveles de prioridad aplicables al servicio. En este contexto, se solicita confirmar que los tiempos del SLA se suspenderán cuando el contratista se encuentre a la espera de accesos, información, autorizaciones, ejecución de comandos, ventanas de cambio, intervención del personal del SRI o actuaciones de terceros que sean responsabilidad de la Entidad o de terceros ajenos al contratista, y que dichos períodos quedarán debidamente registrados y trazados en la herramienta de gestión de servicios (ITSM) u otro mecanismo de control acordado entre las partes para efectos de la medición y auditoría de los niveles de servicio.

RESPUESTA 55.-

Estimado oferente, en la Solicitud de Ofertas (SDO) no contienen una cláusula expresa de suspensión de los tiempos del Acuerdo de Nivel de Servicio ante la espera de accesos, información, autorizaciones o intervenciones que sean responsabilidad del SRI o de terceros ajenos al contratista. Sin perjuicio de ello, el numeral 2 del apartado GESTIÓN DE EVENTOS (ACUERDO DE NIVEL DE SERVICIO), reconoce que “es responsabilidad del contratista hacer todas las solicitudes y gestiones necesarias de forma oportuna y previsible” para obtener la información requerida, “sin perjuicio del cumplimiento del ACUERDO DE NIVEL DE SERVICIO”.

Los tiempos del SLA se detendrán cuando existan actividades atribuibles al SRI, siempre y cuando se evidencien correctamente en la plataforma ITSM, u otros medios de verificación alternativos.

PREGUNTA 56.-

En la Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "ACUERDO DE NIVEL DE SERVICIO", páginas 142 a 146, se establecen los tiempos de atención, contención y los niveles de prioridad para la gestión de incidentes de ciberseguridad. Asimismo, en la Sección VIII "Condiciones Especiales del Contrato", apartado de multas por incumplimiento de los niveles de servicio, se contemplan penalidades por exceder el tiempo máximo para "resolver incidentes". En este contexto, se solicita aclarar cuál es el tiempo máximo de resolución aplicable para cada nivel de prioridad, considerando que la tabla del SLA establece tiempos de atención y un tiempo de contención, pero no define expresamente un tiempo de resolución para cada prioridad. Adicionalmente, se solicita confirmar que no se aplicarán multas por resolución cuando el cumplimiento de dicha actividad dependa de accesos, autorizaciones, información, ejecución de cambios, ventanas de mantenimiento o cualquier otra intervención que sea responsabilidad del SRI o de terceros ajenos al contratista.

RESPUESTA 56.-

Estimado oferente:

Se aclara que, para **INCIDENTES DE CIBERSEGURIDAD, EVENTOS DE CIBERSEGURIDAD y REQUERIMIENTOS DE SOPORTE TÉCNICO** se aplica los tiempos establecidos para cada prioridad en la “Tabla 2. Escala de tiempo del servicio en función de la prioridad.”, considerando que *“El tiempo de atención se define como el intervalo comprendido entre el momento en que el SRI realiza un reporte de seguridad o requerimiento de soporte y el momento en que se inicia el análisis técnico por parte del personal del servicio. La notificación automática de recepción del mensaje no es aceptada como el inicio del análisis técnico.”*

Por lo tanto, el contratista deberá iniciar la atención de la solicitud realizada por el SRI en los tiempos correspondientes a cada prioridad, dejando constancia de que se inició el análisis técnico con evidencia verificable y auditable que permita determinar la fecha y

hora en la que el personal especializado del servicio inició las actividades de análisis, investigación o gestión correspondientes.

Para tal efecto, será responsabilidad del contratista mantener una bitácora o registro de las actividades realizadas, la cual deberá contener la información y los respaldos, documentos, registros, evidencias técnicas o cualquier otro material pertinente que permita verificar y acreditar de manera objetiva las actividades ejecutadas, así como el cumplimiento de los tiempos establecidos en la tabla de niveles de servicio.

Respecto al tiempo de resolución de incidentes, este deberá entenderse como el tiempo requerido para ejecutar las actividades de contención de ciberamenazas, cuyo plazo máximo establecido es de cuatro (4) horas, conforme a lo indicado en la Tabla 2 del Acuerdo de Nivel de Servicio.

Este tiempo de contención será aplicable de manera uniforme, independientemente de la prioridad asignada al incidente.

Considerando que:

*“El tiempo de contención de ciberamenazas se define como el intervalo comprendido entre la materialización de una ciberamenaza –según los registros de los sistemas y controles involucrados– y el momento en que se logra detener su avance o propagación. La **tabla 2** aplica únicamente a los casos en los que la contención se efectúa sin requerir intervención sobre los sistemas institucionales.”*

En consecuencia, las penalidades previstas en la Sección VIII – Condiciones Especiales del Contrato (CEC) serán aplicadas conforme a las condiciones establecidas, no se establece un tiempo máximo de resolución diferenciado por nivel de prioridad.

PREGUNTA 57.-

En la Sección VI "Requisitos de los Bienes y Servicios Conexos", apartado "GESTIÓN DE EVENTOS DE CIBERSEGURIDAD" y "GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD", páginas 131 y 156, respectivamente, así como en la Sección VIII "Condiciones Especiales del Contrato", donde se establecen los entregables e informes asociados a la prestación del servicio, se solicita aclarar, para efectos de la planificación de recursos y la aplicación de los niveles de servicio y penalidades, si existe un número máximo mensual de informes, reportes o documentos que puedan ser solicitados bajo demanda por la Entidad, así como los plazos de entrega aplicables para cada tipo de documento.

RESPUESTA 57.-

Estimado oferente, no existe un límite para los informes bajo demanda, debido a que los eventos o incidentes de ciberseguridad son impredecibles.

Los plazos para entrega de los DOCUMENTOS Y ACTIVIDADES se encuentran definidos en la Sección VIII. Condiciones Especiales de Contrato (CEC), CGC 17.1

PREGUNTA 58.-

En el documento de licitación página 167 Sección VI "Requisitos de los Bienes y Servicios Conexos", en el apartado "IMPLEMENTACIÓN", etapa de puesta en producción, se indica que el contratista deberá "Desinstalar el agente antivirus (Symantec Endpoint Protection) de las estaciones de trabajo" e "Instalar en las estaciones de trabajo todos los elementos de software de punto final incluidos en la solución." Inmediatamente a continuación, el mismo documento establece: "El SRI no puede garantizar la disponibilidad de un mecanismo de instalación o de desinstalación o de distribución automática de software. Es responsabilidad del contratista el cumplimiento satisfactorio de estas actividades y su consideración en la planificación." Se solicita aclarar: ¿El SRI cuenta actualmente con herramientas de gestión centralizada de software (como Microsoft SCCM/MECM, Group Policy Objects -GPO, Ansible, ¿PDQ Deploy o equivalentes) que el contratista pueda utilizar en coordinación con el personal del SRI para la desinstalación e instalación masiva de software en las 3.031 estaciones de trabajo?

RESPUESTA 58.-

Estimado oferente, el numeral 10.d del apartado IMPLEMENTACIÓN, en su nota aclaratoria, establece expresamente que "el SRI no puede garantizar la disponibilidad de un mecanismo de instalación o de desinstalación o de distribución automática de software", siendo "responsabilidad del contratista el cumplimiento satisfactorio de estas actividades y su consideración en la planificación".

PREGUNTA 59.-

En el documento de licitación en la página 167 Sección VI "Requisitos de los Bienes y Servicios Conexos", en el apartado "IMPLEMENTACIÓN", etapa de puesta en producción, se indica que el contratista deberá "Desinstalar el agente antivirus (Symantec Endpoint Protection) de las estaciones de trabajo" e "Instalar en las estaciones de trabajo todos los elementos de software de punto final incluidos en la solución." Inmediatamente a continuación, el mismo documento establece: "El SRI no puede garantizar la disponibilidad de un mecanismo de instalación o de desinstalación o de distribución automática de software. Es responsabilidad del contratista el cumplimiento satisfactorio de estas actividades y su consideración en la planificación." Debido a que el SRI no puede garantizar la disponibilidad de un mecanismo de instalación o de desinstalación o de distribución automática de software se solicita se amplie el plazo de despliegue a al menos 150 días calendario en lugar de los 90 días calendario indicados en el documento.

RESPUESTA 59.-

Estimado oferente, el plazo para la implementación del software y del servicio será de hasta 90 días calendario". No se acepta extender el plazo de implementación; la planificación operativa del oferente debe prever este volumen dentro del marco contractual fijado.

PREGUNTA 60.-

En el documento de licitación en la página 167 Sección VI "Requisitos de los Bienes y Servicios Conexos", en el apartado "IMPLEMENTACIÓN" es de nuestro entendimiento de que si el incumplimiento de despliegue de la solución en el tiempo determinado es atribuible al SRI ya sea por falta de disponibilidad de ventanas de mantenimiento, etc. Dichos tiempos no serán atribuibles al contratante y no generarán multas. Por favor confirmar si es correcto nuestro entendimiento.

RESPUESTA 60.-

Estimado oferente,

Los tiempos perdidos por demoras directamente imputables al contratante, documentadas pertinentemente, no afectarán al plazo del contratista ni generará imposición de multas, requiriéndose la validación y aprobación del Administrador del Contrato.

PREGUNTA 61.-

En el documento "DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios", en la sección "C. Preparación de las Ofertas", numeral "IAO 11.1", entendiéndose que la documentación de respaldo de las especificaciones técnicas de los fabricantes es en idioma inglés, éstos si serán tomados en consideración para justificar el cumplimiento de las especificaciones técnicas, confirmar si nuestro entendimiento es correcto.

RESPUESTA 61.-

Estimado oferente,

La documentación técnica del fabricante (datasheets) deberá contar con su respectiva traducción fidedigna al idioma español, y el oferente deberá garantizar que las traducciones de los términos técnicos sean gramaticalmente correctas, a fin de asegurar un adecuado entendimiento por parte del Comité Técnico de Evaluación y Selección.

PREGUNTA 62.-

En el documento "DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios", en "1. LISTA DE SERVICIOS Y CRONOGRAMA DE ENTREGAS", para el "Componente de Software: Endpoint Detection and Response (EDR)" en "Fecha límite de entrega" se indica "El plazo para la activación del licenciamiento del componente de software será de hasta 15 días calendario contados a partir del día siguiente a la fecha de suscripción del contrato", entendemos que el plazo citado es para la entrega y activación de las suscripciones y que el proceso de despliegue e implementación será acordado entre las partes y será de hasta 90 días laborales, confirmar si nuestro entendimiento es correcto.

RESPUESTA 62.-

Estimado oferente,

Conforme a la subsección 1. LISTA DE SERVICIOS Y CRONOGRAMA DE ENTREGAS, el plazo de 15 días calendario corresponde efectivamente a la activación del licenciamiento del componente de software, contados a partir del día siguiente a la suscripción del contrato.

No obstante, el plazo de implementación previsto en Sección VIII. Condiciones Especiales de Contrato (CEC) de la Solicitud de Ofertas (SDO) se establece en días calendario y no en días laborales, contados a partir del día siguiente a la fecha de activación del licenciamiento.

PREGUNTA 63.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, en “1. LISTA DE SERVICIOS Y CRONOGRAMA DE ENTREGAS”, para el “Componente de Software: Network Detection and Response (NDR)” en “Fecha límite de entrega” se indica “El plazo para la activación del licenciamiento del componente de software será de hasta 15 días calendario contados a partir del día siguiente a la fecha de suscripción del contrato”, entendemos que el plazo citado es para la entrega y activación de las suscripciones y que el proceso de despliegue e implementación será acordado entre las partes y será de hasta 90 días laborales, confirmar si nuestro entendimiento es correcto.

RESPUESTA 63.-

Estimado oferente,

Conforme a la subsección 1. LISTA DE SERVICIOS Y CRONOGRAMA DE ENTREGAS, el plazo de 15 días calendario corresponde efectivamente a la activación del licenciamiento del componente de software, contados a partir del día siguiente a la suscripción del contrato.

No obstante, el plazo de implementación previsto en Sección VIII. Condiciones Especiales de Contrato (CEC) de la Solicitud de Ofertas (SDO) se establece en días calendario y no en días laborales, contados a partir del día siguiente a la fecha de activación del licenciamiento.

PREGUNTA 64.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, en la “Tabla 6. Cantidad de dispositivos a ser cubiertos por el servicio”, se solicita al SRI detalle sistema operativo juntamente con la versión que actualmente está en operación con el fin de determinar compatibilidad del agente.

RESPUESTA 64.-

Estimado oferente,

En la tabla 6., se detalla la cantidad de dispositivos a ser cubiertos por el servicio, adicional en el numeral 5 del apartado EDR se proporcionan las versiones que deben ser soportadas:

- *“Estaciones Windows [de escritorio y portátiles]: Windows 10, 11 y superiores;*
- *Estaciones macOS [de escritorio y portátiles]: macOS 13, 14, 15 y superiores;*
- *Servidores Windows: Windows Server 2016, 2019, 2022, 2025 y superiores;*
Servidores Linux: RHEL 7.4 , 8, 9 y superiores.”

PREGUNTA 65.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, en la “Tabla 8. Estimación de tráfico de los segmentos de red a ser monitoreados en el centro de datos de producción.”, entendemos que el SRI entregará el tráfico agregado a monitorear en dos puertos espejos (port mirror) de 10 Gbps y que tienen disponibilidad de puertos y sfp para realizar las conexiones hacia el equipo NDR y monitorear el tráfico, confirmar si nuestro entendimiento es correcto o caso contrario detallar como se va a entregar el tráfico a ser monitoreado.

RESPUESTA 65.-

Estimado oferente, no se confirma el entendimiento en los términos planteados. La Tabla 8, páginas 110-111, detalla seis (6) segmentos de red diferenciados (DMZ de servicios externos, DMZ de servicios internos, red de acceso a Internet, enlace principal y secundario entre agencias y centro de datos, y enlace entre centros de datos), cada uno con su propio “control de acceso”, “tipo de punto de acceso” (Ethernet 10Gbps Base-SR LC SFP+) y tipo de encapsulamiento, sin que en la Solicitud de Ofertas (SDO) indique que el tráfico de todos estos segmentos se entregará agregado en únicamente dos puertos espejo de 10 Gbps. La determinación del número exacto de puntos de acceso físico y su disposición corresponde al diseño de la solución que el oferente deberá desarrollar durante la etapa de preparación de la implementación (numeral 8, página 134), en coordinación con el personal del SRI, considerando la necesidad de visibilidad sobre cada uno de los segmentos detallados en la Tabla 8 y en el numeral 35 de la función NDR.

PREGUNTA 66.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, en la “Tabla 11. Detalle de los componentes de la infraestructura SDWAN del SRI”, entendemos que la tabla hace referencia a las versiones de los controles de ciberseguridad disponibles para integrarse y que los datos de registros de eventos (“logs”) están incluidos en la Tabla 9, confirmar si nuestro entendimiento es correcto, o caso contrario indicar la cantidad de eventos (“logs”) que registran actualmente las soluciones.

RESPUESTA 66.-

Estimado oferente, se confirma su entendimiento.

PREGUNTA 67.-

En el documento "DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios", sección "BIENES REQUERIDOS" componente "ENDPOINT DETECTION AND RESPONSE (EDR)" se indica en el numeral 11 "El componente EDR debe detectar y bloquear el uso de herramientas de ataque (ej. Metasploit, Empire, Cobalt).", entendemos que lo que busca el SRI es que el componente EDR debe detectar exploits y ataques como los ejecutados por herramientas de explotación usando métodos avanzados de detección de comportamientos anómalos asociados a técnicas de MITRE ATT&CK, confirmar si nuestro entendimiento es correcto.

RESPUESTA 67.-

Estimado oferente, no es correcto su entendimiento, por favor remítase a lo solicitado en el requerimiento:

"El componente EDR debe detectar y bloquear el uso de herramientas de ataque (ej. Metasploit, Empire, Cobalt)."

PREGUNTA 68.-

Crecimiento del tráfico Se indica que el tráfico puede crecer un 5 % anual. Solicitamos confirmar si el dimensionamiento mínimo del NDR debe contemplar desde el inicio el tráfico actual más el crecimiento acumulado del 5 % anual durante los tres años, sin costos adicionales para el SRI.

RESPUESTA 68.-

Estimado oferente, su entendimiento es correcto. El dimensionamiento mínimo de la solución NDR deberá contemplar desde el inicio el tráfico actual indicado en la Solicitud de Ofertas (SDO), más el crecimiento acumulado del 5 % anual durante los tres años de vigencia del servicio, sin que esto implique costos adicionales para el SRI.

PREGUNTA 69.-

Dimensionamiento del NDR El documento solicita un equipo principal en Quito y otro alterno en Guayaquil, pero presenta las mediciones detalladas únicamente para el centro principal e indica que el alterno debe considerar "condiciones equivalentes". Solicitamos proporcionar para cada centro de datos:

- Tráfico promedio y pico por segmento.
- Número de interfaces que se deben monitorear.
- Velocidad y tipo de cada interfaz.
- Cantidad de puertos requeridos.

- Arquitectura de SPAN, TAP o packet broker disponible.
- Requerimientos de alta disponibilidad.
- Espacio de rack, energía y conectividad disponibles.

Asimismo, sírvase confirmar si el equipo alternativo deberá tener exactamente la misma capacidad de procesamiento que el equipo principal.

RESPUESTA 69.-

Estimado oferente, la *“Tabla 8. Estimación de tráfico de los segmentos de red a ser monitoreados en el centro de datos de producción.”*, detalla el tráfico estimado por segmento para el centro de datos principal, precisando en su Nota 3 que *“para la protección del centro de datos alternativo se deben considerar condiciones equivalentes a las del principal”*, y en su Nota 1 que *“el tráfico estimado corresponde a valores pico registrados”*.

Se confirma que el equipo principal y el equipo alternativo deberá tener la misma capacidad. Se confirma que el tráfico puede ser entregado utilizando puertos mirror (SPAN/RSPAN). Con respecto a la alta disponibilidad, el oferente debe garantizar la continuidad del servicio.

La información adicional que se requiera por el oferente que resulte adjudicado será proporcionado por el Administrador de Contrato en la fase correspondiente.

PREGUNTA 70.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “ENDPOINT DETECTION AND RESPONSE (EDR)” se indica en el numeral 9 “El componente EDR debe agrupar los eventos e incidentes de seguridad por nivel de criticidad, en base al análisis de inteligencia artificial (AI) y de aprendizaje automático (ML).”, entendemos que para cumplir con lo solicitado la tecnología debe correlacionar y agrupar automáticamente los eventos relacionados dentro de una misma cadena de ataque, asignando un nivel de criticidad/prioridad basado en IA que reduzca el ruido de alertas individuales y facilite el triage, confirmar si nuestro entendimiento es correcto.

RESPUESTA 70.-

La solución propuesta deberá cumplir íntegramente con lo establecido en el numeral 9 del componente ENDPOINT DETECTION AND RESPONSE (EDR), que establece que el componente deberá *“agrupar los eventos e incidentes de seguridad por nivel de criticidad, en base al análisis de inteligencia artificial (AI) y de aprendizaje automático (ML)”*.

En este sentido, si bien en su consulta se hace referencia a la correlación y agrupación automática de eventos relacionados y a la asignación de un nivel de criticidad basado en IA, no se especifica expresamente que dicha agrupación y asignación de criticidad se

realice con base en el análisis conjunto de inteligencia artificial (AI) y aprendizaje automático (ML), conforme lo requerido en el numeral 9.

Por lo tanto, no es posible confirmar que el entendimiento planteado en su consulta satisfaga íntegramente el requerimiento. La solución ofertada deberá demostrar el cumplimiento de la totalidad de las características establecidas en el numeral 9, incluyendo expresamente el uso de AI y ML para la agrupación de los eventos e incidentes de seguridad por nivel de criticidad.

PREGUNTA 71.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “ENDPOINT DETECTION AND RESPONSE (EDR)” se indica en el numeral 12 “El componente EDR debe impedir el robo de contraseña a partir de la lectura de la memoria RAM”, entendemos que para cumplir con lo solicitado la tecnología debe detectar y bloquear técnicas de extracción de credenciales desde la memoria de procesos del sistema operativo (por ejemplo, volcado de LSASS mediante herramientas tipo Mimikatz), confirmar si nuestro entendimiento es correcto.

RESPUESTA 71.-

Estimado oferente,

La solución propuesta deberá cumplir íntegramente con lo establecido en el numeral correspondiente del componente ENDPOINT DETECTION AND RESPONSE (EDR), que requiere que el componente *“impida el robo de contraseña a partir de la lectura de la memoria RAM”*.

Si bien en su consulta se hace referencia a la detección y bloqueo de técnicas de extracción de credenciales desde la memoria de procesos del sistema operativo, incluyendo como ejemplo el volcado de LSASS mediante herramientas como Mimikatz, no se especifica expresamente que esta capacidad permita impedir el robo de contraseñas mediante la lectura de la memoria RAM, conforme al requerimiento establecido.

En consecuencia, no es posible confirmar que el entendimiento planteado satisfaga íntegramente el requerimiento. La solución ofertada deberá garantizar que el componente EDR sea capaz de detectar y prevenir el acceso no autorizado a información de credenciales contenida en la memoria RAM.

PREGUNTA 72.-

41. En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “ENDPOINT DETECTION AND RESPONSE (EDR)” se indica en el numeral 13 “El componente EDR debe permitir crear una lista blanca de archivos o directorios para exceptuar la inspección”, entendemos que para cumplir con lo solicitado la consola de administración debe permitir configurar

exclusiones de rutas, procesos o certificados específicos, de forma centralizada y aplicable por grupo de políticas, confirmar si nuestro entendimiento es correcto.

RESPUESTA 72.-

Estimado oferente, se confirma el entendimiento. El numeral 13, componente EDR, exige la capacidad de “crear una lista blanca de archivos o directorios para exceptuar la inspección”, funcionalidad que, conforme a prácticas estándar de administración de soluciones EDR, se gestiona mediante la consola de administración centralizada.

PREGUNTA 73.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “ENDPOINT DETECTION AND RESPONSE (EDR)” se indica en el numeral 15 “El componente EDR debe impedir la explotación de vulnerabilidades de sistemas operativos y aplicaciones que incluso se encuentren sin el parche de seguridad instalado.”, entendemos que para cumplir con lo solicitado la tecnología debe contar con un módulo de protección contra explotación de memoria que bloquee las técnicas genéricas de explotación (corrupción de memoria, ROP, inyección de shellcode) independientemente de si el sistema operativo o la aplicación afectada cuenta o no con el parche de seguridad correspondiente instalado, protegiendo así los activos con parchado pendiente, confirmar si nuestro entendimiento es correcto.

RESPUESTA 73.-

Estimado oferente, se confirma el entendimiento. El numeral 15, componente ENDPOINT DETECTION AND RESPONSE (EDR), exige que el componente *“impida la explotación de vulnerabilidades de sistemas operativos y aplicaciones que incluso se encuentren sin el parche de seguridad instalado”*

PREGUNTA 74.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “ENDPOINT DETECTION AND RESPONSE (EDR)” se indica en el numeral 17 “El componente EDR debe detectar y prevenir malware conocido y desconocido o de día cero.”, entendemos que para cumplir con lo solicitado la tecnología debe combinar un motor de IA, que evalúa archivos antes de su ejecución para predecir si son maliciosos sin depender de firmas, con un motor de comportamiento que detiene malware desconocido en tiempo de ejecución, cubriendo tanto amenazas catalogadas como variantes nunca antes vistas, confirmar que nuestro entendimiento es correcto.

RESPUESTA 74.-

Estimado oferente,

Por favor remitirse al requerimiento establecido en el numeral 1 de ENDPOINT

DETECTION AND RESPONSE (EDR):

“El servicio debe incluir un componente de Endpoint Detection and Response (EDR) basado en inteligencia artificial (AI) y aprendizaje automático (ML) que debe cumplir todas las especificaciones técnicas de este apartado.”

Y al numeral 17 del mismo apartado:

“El componente EDR debe detectar y prevenir malware conocido y desconocido o de día cero”

PREGUNTA 75.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “ENDPOINT DETECTION AND RESPONSE (EDR)” se indica en el numeral 18 “El componente EDR debe detectar y prevenir ataques sin archivos (“file-less attacks”)", entendemos que para cumplir con lo solicitado mediante técnicas de análisis de comportamiento anómalo debe identificar y detener técnicas de ataque que se ejecutan únicamente en memoria o mediante intérpretes legítimos del sistema operativo (PowerShell, WMI, macros), sin dejar un archivo malicioso persistente en disco que pueda analizarse por firma. Confirmar si nuestro entendimiento es correcto.

RESPUESTA 75.-

Estimado oferente,

Por favor remitirse al requerimiento establecido en el numeral 1 de ENDPOINT DETECTION AND RESPONSE (EDR):

“El servicio debe incluir un componente de Endpoint Detection and Response (EDR) basado en inteligencia artificial (AI) y aprendizaje automático (ML) que debe cumplir todas las especificaciones técnicas de este apartado.”

Y al numeral 18 del mismo apartado:

“El componente EDR debe detectar y prevenir ataques sin archivos (“file-less attacks”).”

PREGUNTA 76.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “ENDPOINT DETECTION AND RESPONSE (EDR)” se indica en el numeral 19 “El componente EDR debe detectar y bloquear intentos de escalamiento de privilegios, inclusive los que se realizan a nivel de kernel.”, entendemos que para cumplir con lo solicitado la tecnología debe supervisar llamadas al sistema y operaciones a nivel de kernel para identificar patrones de escalamiento de privilegios (por ejemplo, abuso de tokens, explotación de controladores vulnerables), deteniendo la cadena de ataque antes de que el proceso obtenga privilegios elevados de forma no autorizada, confirmar si nuestro entendimiento es correcto.

RESPUESTA 76.-

Estimado oferente,

Por favor remitirse al requerimiento establecido en el numeral 1 de ENDPOINT DETECTION AND RESPONSE (EDR):

“El servicio debe incluir un componente de Endpoint Detection and Response (EDR) basado en inteligencia artificial (AI) y aprendizaje automático (ML) que debe cumplir todas las especificaciones técnicas de este apartado.”

Y al numeral 19 del mismo apartado:

“El componente EDR debe detectar y bloquear intentos de escalamiento de privilegios, inclusive los que se realizan a nivel de kernel.”

PREGUNTA 77.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “ENDPOINT DETECTION AND RESPONSE (EDR)” se indica en el numeral 20 “El componente EDR debe coleccionar al menos la siguiente información de telemetría de equipos Windows: proceso ejecutado (tiempo de inicio y tamaño del archivo); creación/escritura/renombramiento/eliminación/modificación de archivos; archivos DLL (ruta, dirección base, PID, tamaño, firma, hashes MD5/SHA256); creación y terminación de procesos (proceso padre, PID, ruta, argumentos, hashes, firma digital); información de red (IP, puertos, estado, protocolo, DNS, HTTP); registros de Windows (creación, modificación, eliminación, restauración); sesiones del sistema operativo (inicio/cierre de sesión, conexión/desconexión).”, entendemos que para cumplir con lo solicitado el agente debe recolectar de forma nativa y continua la telemetría y que las mismas se visualizarán si éstas están disponibles y son ejemplos de la telemetría que podría visualizarse, confirmar si nuestro entendimiento es correcto.

RESPUESTA 77.-

Estimado oferente,

Por favor remitirse al requerimiento establecido en el numeral 1 de ENDPOINT DETECTION AND RESPONSE (EDR):

“El servicio debe incluir un componente de Endpoint Detection and Response (EDR) basado en inteligencia artificial (AI) y aprendizaje automático (ML) que debe cumplir todas las especificaciones técnicas de este apartado.”

Y al numeral 20 del mismo apartado:

“El componente EDR debe coleccionar al menos la siguiente información de telemetría de equipos Windows:

- *Proceso ejecutado, incluyendo el tiempo de inicio y el tamaño del archivo asociado.*
- *Actividades de creación, escritura, renombramiento, eliminación, modificación de archivos.*

- Archivos DLL: ruta completa, dirección base, id del proceso, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL.
- Creación y terminación de los procesos, incluyendo los siguientes atributos: nombre del proceso padre, ID del proceso, ruta completa, argumentos de la línea de comando, valores hash, detalles de la firma digital.
- Información de red: dirección IP, puerto origen y destino, estado de conexión, protocolo usado (TCP, UDP), consultas DNS, conexiones Web (HTTP).
- Acciones sobre los registros de Windows: Creación, modificación, eliminación, adición, restauración y guardado de llaves del registro.
- Sesiones del sistema operativo: inicio de sesión, cierre de sesión, conexión y desconexión.”

PREGUNTA 78.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “ENDPOINT DETECTION AND RESPONSE (EDR)” se indica en el numeral 20 “El componente EDR debe coleccionar al menos la siguiente información de telemetría de equipos Linux y macOS: información de procesos ('daemons'): inicio/detención, PID padre, PID, hashes (MD5, SHA256); argumentos de línea de comando; información de red (IP, puertos, estado, protocolo TCP/UDP).”, entendemos que para cumplir con lo solicitado el agente debe recolectar de forma nativa y continua la telemetría y que las mismas se visualizarán si éstas están disponibles y son ejemplos de la telemetría que podría visualizarse no mandatorios, confirmar si nuestro entendimiento es correcto.

RESPUESTA 78.-

Estimado oferente,

Por favor remitirse al requerimiento establecido en el numeral 1 de ENDPOINT DETECTION AND RESPONSE (EDR):

“El servicio debe incluir un componente de Endpoint Detection and Response (EDR) basado en inteligencia artificial (AI) y aprendizaje automático (ML) que debe cumplir todas las especificaciones técnicas de este apartado.”

Y al numeral 20 del mismo apartado:

“El componente EDR debe coleccionar al menos la siguiente información de telemetría de equipos Windows:

- Proceso ejecutado, incluyendo el tiempo de inicio y el tamaño del archivo asociado.
- Actividades de creación, escritura, renombre, eliminación, modificación de archivos.
- Archivos DLL: ruta completa, dirección base, id del proceso, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL.
- Creación y terminación de los procesos, incluyendo los siguientes atributos:

nombre del proceso padre, ID del proceso, ruta completa, argumentos de la línea de comando, valores hash, detalles de la firma digital.

- *Información de red: dirección IP, puerto origen y destino, estado de conexión, protocolo usado (TCP, UDP), consultas DNS, conexiones Web (HTTP).*
- *Acciones sobre los registros de Windows: Creación, modificación, eliminación, adición, restauración y guardado de llaves del registro.*
- *Sesiones del sistema operativo: inicio de sesión, cierre de sesión, conexión y desconexión.”*

PREGUNTA 79.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “ENDPOINT DETECTION AND RESPONSE (EDR)” se indica en el numeral 22 “El componente EDR debe integrarse con el sistema de directorio Microsof del SRI (ver INFRAESTRUCTURA ACTUAL) para la aplicación y organización de las políticas.”, se solicita a SRI indique el sistema operativo y versión de los controladores de dominio, el nivel funcional del dominio y bosque, la estructura de dominios o bosques involucrados, la versión o modalidad de Microsof Entra ID utilizada, y si existe sincronización entre Active Directory local y Entra ID. En caso de existir sincronización, además se debe indicar la herramienta o mecanismo utilizado.

RESPUESTA 79.-

Estimado oferente,

Por favor se solicita remitirse a lo establecido en el apartado INFRAESTRUCTURA ACTUAL, en caso de ser necesaria información adicional la misma será proporcionada al oferente que resulte adjudicado.

PREGUNTA 80.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “ENDPOINT DETECTION AND RESPONSE (EDR)” se indica en el numeral 23 “El componente EDR debe identificar el comportamiento del equipo de punto final al menos en base a la siguiente información: memoria RAM instalada, tipo de equipo, modelo, procesador, almacenamiento, sistema operativo, aplicaciones instaladas, usuarios que han iniciado sesión, carpetas compartidas [Windows], servicios [Windows], demonios [Linux/macOS].”, entendemos que para cumplir con lo solicitado el agente debe generar y mantener actualizado un inventario detallado de hardware y software de cada endpoint y que la información indicada son ejemplos y no mandatorios, confirmar si nuestro entendimiento es correcto.

RESPUESTA 80.-

Estimado oferente,

Por favor remitirse al requerimiento establecido en el numeral 1 de ENDPOINT

DETECTION AND RESPONSE (EDR):

“El servicio debe incluir un componente de Endpoint Detection and Response (EDR) basado en inteligencia artificial (AI) y aprendizaje automático (ML) que debe cumplir todas las especificaciones técnicas de este apartado.”

Y al numeral 23 del mismo apartado:

“El componente EDR debe identificar el comportamiento del equipo de punto final al menos en base a la siguiente información:

- Memoria RAM instalada,
- Tipo de equipo,
- Modelo,
- Procesador,
- Almacenamiento,
- Sistema operativo,
- Aplicaciones instaladas,
- Usuarios que ha iniciado sesión,
- Carpetas compartidas [en equipos Windows],
- Servicios [en equipos Windows],
- Demonios [en equipos Linux/macOS].”

Hay que considerar que los requisitos establecidos en la Solicitud de la Oferta (SDO) no son opcionales, responden a una necesidad institucional.

PREGUNTA 81.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “ENDPOINT DETECTION AND RESPONSE (EDR)” se indica en el numeral 16 “El componente EDR debe impedir la explotación de vulnerabilidades de día cero, es decir, inclusive aquellas para las cuales aún no existe un CVE. ”entendemos que para cumplir con lo solicitado la protección debe fundamentarse en el análisis de comportamiento en tiempo de ejecución y no en bases de firmas o CVE conocidos, de forma que las técnicas de explotación de día cero se detengan por su comportamiento anómalo (por ejemplo, ejecución de código desde regiones de memoria no autorizadas) antes de que exista un CVE publicado. Solicitamos que la entidad contratante confirme la aceptación de este mecanismo de cumplimiento”,

RESPUESTA 81.-

Estimado oferente,

Por favor remitirse al requerimiento establecido en el numeral 1 de ENDPOINT DETECTION AND RESPONSE (EDR):

“El servicio debe incluir un componente de Endpoint Detection and Response (EDR) basado en inteligencia artificial (AI) y aprendizaje automático (ML) que debe cumplir todas las

especificaciones técnicas de este apartado.”

Y al numeral 16 del mismo apartado:

“El componente EDR debe impedir la explotación de vulnerabilidades de día cero, es decir, inclusive aquellas para las cuales aún no existe un CVE.”

PREGUNTA 82.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “GESTIÓN DE AMENAZAS DE IDENTIDAD” en el numeral 64 se solicita: “La gestión de amenazas de identidad debe ser capaz de incorporar al menos la siguiente información de registros de eventos desde el sistema de Active Directory del SRI: Eventos de inicio de sesión de red” Hacemos notar que el Directorio Activo no registra la información completa de los eventos de inicio de sesión de red (detalles de uso de recursos compartidos) por lo tanto entendemos que lo solicitado será exigible si el sistema origen proporciona este detalle. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 82.-

Estimado oferente, se confirma el entendimiento. En el numeral 64 de la Sección 6, componente GESTIÓN DE AMENAZAS DE IDENTIDAD, la función "debe ser capaz de incorporar al menos la siguiente información de registros". La herramienta consumirá la telemetría hasta el nivel de granularidad configurado o disponible desde el propio sistema de control (Active Directory).

PREGUNTA 83.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “GESTIÓN DE AMENAZAS DE IDENTIDAD” en el numeral 67 se solicita: “La gestión de amenazas de identidad debe contar con la capacidad de identificar las amenazas de identidad en escenarios tales como conexiones de escritorio remoto, conexiones VPN de acceso remoto y de inicio de sesión local.”

Hacemos notar que el ITDR con solo la información del Directorio Activo no puede identificar conexiones que se realizan a través de VPN y RDP ya que esta información se registra en otros componentes como Firewalls, Gateway VPN y servidores, por lo tanto, según nuestro entendimiento se permitirá cumplir este requisito referenciando a otro componente como INTELIGENCIA UNIFICADA DE CIBERDEFENSA. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 83.-

Estimado oferente,

El numeral 58 de la Sección 6, componente GESTIÓN DE AMENAZAS DE IDENTIDAD, establece que:

“Las especificaciones técnicas de la función de Gestión de Amenazas de Identidad pueden ser implementadas como un componente independiente o como la funcionalidad de uno o varios de los componentes tecnológicos incluidos en la solución contratada. Para este efecto puede utilizar la telemetría de punto final o de red según corresponda a cada caso.”

PREGUNTA 84.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “GESTIÓN DE AMENAZAS DE IDENTIDAD” en el numeral 72 se solicita: “La gestión de amenazas de identidad debe hacer seguimiento de las actividades de los usuarios desde el inicio de las sesiones hasta su cierre.”

Hacemos notar que el ITDR con solo la información del Directorio Activo recibe el registro de actividades de inicio de sesión, cambio de contraseña y cierre, no otro tipo de actividades. Si se desea mayor alcance se requiere de otros componentes como del EDR por lo tanto entendemos que el SRI está solicitando el seguimiento de las actividades que puede brindar el Directorio Activo y de no ser así se puede hacer uso de otros componentes. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 84.-

Estimado oferente,

El numeral 58 de la Sección 6, componente GESTIÓN DE AMENAZAS DE IDENTIDAD, establece que:

“Las especificaciones técnicas de la función de Gestión de Amenazas de Identidad pueden ser implementadas como un componente independiente o como la funcionalidad de uno o varios de los componentes tecnológicos incluidos en la solución contratada. Para este efecto puede utilizar la telemetría de punto final o de red según corresponda a cada caso.”

PREGUNTA 85.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “GESTIÓN DE AMENAZAS DE IDENTIDAD” en el numeral 75 se solicita: “La gestión de amenazas de identidad debe hacer seguimiento de los accesos RDP y SSH que realizan los usuarios.” Hacemos notar que el ITDR con solo la información del Directorio Activo no puede hacer seguimiento de las sesiones RDP y SSH ya que esta información no queda registrada en este control de seguridad, para este fin se necesitan otros componentes como el EDR y el NDR con las limitantes dependiendo si se puede abrir la comunicación (SSH) que estén cifradas. Por lo tanto, entendemos que este requerimiento puede cumplirse con la referencia a otros componentes y no solo con el ITDR. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 85.-

Estimado oferente,

El numeral 58 de la Sección 6, componente GESTIÓN DE AMENAZAS DE IDENTIDAD, establece que:

“Las especificaciones técnicas de la función de Gestión de Amenazas de Identidad pueden ser implementadas como un componente independiente o como la funcionalidad de uno o varios de los componentes tecnológicos incluidos en la solución contratada. Para este efecto puede utilizar la telemetría de punto final o de red según corresponda a cada caso.”

PREGUNTA 86.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “GESTIÓN DE AMENAZAS DE IDENTIDAD” en el numeral 90 se solicita: “Para determinar anomalías de comportamiento, la gestión de amenazas de identidad debe discriminar las conexiones que se realizan a través de VPN de acceso remoto y detectar accesos sospechosos.” Hacemos notar que el ITDR con solo la información del Directorio Activo no puede identificar conexiones que se realizan a través de VPN y de acceso remoto ya que esta información se registra en otros componentes como Firewalls, servidores, por lo tanto, según nuestro entendimiento se permitirá cumplir este requisito referenciando a otro componente como INTELIGENCIA UNIFICADA DE CIBERDEFENSA. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 86.-

Estimado oferente,

El numeral 58 de la Sección 6, componente GESTIÓN DE AMENAZAS DE IDENTIDAD, establece que:

“Las especificaciones técnicas de la función de Gestión de Amenazas de Identidad pueden ser implementadas como un componente independiente o como la funcionalidad de uno o varios de los componentes tecnológicos incluidos en la solución contratada. Para este efecto puede utilizar la telemetría de punto final o de red según corresponda a cada caso.”

PREGUNTA 87.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 97 se solicita: “El componente central de inteligencia unificada de ciberdefensa debe garantizar la retención de los datos de acuerdo con la siguiente priorización: Datos acopiados: un (1) mes...” Según nuestro entendimiento esto significa que el componente citado debe garantizar una retención de los logs en su formato original (raw logs) recibidos de las fuentes del SRI, por

un mes accesible desde la consola. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 87.-

Estimado oferente, se confirma el entendimiento. El numeral 97 de la Sección 6, componente INTELIGENCIA UNIFICADA DE CIBERDEFENSA, establece que el componente “debe garantizar la retención de los datos de acuerdo con la siguiente priorización: Datos acopiados: un (1) mes; Datos producidos por el análisis: seis (6) meses”.

PREGUNTA 88.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 97 se solicita: “El componente central de inteligencia unificada de ciberdefensa debe garantizar la retención de los datos de acuerdo con la siguiente priorización: ... Datos producidos por el análisis: seis (6) meses.” Según nuestro entendimiento esto significa que la solución debe mantener los eventos procesados y enriquecidos, recibidos de las fuentes del SRI, por seis (6) meses accesibles desde la consola. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 88.-

Estimado oferente,

El numeral 97 de la Sección 6, solicita:

“El componente central de inteligencia unificada de ciberdefensa debe garantizar la retención de los datos de acuerdo con la siguiente priorización:

- *Datos acopiados: un (1) mes,*
- *Datos producidos por el análisis: seis (6) meses.”*

Siendo los “*datos producidos por el análisis*” aquellos datos producidos por la solución ofertada luego del análisis realizado.

PREGUNTA 89.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 107 se solicita. “El servicio debe tener activadas tanto las fuentes Cyber Threat Intelligence (CTI) de los propios fabricantes de los componentes tecnológicos incluidos, así como al menos una fuente CTI externa que sea de terceros (distintos a dichos fabricantes)”.

Según nuestro entendimiento no es mandatorio que el servicio incluya Fuentes de Cyber Threat Intelligence de todos los fabricantes de los componentes ya que por ejemplo algunos fabricantes de NDR no basan su capacidad de detección de fuentes de inteligencia (Darktrace) y por lo tanto no mantienen una fuente de inteligencia propia. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 89.-

Estimado oferente, es mandatorio que los componentes tecnológicos que conforman el servicio **“INTELIGENCIA UNIFICADA DE CIBERDEFENSA”** tengan activadas fuentes CTI propias del fabricante, así como al menos una fuente CTI externa que sea de terceros (distintos a dichos fabricantes).

PREGUNTA 90.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 108 se solicita. “El componente central de inteligencia unificada de ciberdefensa debe generar indicadores de compromiso (IOC) en base a las amenazas detectadas en el sistema”.

Según nuestro entendimiento con este requerimiento se está solicitando que la solución identifique y documente el hallazgo de Indicadores de Compromiso cuando se detecte una amenaza. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 90.-

Estimado oferente, el componente indicado debe generar indicadores de compromiso que serán utilizados posteriormente para detener de manera proactiva ataques a los sistemas.

PREGUNTA 91.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 112 se solicita. “El componente central de inteligencia unificada de ciberdefensa debe integrarse de forma nativa con las funciones y componentes tecnológicos incluidos en la solución contratada, listados a continuación, para acopiar e incorporar en su análisis la información de telemetría de estos”. Según nuestro entendimiento por “integrarse de forma nativa” se refieren a que el componente de Inteligencia Unificada de Ciberdefensa debe tener una integración ya desarrollada con los otros componentes cuando son de otra marca, por ejemplo, si el NDR fuera de otra marca a la solución de INTELIGENCIA UNIFICADA DE CIBERDEFENSA”. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 91.-

Estimado oferente, las integraciones nativas implican que, aunque se incluyan componentes con tecnologías de diferentes fabricantes en la solución ofertada, existen conectores prediseñados y soportados out-of-the-box por cada uno para integrarse entre sí, no deben ser integraciones desarrolladas por el oferente.

PREGUNTA 92.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 114 se solicita. “El componente central de inteligencia unificada de ciberdefensa debe importar desde la función NDR al menos la siguiente información de telemetría...Volumen de datos transferidos (entrada/salida); Patrones temporales de comunicación...”.

Hacemos notar que lo solicitado es posible solo cuando el componente NDR y de INTELIGENCIA UNIFICADA DE CIBERDEFENSA son de una misma marca. Las integraciones comunes entre soluciones de marcas diferentes están limitadas a syslog y API importando alertas y artefactos mas no lo solicitado, por lo tanto, entendemos que se aceptará un desarrollo personalizado para cumplir esta parte siempre y cuando esta información esté disponible por parte del NDR mediante API. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 92.-

Estimado oferente, no se admite un desarrollo personalizado.

Por favor remitirse a lo solicitado en el numeral 112 del apartado INTELIGENCIA UNIFICADA DE CIBERDEFENSA

“El componente central de inteligencia unificada de ciberdefensa debe integrarse de forma nativa con las funciones y componentes tecnológicos incluidos en la solución contratada, listados a continuación, para acopiar e incorporar en su análisis la información de telemetría de estos.

- *Endpoint Detection and Response (EDR),*
- *Network Detection and Response (NDR),*
- *Función de gestión de amenazas de identidad.”*

PREGUNTA 93.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 115 se solicita. “El componente central de inteligencia unificada de ciberdefensa debe acopiar e incorporar en su análisis los registros de eventos de los siguientes controles de ciberseguridad institucionales: Broadcom/Symantec ProxySG...”.

Según nuestro entendimiento se admitirá el desarrollo de una integración personalizada cuando no exista un conector con la plataforma solicitada. Por favor indicar si es correcto nuestro entendimiento o aclarar. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 93.-

Estimado oferente, el componente central de inteligencia unificada de ciberdefensa debe

acopiar e incorporar en su análisis los registros de eventos de los controles de ciberseguridad institucionales indicados, se admite desarrollos personalizados y el uso de protocolos estándar (SYSLOG).

Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 94.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 115 se solicita. “El componente central de inteligencia unificada de ciberdefensa debe acopiar e incorporar en su análisis los registros de eventos de los siguientes controles de ciberseguridad institucionales: IBM Verify Identity Governance ...”.

Según nuestro entendimiento se validará la compatibilidad con la versión de la plataforma y de ser el caso se desarrollará un conector personalizado de ser el caso y siempre y cuando el componente soporte dicha integración. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 94.-

Estimado oferente, el componente central de inteligencia unificada de ciberdefensa debe acopiar e incorporar en su análisis los registros de eventos de los controles de ciberseguridad institucionales indicados, se admite desarrollos personalizados y el uso de protocolos estándar (SYSLOG).

Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 95.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 117 se solicita. “El componente central de inteligencia unificada de ciberdefensa debe ser capaz de incorporar al menos los siguientes datos generados desde el sistema Proofpoint Core Email Protection del SRI...

- Familia de amenaza identificada”.

Según nuestro entendimiento esta información de incluirá si la solución de protección de correo lo provee y se permitirá incluir este parámetro en la integración personalizada mediante API. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 95.-

Estimado oferente, el componente central de inteligencia unificada de ciberdefensa debe ser capaz de incorporar al menos los datos indicados desde el sistema Proofpoint Core Email Protection del SRI, los datos indicados estarán disponibles para la incorporación, se admite desarrollos personalizados y el uso de protocolos estándar (SYSLOG, API)

Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 96.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 118 se solicita. “El componente central de inteligencia unificada de ciberdefensa debe ser capaz de incorporar al menos los siguientes datos generados desde el sistema Broadcom/Symantec ProxySG del SRI ... Dirección de acceso”. Según nuestro entendimiento por dirección de acceso se refiere a la categoría del sitio accedido y se permitirá incluir este parámetro en la integración mediante API. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 96.-

Estimado oferente, se refiere a la dirección IP desde la cual se accede, este dato estará disponible para que pueda ser incorporado al componente central de inteligencia unificada de ciberdefensa.

PREGUNTA 97.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 120 se solicita. “El componente central de inteligencia unificada de ciberdefensa debe ser capaz de acopiar e incorporar en su análisis los registros de eventos de los siguientes componentes tecnológicos: Red Hat Single Sign-On (SSO) de intranet, Red Hat Identity Policy Audit (IPA),”. Según nuestro entendimiento se admitirá el desarrollo de una integración personalizada en caso de que no exista un conector desarrollado. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 97.-

Estimado oferente, el componente central de inteligencia unificada de ciberdefensa debe ser capaz de acopiar e incorporar en su análisis los registros de eventos de los componentes tecnológicos indicados en el numeral 120 de INTELIGENCIA UNIFICADA DE CIBERDEFENSA, para este fin se admite desarrollos personalizados y protocolos estándar. Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 98.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 121 se solicita. “El componente central de inteligencia unificada de ciberdefensa debe ser capaz de incorporar al menos los siguientes datos generados desde el sistema de Red Hat Single Sign-On (SSO) de intranet del SRI” Según nuestro entendimiento se admitirá el desarrollo de una integración personalizada en caso de que no exista un conector desarrollado que extraiga los parámetros solicitados siempre y cuando estén disponibles para terceros. Por favor indicar si es correcto nuestro

entendimiento o aclarar.

RESPUESTA 98.-

Estimado oferente, el componente central de inteligencia unificada de ciberdefensa debe ser capaz de incorporar al menos los datos indicados desde el sistema de Red Hat Single Sign On (SSO) de intranet del SRI, los datos estarán disponibles para su incorporación, para este fin se admite desarrollos personalizados y el uso de protocolos estándar. Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 99.-

En el documento “DOCUMENTO ESTÁNDAR DE LICITACIÓN Solicitud de Ofertas de Bienes y Servicios”, sección “BIENES REQUERIDOS” componente “INTELIGENCIA UNIFICADA DE CIBERDEFENSA” en el numeral 122 se solicita. “El componente central de inteligencia unificada de ciberdefensa debe ser capaz de incorporar al menos los siguientes datos generados desde el sistema de Red Hat Identity Policy Audit (IPA) del SRI”
Según nuestro entendimiento se admitirá el desarrollo de una integración personalizada en caso de que no exista un conector desarrollado que extraiga los parámetros solicitados siempre y cuando estén disponibles para terceros. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 99.-

Estimado oferente, el componente central de inteligencia unificada de ciberdefensa debe ser capaz de incorporar al menos los datos indicados desde el sistema de Red Hat Identity Policy Audit (IPA) del SRI, los datos estarán disponibles para su incorporación, para este fin se admite desarrollos personalizados y el uso de protocolos estándar. Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 100.-

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 138 se solicita. “Los flujos de trabajo que se utilicen para automatizar y ejecutar acciones deberán ser compatibles al menos con Python o JavaScript o deberán permitir el uso de herramientas tipo low-code-no-code para el efecto”
Según nuestro entendimiento la compatibilidad con Python o Javascript puede ser suplidos con el uso de herramientas tipo low-code-no-code (sin código) ya que con estas herramientas se evita el uso de código de un proveedor particular. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 100.-

Estimado oferente, se puede utilizar herramientas tipo low-code-no-code.

PREGUNTA 102.-

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 152 se solicita. “La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes controles de ciberseguridad institucionales: Broadcom/Symantec ProxySG”

Según nuestro entendimiento se admitirá el desarrollo de una integración personalizada en caso de que no exista un conector desarrollado que permita implementar las tareas de respuesta automáticas. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 102.-

Estimado oferente, su entendimiento es correcto, se aceptan desarrollos personalizados y el uso de protocolos estándar para que la función central de respuesta unificada de ciberdefensa sea capaz de realizar tareas automáticas a través de los controles de ciberseguridad institucionales indicados.

Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 103.-

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 152 se solicita. “La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes componentes tecnológicos institucionales: Palo Alto Networks ION SDWAN,” Según nuestro entendimiento se admitirá el desarrollo de una integración personalizada en caso de que no exista un conector desarrollado que permita implementar las tareas de respuesta automáticas. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 103.-

Estimado oferente, el numeral que hace referencia a “La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes componentes tecnológicos institucionales: Palo Alto Networks ION SDWAN,” es el 153, en ese sentido, se aceptan desarrollos personalizados y el uso de protocolos estándar para lo indicado en dicho numeral.

Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 104.-

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 152 se solicita. “La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes

componentes tecnológicos institucionales: IBM Verify Identity Governance,”
Según nuestro entendimiento se admitirá el desarrollo de una integración personalizada en caso de que no exista un conector desarrollado que permita implementar las tareas de respuesta automáticas. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 104.-

Estimado oferente, el numeral que hace referencia a “La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes componentes tecnológicos institucionales: IBM Verify Identity Governance,” es el 153, en ese sentido, se aceptan desarrollos personalizados y el uso de protocolos estándar para lo indicado en dicho numeral.

Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 105.-

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 155 se solicita. “La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar al menos las siguientes tareas automáticas sobre el sistema Palo Alto Networks ION SDWAN del SRI (ver INFRAESTRUCTURA ACTUAL),”

Según nuestro entendimiento se admitirá el desarrollo de una integración personalizada en caso de que no exista un conector desarrollado que permita implementar las tareas de respuesta automáticas. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 105.-

Estimado oferente, su entendimiento es correcto, se admiten desarrollos personalizados y el uso de protocolos estándar para que la función central de respuesta unificada de ciberdefensa sea capaz de realizar al menos las tareas automáticas indicadas sobre el sistema Palo Alto Networks ION SDWAN del SRI.

Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 106.-

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 156 se solicita. “La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar al menos las siguientes tareas automáticas sobre el sistema IBM Verify Identity Governance del SRI.

Según nuestro entendimiento se admitirá el desarrollo de una integración personalizada en caso de que no exista un conector desarrollado que permita implementar las tareas de respuesta automáticas. Por favor indicar si es correcto nuestro entendimiento o aclarar.

RESPUESTA 106.-

Estimado oferente, su entendimiento es correcto, se admiten desarrollos personalizados y el uso de protocolos estándar para que la función central de respuesta unificada de ciberdefensa sea capaz de realizar al menos las tareas automáticas indicadas sobre el sistema IBM Verify Identity Governance del SRI.

Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 107.-

En la sección VI. Requisitos de los Bienes y Servicios Conexos, subsección 2. LISTA DE SERVICIOS / SERVICIOS CONEXOS Y CRONOGRAMA DE CUMPLIMIENTO, en el apartado IMPLEMENTACIÓN, numeral 8, página 133, se indica que la etapa de preparación consistirá en la planificación y en la elaboración del plan de implementación y de la arquitectura de ciberdefensa, entregables que se producen dentro de los mismos 90 días previstos para la totalidad de la implementación. El documento no prevé una reunión de arranque del proyecto, no fija el plazo del que dispone el Administrador de Contrato para pronunciarse sobre dichos entregables (plan de implementación y arquitectura) ni establece el efecto que su revisión produce sobre el plazo contractual, pese a que ambos constituyen la línea base contra la cual se mide el avance del proyecto. ¿Se realizará una reunión de arranque formal del proyecto y en qué plazo contado desde la suscripción del contrato? ¿Cuál es el plazo máximo del que dispondrá el Administrador de Contrato para pronunciarse sobre el plan de implementación y la arquitectura de ciberdefensa? ¿Se suspende el plazo de implementación mientras dichos entregables se encuentren en revisión del Comprador?

RESPUESTA 107.-

Estimado oferente, si considera necesaria la reunión de arranque la puede hacer dentro del periodo de implementación. No hay un plazo máximo definido para la entrega del plan de implementación y arquitectura de ciberseguridad ni tampoco para su aprobación, todo debe realizarse dentro del periodo de implementación.

PREGUNTA 109.-

Lote único frente a evaluación por artículos

En los DDL se indica que la contratación corresponde a un “LOTE ÚNICO”; sin embargo, en la IAO 35.2(a) se establece que las ofertas serán evaluadas por artículos y que el contrato

comprenderá los artículos adjudicados al oferente seleccionado.

Solicitamos aclarar si la adjudicación se realizará de manera integral por la totalidad del lote único —ítems 1 al 7— o si el SRI podrá adjudicar individualmente determinados artículos. En caso de adjudicación por artículos, sírvase indicar cómo se garantizará la interoperabilidad y responsabilidad integral de la solución.

RESPUESTA 109.-

Estimado oferente,

La adjudicación será por la totalidad de los ítems ofertados. En función de lo anterior la contratación corresponde a un “LOTE ÚNICO”.

PREGUNTA 110.-

Once períodos “trimestrales” El servicio contempla 11 períodos de 91 días, equivalentes a 1.001 días, y no a tres años completos. Solicitamos confirmar que la expresión “trimestral” corresponde específicamente a períodos contractuales de 91 días y que se pagarán 11 períodos independientes. Sírvese además indicar las fechas estimadas de inicio y terminación de cada período.

RESPUESTA 110.-

Estimado oferente, de acuerdo con el numeral 8.3 el plazo de vigencia del servicio será de 1.001 días, fraccionados contractualmente en 11 periodos uniformes de 91 días cada uno, las fechas estimadas para el inicio rigen estrictamente a partir del hito de culminación de los 90 días previstos para implementación.

PREGUNTA 111.-

Inicio de la vigencia del licenciamiento Las licencias se activan antes de la implementación y su vigencia comienza desde dicha activación.

Solicitamos confirmar que el plazo de 1.092 días de licenciamiento y soporte de fábrica será suficiente para cubrir toda la implementación y los 11 períodos del servicio. En caso de retrasos de implementación no imputables al contratista, sírvase confirmar que el SRI reconocerá la extensión del licenciamiento que resulte necesaria.

RESPUESTA 111.-

Estimada oferente,

En el caso que el retraso de la implementación sea imputable al Servicio de Rentas Internas se aplicará lo previsto en la ley Orgánica del Sistema de Contratación Pública y su Reglamento General en lo que respecta a la suspensión de la ejecución del plazo contractual.

PREGUNTA 112.-

Para validar la experiencia del personal técnico, se aceptarán certificados emitidos por el empleador, ¿Solicitamos confirmar si un mismo certificado puede acreditar simultáneamente el tiempo de experiencia y el número de proyectos del profesional?

RESPUESTA 112.-

Estimado Oferente,

De conformidad con lo establecido en el numeral 5 de la Sección III. Criterios de Evaluación y Calificación, página 67:

“Los certificados de experiencia pueden ser emitidos por los clientes finales o por el fabricante.”

Se aclara que los certificados de experiencia emitidos por los clientes finales o por el fabricante podrán acreditar simultáneamente el tiempo de experiencia y el número de proyectos en los que haya participado el profesional, siempre que la información contenida en dichos documentos permita verificar de manera clara y fehaciente el cumplimiento de los requisitos solicitados.

Los certificados deberán estar elaborados en hoja membretada y contener, como mínimo, la siguiente información: nombres y apellidos del profesional, cargo(s) desempeñado(s) relacionado(s) con el perfil requerido, período o tiempo de experiencia acreditado, nombre del proyecto o proyectos ejecutados, descripción general de la participación o funciones realizadas, firma y sello de la entidad emisora, así como los datos de contacto necesarios para efectos de validación.

PREGUNTA 113.-

¿Para acreditar experiencia específica, se aceptan actas de recepción, Contratos en caso de que no exista certificado de experiencia?

RESPUESTA 113.-

Estimado Oferente, favor remitirse a lo solicitado en Sección III. Criterios de Evaluación y Calificación, página 60, literal (b) Experiencia específica que señala:

“Documentos de sustento: Certificados de experiencia o actas de entrega recepción definitivas, que acrediten fehacientemente la experiencia solicitada, emitidos dentro de los 10 años previos a la fecha de publicación del presente proceso de contratación.”

No se admitirán certificados de experiencia emitidos por el mismo oferente.”

PREGUNTA 114.-

Con referencia al numeral IAO 21.1 Presentación de la oferta establece que la oferta física original deberá entregarse debidamente firmada, foliada y con todas sus hojas sumilladas o inicialadas, además de incluir una versión en medio magnético (formato digital) que permita realizar búsquedas de texto.

RESPUESTA 114.-

Estimado oferente, favor remitirse a lo establecido en el Sección II. Datos de la Licitación (DDL), IAO 21.1, página 48.

PREGUNTA 115.-

Considerando que el proceso de conversión de documentos escaneados a formato OCR puede generar alteraciones en la estructura, formato o distribución del contenido, ¿en caso de existir diferencias de forma entre la versión física original y la versión digital, entendemos que la que prevalecerá la física.

RESPUESTA 115.-

Estimado oferente, su interpretación es correcta; no obstante, el oferente deberá garantizar que los documentos escaneados en formato OCR correspondan fielmente a la versión física original.

PREGUNTA 116.-

Seguro de equipos NDR

Solicitamos confirmar las coberturas, montos, beneficiario, deducibles y condiciones mínimas de la póliza requerida para los equipos NDR entregados como servicio.

RESPUESTA 116.-

Estimado oferente,

Favor remitirse a lo establecido en el numeral 14 de la Sección VI. Requisitos de los Bienes y Servicios Conexos, apartado DESPLIEGUE DEL HARDWARE.

Es responsabilidad del oferente realizar los acercamientos respectivos con la aseguradora que considere pertinente a fin de establecer las mejores condiciones de la póliza.

PREGUNTA 117.-

Estimada entidad, en el punto 7 del numeral SERVICIO DE GESTION DE CIBERDEFENSA, entendemos que el mantenimiento preventivo a realizar sobre los componentes tecnológicos debe ser coordinado con el administrador del contrato y se debe emitir un informe final de los trabajos realizados. Confirmar.

RESPUESTA 117.-

Estimado oferente, en el numeral 7 del apartado SERVICIO DE GESTIÓN DE CIBERDEFENSA (Metodología) establece que *“Es responsabilidad del contratista realizar el mantenimiento periódico de los componentes tecnológicos incluidos en la solución contratada para garantizar su correcto funcionamiento y la entrega del servicio.”*

Además, en el numeral 2 de las CONDICIONES GENERALES de METODOLOGÍA DE TRABAJO se establece que:

“Todas las actividades que impliquen cambios en la configuración, en la operación o en el nivel de seguridad informática de los sistemas o componentes instalados o desplegados que representen un impacto o afectación a la operación de los servicios o componentes tecnológicos institucionales deberán ser informadas al administrador del contrato y deberán ser aplicadas de manera controlada en coordinación con el personal del SRI.”

En observancia al numeral 2 previamente detallado, dichas acciones deberán ser canalizadas controladamente con el administrador del contrato y respaldadas mediante los reportes operativos del periodo.

PREGUNTA 118.-

Propiedad de los equipos

Solicitamos confirmar que los equipos NDR entregados como servicio continuarán siendo propiedad del contratista y serán retirados al finalizar el contrato, después del borrado seguro de información.

RESPUESTA 118.-

Estimado oferente, se confirma el entendimiento. El apartado DESPLIEGUE DEL HARDWARE, numeral 1, establece que *“para la activación y funcionamiento de las licencias de software del componente Network Detection and Response (NDR), el contratista deberá incluir en el servicio de ciberdefensa, en calidad de préstamo, el hardware necesario para su operación”*, lo cual confirma que los equipos NDR se entregan bajo la modalidad de préstamo dentro del servicio contratado y no se transfieren en propiedad al SRI.

Asimismo, el numeral 15 del mismo apartado, y el numeral 4 de las CONDICIONES GENERALES DE SERVICIOS CONEXOS REQUERIDOS, establecen que, antes de que el contratista retire los equipos instalados al final del contrato, deberá ejecutarse un procedimiento de borrado seguro de datos.

PREGUNTA 120.-

Certificaciones técnicas de especialistas

La redacción podría interpretarse como que cada uno de los tres especialistas debe estar certificado en dos componentes tecnológicos.

Solicitamos confirmar si cada especialista de implementación deberá contar individualmente

con certificaciones de fabricante en al menos dos componentes de la solución, o si el requisito podrá cumplirse de manera conjunta entre los tres especialistas.

RESPUESTA 120.-

Estimado Oferente, **cada** Especialista de implementación requiere contar con: *“Certificación técnica vigente nivel profesional, avanzado o equivalente emitida por el fabricante de al menos dos de los componentes tecnológicos incluidos en la solución ofertada.”* De acuerdo con el requisito establecido en la página 63 de la Sección III. Criterios de Evaluación y Calificación.

PREGUNTA 121.-

Certificaciones equivalentes

Solicitamos indicar los criterios objetivos que se utilizarán para determinar que una certificación corresponde a nivel profesional, avanzado o equivalente, especialmente cuando los fabricantes utilizan denominaciones y esquemas de certificación diferentes.

RESPUESTA 121.-

Estimado oferente,

En atención a la consulta realizada, se aclara que la validación de las certificaciones técnicas de nivel profesional, avanzado o equivalente se realizará considerando la correspondencia técnica y funcional de la certificación presentada respecto al componente tecnológico ofertado.

Para determinar la equivalencia de una certificación, se considerarán como criterios objetivos, entre otros, los siguientes aspectos:

- Que la certificación sea emitida oficialmente por el fabricante de la tecnología correspondiente o por una entidad reconocida y autorizada por este.
- Que la certificación corresponda a un nivel de conocimiento y especialización igual o superior al nivel profesional o avanzado requerido, de acuerdo con el esquema de certificación definido por cada fabricante.
- Que el contenido, alcance, competencias evaluadas y requisitos de obtención de la certificación guarden relación con las funciones técnicas asociadas al componente tecnológico incluido en la solución ofertada.
- Que la certificación acredite conocimientos especializados para la implementación, administración, configuración, operación, integración, mantenimiento o soporte de la tecnología correspondiente.

Considerando que los fabricantes pueden utilizar diferentes nomenclaturas para sus esquemas de certificación, la denominación específica del nivel no será el único criterio de evaluación; se analizará la documentación oficial del fabricante que permita validar la equivalencia técnica del nivel presentado.

El oferente deberá presentar la documentación de respaldo correspondiente, incluyendo los certificados emitidos por el fabricante y la información técnica disponible que permita verificar el alcance y nivel de la certificación. La validación final de la equivalencia será realizada por el SRI conforme a la documentación presentada y a las características de la solución ofertada.

PREGUNTA 122.-

Personal extranjero

Considerando que no se exige el registro de títulos extranjeros en la SENESCYT, solicitamos confirmar que se aceptarán títulos, certificaciones y certificados de experiencia emitidos en el extranjero mediante copia simple y traducción al español, sin apostilla para la presentación de la oferta.

RESPUESTA 122.-

Estimado oferente, conforme lo dispuesto en la IAO 21.1 de la Sección II, Datos de la Licitación (DDL), página 48, para la presentación de la oferta se aceptarán copias simples acompañadas de su respectiva traducción fidedigna al español. Sin perjuicio de ello, para la suscripción del contrato será obligatorio presentar los documentos otorgados en territorio extranjero debidamente legalizados ante agente diplomático o cónsul del Ecuador acreditado en dicho país, o apostillados, según corresponda.

PREGUNTA 123.-

Personal del fabricante

Solicitamos confirmar si el personal MDR, de cacería de amenazas y de respuesta a incidentes perteneciente al fabricante puede ser presentado como parte del equipo mediante carta de compromiso o certificado del fabricante, sin que exista relación laboral directa con el oferente.

RESPUESTA 123.-

Estimado oferente,
Es correcto su entendimiento.

PREGUNTA 124.-

Pago del licenciamiento

Las licencias deben activarse hasta 15 días después de la firma, pero el 100 % del licenciamiento y de la implementación se pagará únicamente al finalizar la implementación, que puede durar hasta 90 días después de la activación. Considerando que el licenciamiento debe ser activado y pagado al fabricante al inicio del contrato, solicitamos confirmar si el SRI aceptará realizar el pago del rubro de licenciamiento una vez acreditada su activación y suscrita el acta correspondiente, de manera independiente al pago de la implementación.

RESPUESTA 124.-

Estimado oferente,
No se acepta su solicitud, el pago se realizará según lo que se encuentra estipulado en CGC 17.1 FORMA Y CONDICIONES DE PAGO de la Sección VIII. Condiciones Especiales de Contrato (CEC).

PREGUNTA 125.-

Plazo efectivo de pago

Las CEC indican que el procedimiento termina con la emisión del CUR y que la acreditación depende de las directrices del Ministerio de Economía y Finanzas. También se establece que

los intereses se reconocerán después de 60 días únicamente cuando el retraso sea imputable al SRI.

Solicitamos precisar el plazo máximo, contado desde la suscripción del acta de entrega-recepción y presentación de la factura, dentro del cual el SRI emitirá el CUR de pago. Asimismo, solicitamos confirmar si los retrasos posteriores a la emisión del CUR no serán imputables al contratista ni afectarán la continuidad del servicio.

RESPUESTA 125.-

Estimado Oferente, el SRI emitirá el CUR de pago en un plazo de hasta 15 días siempre que toda la documentación ingresada para procesar el pago sea entregada de manera oportuna y se encuentre correcta conforme a la oferta presentada, DDL y comunicaciones con el Administrador de Contrato.

Los retrasos posteriores a la emisión del CUR, la Solicitud de Ofertas (SDO) indica lo siguiente: *“La acreditación del pago corresponderá a los plazos y directrices que emita el Ministerio de Economía y Finanzas”* y la ejecución contractual debe continuar conforme los plazos establecidos en el Contrato.

PREGUNTA 126.-

Facturación promedio anual

Para acreditar la facturación promedio anual de los últimos cinco años, sírvase confirmar si

será suficiente presentar estados financieros y declaraciones de impuestos, o si adicionalmente deben adjuntarse facturas individuales. Solicitamos también confirmar cuáles serán exactamente los cinco ejercicios fiscales considerados.

RESPUESTA 126.-

Estimado el oferente, la Solicitud de la Oferta (SDO) en la Sección III Criterios de Evaluación y Calificación, indica: ***“En relación con los últimos 5 años con cierre fiscal, se deberá entregar copia simple de los estados financieros, declaraciones de impuestos anuales, facturas por la venta y/o servicios de tecnología o documentación equivalente en el país de origen, presentados ante autoridad competente. La documentación debe presentarse en dólares de los Estados Unidos de América. De estar denominados en otra moneda, incluirán la conversión a dólares de los Estados Unidos de América utilizando la tasa transaccional para la venta del tipo de cambio publicada en la página del Banco Central del Ecuador <https://www.bce.fin.ec/cotizaciones/consulta-por-monedas-extranjeras>, a la fecha del último día del ejercicio fiscal correspondiente”*** (lo resaltado me pertenece); la facturación a ser presentada será únicamente la que permita evidenciar el cumplimiento del parámetro establecido en la SDO.

Respecto a los cinco ejercicios fiscales a considerar favor remitirse a la Sección V. Formularios de la Oferta, página 96, Formulario - Capacidad Financiera

PREGUNTA 128.-

Estimada Entidad, en la sección VI. Requisitos de los Bienes y Servicios Conexos, subsección

2. LISTA DE SERVICIOS / SERVICIOS CONEXOS Y CRONOGRAMA DE CUMPLIMIENTO, en el apartado de METODOLOGÍA DE TRABAJO, CONDICIONES GENERALES, numeral 2, página 110, se establece que todas las actividades que impliquen cambios en la configuración, en la operación o en el funcionamiento de los componentes institucionales deben gestionarse como cambio tecnológico, con documento de actividades, plan de contingencia y procedimiento de reverso; y en el apartado de IMPLEMENTACIÓN, página 134, se indica que dichas actividades se ejecutarán en ventanas de mantenimiento programadas en función de las condiciones institucionales del SRI. El documento no informa el número de ventanas disponibles, su duración, su horario, los periodos en los que no se autorizan cambios ni el plazo de aprobación de las solicitudes de cambio tecnológico, siendo estas las restricciones que gobiernan la ruta crítica y sin las cuales el cronograma de implementación no resulta construible. ¿Cuántas ventanas de mantenimiento estarán disponibles por mes, de qué duración y en qué horario habitual? ¿Cuáles son los periodos de congelamiento operativo en los que no se autorizan cambios, tales como los correspondientes a vencimientos tributarios? ¿Cuál es el plazo de aprobación de las solicitudes de cambio tecnológico por parte de las instancias competentes del SRI?

RESPUESTA 128.-

Estimado oferente, se proporcionará toda la información adicional al oferente que resulte adjudicado.

PREGUNTA 129.-

Estimada entidad, confirmar si la entidad deshabilitará la opción Tamper Protection antes del proceso de desinstalación solicitada para el producto Symantec Endpoint Protection.

RESPUESTA 129.-

Estimado oferente, la desinstalación del software correspondiente al agente de antivirus deberá desarrollarse siguiendo las recomendaciones del fabricante.

Cabe indicar que la solicitud de oferta (SDO) establece que:

“El SRI no puede garantizar la disponibilidad de un mecanismo de instalación o de desinstalación o de distribución automática de software. Es responsabilidad del contratista el cumplimiento satisfactorio de estas actividades y su consideración en la planificación.”

PREGUNTA 130.-

Estimada entidad, confirmar si la licencia y la consola de Symantec Endpoint Protection se encuentran con soporte de fábrica vigente y disponible.

RESPUESTA 130.-

Estimado oferente, se confirma que la licencia y la consola de Symantec Endpoint Protection cuenta con soporte de fábrica hasta el 27 mayo de 2027.

PREGUNTA 131.-

Estimada entidad en ítem que se solicita: El agente EDR debe soportar los siguientes sistemas operativos: Estaciones Windows [de escritorio y portátiles]: Windows 10, 11 y superiores; Estaciones macOS [de escritorio y portátiles]: macOS 13, 14, 15 y superiores; Servidores Windows: Windows Server 2016, 2019, 2022, 2025 y superiores; Servidores Linux: RHEL 7.4, 8, 9 y superiores. Confirmar la cantidad de equipos con Red Hat Enterprise Linux 7.4 y otras versiones que puedan requerir agentes tipo legacy, por tema de compatibilidad.

RESPUESTA 131.-

Estimado oferente, no se dispone de un desglose por versión específica de RHEL que permita cuantificar los equipos que podrían requerir agentes de tipo legacy. Se recomienda que el oferente dimensione su propuesta técnica considerando la totalidad de los 660 hosts RHEL reportados en la Tabla 6 como universo máximo potencial de equipos con versiones heredadas, y que valide dicho detalle durante la etapa de preparación de la implementación, conforme lo permite la nota de la INFRAESTRUCTURA ACTUAL

PREGUNTA 132.-

Estimada entidad, confirmar el tamaño en GB generado por el volumen diario de eventos de información y la capacidad en almacenamiento actualmente utilizada.

RESPUESTA 132.-

Estimado oferente,

En la Tabla 9 (numeral 12 de INFRAESTRUCTURA ACTUAL) se detalla el tamaño aproximado de los registros de eventos (logs) de los principales componentes tecnológicos, expresado en periodos diarios o mensuales, con una estimación de crecimiento del 5% anual.

Esta información constituye la base disponible para el dimensionamiento del volumen de datos. El SRI no proveerá una cifra consolidada única de “volumen diario total” ni la “capacidad de almacenamiento actualmente utilizada” en sus sistemas propios, ya que

dicho dimensionamiento es responsabilidad del contratista, conforme a lo establecido en el numeral 96 de INTELIGENCIA UNIFICADA DE CIBERDEFENSA.

PREGUNTA 133.-

Estimada entidad, confirmar las características físicas de los racks (dimensiones, profundidad, tipo de tomas eléctricas).

RESPUESTA 133.-

Estimado oferente, los centros de datos institucionales disponen de gabinetes de telecomunicaciones y servidores estándar de 19 pulgadas (1U o 2U), y provisión eléctrica regulada. Las especificaciones exactas se levantarán en conjunto con el contratista durante la fase de Preparación.

PREGUNTA 134.-

Estimada entidad, confirmar si será posible realizar una inspección técnica previa en los centros de datos. Con quien podemos coordinar para realizar esta inspección.

RESPUESTA 134.-

Estimado oferente, acorde a los plazos previstos, no están autorizadas evaluaciones in-situ (assessments) en el transcurso de la etapa precontractual. Las especificaciones de tráfico actual (y la estimación del 5% anual estipulada) componen el insumo central suficiente para un dimensionamiento referencial y escalable que asuma la variabilidad regular del mercado.

PREGUNTA 136.-

Estimada entidad referente al punto: La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes componentes tecnológicos institucionales: Microsoft Exchange (local y online), Palo Alto Networks ION SDWAN, IBM Verify Identity Governance, VMware vCenter/vSphere, Otros componentes tecnológicos existentes con los que el servicio requiera integrarse para realizar acciones de contención. NOTAS: Es responsabilidad del contratista incluir en la función central de respuesta unificada de ciberdefensa las integraciones y las acciones de respuesta necesarias para lograr una respuesta efectiva y oportuna ante amenazas de ciberseguridad en el entorno institucional. El alcance de cada integración puede variar a medida que los fabricantes involucrados liberen nuevas versiones. Dado que dependemos de que las plataformas mencionadas garanticen una interfaz de integración via API para poder realizar la automatización, entendemos que, si en algún momento una de estas plataformas llegase a cambiar estas condiciones, no es responsabilidad del servicio brindado por el contratista la afectación generada; y que será responsabilidad del contratista volver a construir la integración en base al mejor esfuerzo siempre que la

plataforma lo permita.

RESPUESTA 136.-

Estimado oferente, su entendimiento es correcto.

PREGUNTA 137.-

Estimada entidad referente al punto: La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes controles de ciberseguridad institucionales Check Point VSX, Proofpoint Core Email protection, Broadcom/Symantec ProxySG, Otros controles de ciberseguridad existentes con los que el servicio requiera integrarse para realizar acciones de contención. Favor confirmar que todas estas fuentes soporten API para respuesta unificada.

RESPUESTA 137.-

Estimado oferente, el numeral 149 referente a las tareas automáticas sobre los citados controles, recalca en su NOTA 1 que *"Es responsabilidad del contratista incluir en la función central de respuesta unificada de ciberdefensa las integraciones y las acciones de respuesta necesarias para lograr una respuesta efectiva y oportuna ante amenazas de ciberseguridad en el entorno institucional"*.

Por lo tanto, se aceptan desarrollos personalizados y el uso de protocolos estándar para que la función central de respuesta unificada de ciberdefensa sea capaz de realizar tareas automáticas a través de los controles de ciberseguridad institucionales indicados. Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 138.-

Estimada entidad referente al punto: El servicio debe incluir un equipo de gestión de eventos de ciberseguridad para remediar los eventos de ciberseguridad suscitados durante la vigencia del contrato. Se entiende que la remediación se lo realizará únicamente sobre las plataformas contratadas o cubiertas por el servicio. Favor confirmar.

RESPUESTA 138.-

Estimado oferente, su entendimiento es incorrecto, El numeral 14 de GESTIÓN DE EVENTOS DE CIBERSEGURIDAD aclara que *"Las acciones de remediación se deben aplicar directamente en los controles de ciberseguridad incluidos en la solución contratada o indirectamente en los controles de ciberseguridad institucionales integrados con el servicio"*.

PREGUNTA 139.-

Estimada entidad referente al punto: La gestión de los eventos de ciberseguridad debe incluir su remediación mediante la aplicación de las acciones necesarias para eliminar su ocurrencia o reducirla significativamente. Se entiende que la remediación se la realizará únicamente sobre las plataformas contratadas o cubiertas por el servicio. Favor confirmar.

RESPUESTA 139.-

Estimado oferente, su entendimiento es incorrecto, El numeral 14 de GESTIÓN DE EVENTOS DE CIBERSEGURIDAD aclara que *"Las acciones de remediación se deben aplicar directamente en los controles de ciberseguridad incluidos en la solución contratada o indirectamente en los controles de ciberseguridad institucionales integrados con el servicio"*.

PREGUNTA 140.-

Estimada entidad referente al punto: Las acciones de remediación se deben aplicar directamente en los controles de ciberseguridad incluidos en la solución contratada o indirectamente en los controles de ciberseguridad institucionales integrados con el servicio. Entendemos que las acciones de remediación deberán aplicar únicamente en la solución contratada. Por favor es necesario mayor contexto del alcance que esperan cuando se indica: *el apartado indirectamente en los controles de ciberseguridad institucionales integrados con el servicio*.

RESPUESTA 140.-

Estimado oferente,

El componente de Inteligencia unificada de ciberdefensa debe tener la capacidad de bloquear o contener una ciberamenaza tanto a través de los componentes internos (EDR, NDR , etc) de la solución como a través de las integraciones con los controles de seguridad informática institucionales.

PREGUNTA 141.-

Estimada entidad referente al punto: El servicio debe tomar todas las acciones necesarias para mantener un nivel óptimo de detección y respuesta de la arquitectura de ciberdefensa incluida; esto es, que la arquitectura de ciberdefensa esté correctamente afinada y operativa para que detecte y responda automáticamente todas las amenazas de ciberseguridad. Favor confirmar que las acciones necesarias se aplicarán únicamente sobre las soluciones contratadas o cubiertas por el servicio.

RESPUESTA 141.-

Estimado oferente, su entendimiento es incorrecto, El numeral 15 estipula que *"El servicio debe velar por que se mantenga un esquema de integración óptimo entre los controles de ciberseguridad incluidos en la solución contratada, y además con controles de ciberseguridad institucionales integrados con el servicio"*. En consecuencia, el afinamiento y las acciones de optimización incluyen de forma ineludible las integraciones con el entorno institucional.

PREGUNTA 142.-

Estimada entidad referente al punto: El servicio debe proveer al personal de Soporte a Usuarios y de Seguridad Informática de un juego de herramientas ("toolkit") portable, incluyendo su medio físico, que les permita reaccionar y colaborar con el servicio en los casos de incidentes de ciberseguridad que afecten las estaciones de trabajo (ej. de escritorio y portátiles). Favor confirmar ¿Cuántos kits deberán entregarse, qué herramientas, licencias, sistemas operativos, medios físicos y capacidades mínimas deberán contener y quién será su custodio?

RESPUESTA 142.-

Estimado oferente, Se recomienda en su oferta técnica, una cantidad de toolkits acorde con la estructura y distribución territorial del personal de Soporte a Usuarios y de Seguridad Informática del SRI (considerando la Tabla 7, que refleja la distribución de estaciones de trabajo por zonal), así como un detalle de herramientas forenses y de respuesta a incidentes de uso estándar en la industria, compatibles con los sistemas operativos Windows y macOS indicados en el numeral 5 de EDR. La designación del custodio y la validación final de las capacidades mínimas del toolkit deberán acordarse con el administrador del contrato durante la etapa de preparación de la implementación.

PREGUNTA 144.-

Estimada entidad en el formulario AUTORIZACION DEL FABRICANTE, solicitamos que se acepte el formulario emitido directamente por el fabricante en su formato, siempre que se conserve los datos que la entidad solicita. Los fabricantes tienen políticas muy estrictas desde sus departamentos legales con relación a los formatos de sus formularios aprobados, es por esto que solicitamos lo anterior.

RESPUESTA 144.-

Estimado oferente, el formulario AUTORIZACION DEL FABRICANTE no aplica para el presente proceso.

PREGUNTA 145.-

Estimada entidad, entendemos que las licencias del agente Symantec WSS serán

entregadas por el SRI para su instalación. Por favor confirmar.

RESPUESTA 145.-

Estimado oferente, su entendimiento es correcto.

PREGUNTA 146.-

Estimada entidad, entendemos que las licencias del agente Symantec WSS tiene soporte activo de fábrica y que se contará con el soporte del administrador para que garantice el funcionamiento, ya que entendemos que nuestro alcance es instalar, pero no que funcione en cada endpoint. Por favor confirmar.

RESPUESTA 146.-

Estimado oferente, su entendimiento es incorrecto, se confirma que el licenciamiento institucional del agente Symantec WSS cuenta con soporte activo de fábrica, con vigencia extendida hasta el 27 de mayo de 2027.

Sin embargo, su entendimiento respecto a que el alcance del contratista se limita únicamente a instalar sin garantizar su funcionamiento es incorrecto. De acuerdo con el numeral 10.f de la sección 7.1 IMPLEMENTACIÓN, es obligación directa del contratista *"Registrar la validación de la instalación y operación satisfactoria de los componentes de cada punto final cubierto por el servicio"*.

Adicionalmente, la NOTA del numeral 10.d recalca imperativamente que *"Es responsabilidad del contratista el cumplimiento satisfactorio de estas actividades"*.

PREGUNTA 147.-

Estimada entidad en el punto 12.d, entendemos que se nos brindará como insumo el estado actual de ciberdefensa institucional del SRI previo a la instalación. Confirmar.

RESPUESTA 147.-

Estimado oferente,

Con base a la información que obtendrá durante la implementación de la solución deberá realizarse la comparación.

PREGUNTA 148.-

Estimada entidad, para el punto 2 del ALCANCE, Servicio de Gestión de Ciberdefensa: Confirmar si los componentes de hardware para brindar este servicio solicitado por el SRI pueden ser equipos usados/refurbished o deben ser nuevos de fábrica y con soporte directo de los fabricantes por los 3 años que se debe brindar el servicio. Por favor confirmar.

RESPUESTA 148.-

Estimado oferente, de conformidad con lo establecido en la Solicitud de Ofertas (SDO), los componentes de hardware incluidos en el servicio de gestión de ciberdefensa deberán contar con el licenciamiento, suscripciones, soporte de fábrica y garantía técnica necesarios para garantizar su adecuada operación durante toda la vigencia del contrato, conforme a los numerales 11 y 13 del apartado DESPLIEGUE DEL HARDWARE.

Asimismo, el numeral 10 del mismo apartado establece que el contratista deberá instalar la última versión estable liberada, con el último paquete de parches y actualizaciones del firmware y software de cada componente de hardware desplegado, y el numeral 12 dispone que es responsabilidad del proveedor realizar las actualizaciones periódicas de dichos componentes de acuerdo con las mejores prácticas del fabricante.

En consecuencia, los equipos suministrados podrán ser **nuevos o usados** siempre que garanticen la vigencia de la garantía técnica, el soporte oficial del fabricante y la posibilidad de recibir actualizaciones durante toda la ejecución del contrato. El soporte de fábrica deberá mantenerse por todo el período de vigencia contractual, de acuerdo con lo establecido en la Solicitud de la Oferta (SDO).

PREGUNTA 149.-

Estimada entidad, en el punto 8.c del ítem IMPLEMENTACION se indica: Aplicar las recomendaciones y mejores prácticas de fábrica para la configuración del hardware, del firmware y del software de cada componente. Entendemos que eso implica que los componentes de hardware deben ser nuevos de fábrica y contar con el soporte del fabricante, para poder actualizar el firmware durante el tiempo que dure el servicio.

RESPUESTA 149.-

Estimado oferente, de conformidad con lo establecido en la Solicitud de Ofertas (SDO), los componentes de hardware incluidos en el servicio de gestión de ciberdefensa deberán contar con el licenciamiento, suscripciones, soporte de fábrica y garantía técnica necesarios para garantizar su adecuada operación durante toda la vigencia del contrato, conforme a los numerales 11 y 13 del apartado DESPLIEGUE DEL HARDWARE.

Asimismo, el numeral 10 del mismo apartado establece que el contratista deberá instalar la última versión estable liberada, con el último paquete de parches y actualizaciones del firmware y software de cada componente de hardware desplegado, y el numeral 12 dispone que es responsabilidad del proveedor realizar las actualizaciones periódicas de dichos componentes de acuerdo con las mejores prácticas del fabricante.

En consecuencia, los equipos suministrados podrán ser **nuevos o usados** siempre que garanticen la vigencia de la garantía técnica, el soporte oficial del fabricante y la posibilidad de recibir actualizaciones durante toda la ejecución del contrato. El soporte de

fábrica deberá mantenerse por todo el período de vigencia contractual, de acuerdo con lo establecido en la Solicitud de la Oferta (SDO).

PREGUNTA 150.-

Estimada entidad, por favor confirmar que tipo de certificación deben cumplir los patch cords.

RESPUESTA 150.-

Estimado oferente, se requiere que se sustente la certificación de los patch cords conforme a los estándares internacionales de la industria aplicables de acuerdo con el tipo de medio.

PREGUNTA 151.-

Estimada entidad, es posible realizar una inspección física para revisar distancias y espacios para los equipos. Si la respuesta es afirmativa por favor mencionar el contacto y el día para realizar la inspección

RESPUESTA 151.-

Estimado oferente, acorde a los plazos previstos, no se autorizan evaluaciones in-situ (assessments) en el transcurso de la etapa precontractual. Las especificaciones de tráfico actual (y la estimación del 5% anual estipulada) componen el insumo central suficiente para un dimensionamiento referencial y escalable que asuma la variabilidad regular del mercado.

PREGUNTA 152.-

Estimada entidad, entendemos que las actividades de implementación solicitadas en el punto IMPLEMENTACIÓN, deben ser realizadas por el fabricante con su personal directo de forma remota o presencial, y con el apoyo del contratista de forma presencial. Por favor confirmar

RESPUESTA 152.-

Estimado oferente, su entendimiento es incorrecto, favor referirse a los numerales 3-6 del apartado IMPLEMENTACIÓN de la Sección VI. Requisitos de los Bienes y Servicios Conexos, en los que se establece

3. *“Es responsabilidad del Contratista en conjunto con el personal especializado del Fabricante velar por que se incluyan en cada etapa todas las actividades y recursos necesarios para conseguir una implementación exitosa con un impacto reducido y controlado.*

4. *Todas las actividades de la implementación asociadas con la intervención de equipos tecnológicos deberán realizarse presencialmente por el personal técnico del Contratista.*
5. *Todas las actividades de la etapa de **puesta en producción** asociadas con la intervención de equipos tecnológicos deberán realizarse presencialmente por el personal técnico del Contratista con la asistencia remota del personal especializado del fabricante.*
6. *Si el SRI considera necesaria la intervención del personal especializado del Fabricante en cualquiera de las etapas de implementación, este podrá solicitarla formalmente, aplicándose el **ACUERDO DE NIVEL DE SERVICIO** para Asistencia Técnica con prioridad 3.”*

PREGUNTA 153.-

Estimada entidad, entendemos que las actividades de puesta en producción solicitadas en el punto IMPLEMENTACIÓN, deben ser realizadas por el fabricante con su personal directo de forma presencial, y con el acompañamiento del contratista de forma presencial. Por favor confirmar

RESPUESTA 153.-

Estimado oferente, su entendimiento es incorrecto, favor referirse a los numerales 3-6 del apartado IMPLEMENTACIÓN de la Sección VI. Requisitos de los Bienes y Servicios Conexos, en los que se establece

3. *“Es responsabilidad del Contratista en conjunto con el personal especializado del Fabricante velar por que se incluyan en cada etapa todas las actividades y recursos necesarios para conseguir una implementación exitosa con un impacto reducido y controlado.*
4. *Todas las actividades de la implementación asociadas con la intervención de equipos tecnológicos deberán realizarse presencialmente por el personal técnico del Contratista.*
5. *Todas las actividades de la etapa de **puesta en producción** asociadas con la intervención de equipos tecnológicos deberán realizarse presencialmente por el personal técnico del Contratista con la asistencia remota del personal especializado del fabricante.*
6. *Si el SRI considera necesaria la intervención del personal especializado del Fabricante en cualquiera de las etapas de implementación, este podrá solicitarla formalmente, aplicándose el **ACUERDO DE NIVEL DE SERVICIO** para Asistencia Técnica con prioridad 3.”*

PREGUNTA 154.-

Estimada entidad, para el punto IMPLEMENTACIÓN, entendemos que para cada integración solicitada y que no es parte integral del presente contrato, se tiene soporte activo con el fabricante y se contará con el acompañamiento del administrador de ese componente o sistema.

RESPUESTA 154.-

Estimado oferente,

Dependiendo de la naturaleza y funciones del componente tecnológico al que se tenga que integrar el SRI proveerá la asistencia o acompañamiento del administrador del componente, del proveedor o del fabricante según corresponda en cada caso.

PREGUNTA 155.-

Estimada entidad, en el punto PLAZO DE EJECUCION se indica que este contrato tiene 1106 días calendario contados a partir del día siguiente a la fecha de suscripción del contrato. Es de conocimiento público los tiempos extendidos que existen para entrega de hardware en los fabricantes por escasez de memorias y discos, esto hace complejo tener solo 90 días para la fase de IMPLEMENTACION, la cual incluye importar hardware especializado para brindar el servicio, por favor analizar la posibilidad de contar con 120 días calendario para la etapa de implementación .

RESPUESTA 155.-

Estimado oferente, no se acepta su solicitud.

PREGUNTA 157.-

Estimada entidad, en el punto 10.a, puesta en producción del punto IMPLEMENTACION, entendemos que las ventanas de mantenimiento que sean requeridas no contabilizarán los 90 días de implementación, ya que dependemos de la disponibilidad del SRI para realizar estas ventanas, por tanto nos generará tiempos muertos sin avanzar con la puesta en producción. Por favor confirmar.

RESPUESTA 157.-

Estimado oferente,

En el apartado IMPLEMENTACIÓN de la Sección VI. Requisitos de los Bienes y Servicios Conexos de la página 133 establece:

*“El servicio de implementación comprenderá las **etapas** que se indican a continuación, según corresponda a cada componente:*

6.a. Preparación,

6.b. Transición,

- 6.c. Puesta en producción,
- 6.d. Estabilización,
- 6.e. Documentación."

En la Sección VIII. Condiciones Especiales de Contrato (CEC), página 184:

- a) *"El plazo para la implementación del software y del servicio será de hasta 90 días calendario contados a partir del día siguiente a la fecha de activación del licenciamiento."*

En consecuencia, las actividades de preparación, transición, puesta en producción, estabilización y documentación, incluidas las coordinaciones necesarias para la ejecución de ventanas de mantenimiento con el SRI, deberán ser planificadas por el contratista dentro del plazo contractual establecido. Las ventanas de mantenimiento no suspenden ni amplían el plazo de implementación previsto en los pliegos.

PREGUNTA 158.-

Estimada entidad, entendemos que el en punto 10.e de la etapa de puesta en producción del punto INSTALACION, el acompañamiento a los administradores de los servidores de centros de datos, debe ser realizado por el fabricante para garantizar el funcionamiento dado la criticidad de la implementación.

RESPUESTA 158.-

Estimado oferente, el entendimiento no es correcto.

El numeral 10.e de la etapa Puesta en Producción establece que el contratista debe *"Proveer acompañamiento a los administradores de los servidores de centros de datos para instalar los correspondientes elementos de software de punto final incluidos en la solución"*, sin disponer que dicha actividad deba ser realizada exclusivamente por personal del fabricante.

Adicionalmente, el numeral 4 del apartado IMPLEMENTACIÓN establece que *"Todas las actividades de la implementación asociadas con la intervención de equipos tecnológicos deberán realizarse presencialmente por el personal técnico del Contratista"*.

De igual forma, el numeral 5 dispone que *"Todas las actividades de la etapa de puesta en producción asociadas con la intervención de equipos tecnológicos deberán realizarse presencialmente por el personal técnico del Contratista con la asistencia remota del personal especializado del fabricante"*.

Asimismo, el numeral 6 prevé que, si el SRI considera necesaria la intervención del personal especializado del fabricante en cualquiera de las etapas de implementación, podrá solicitarla formalmente, aplicándose el Acuerdo de Nivel de Servicio para Asistencia Técnica con prioridad 3.

En consecuencia, el acompañamiento previsto en el numeral 10.e debe ser proporcionado por el personal técnico del contratista, con la asistencia remota del personal especializado del fabricante durante la etapa de puesta en producción, conforme a lo establecido en la Solicitud de Ofertas (SDO).

PREGUNTA 159.-

Estimada entidad, en el punto 11.a de etapa de estabilización del punto INSTALACION, solicitamos que el parámetro definido para nivel de estabilidad razonable se ajuste a un 80% de los dispositivos.

RESPUESTA 159.-

El numeral 11.a de la etapa de Estabilización de IMPLEMENTACIÓN establece que el servicio debe *"Mantener monitoreados los nuevos componentes hasta certificar un nivel de estabilidad razonable para el SRI"*.

La estabilidad razonable será evaluada por el SRI en función del correcto funcionamiento de los componentes implementados, la ausencia de incidencias atribuibles a la implementación, la atención de las actividades de corrección y afinamiento que resulten necesarias y el cumplimiento de los demás requisitos técnicos y de aceptación establecidos en la Solicitud de Ofertas (SDO), previo a la suscripción del acta correspondiente.

PREGUNTA 160.-

Estimada entidad, dado que en el punto 11.e. de la etapa de estabilización, del punto IMPLEMENTACION, solicitan que el personal técnico especializado del fabricante de acompañamiento para disminuir el impacto de los problemas de la operación, entendemos que debe ser ese personal del fabricante quien realice todas las tareas de implementación en todas sus etapas

RESPUESTA 160.-

Estimado oferente, el entendimiento no es correcto.

El numeral 11.e de la etapa de Estabilización establece que el contratista debe "Proveer acompañamiento del personal técnico especializado del fabricante para resolver en el menor tiempo posible y con el mínimo impacto los problemas que impacten la operación institucional debido a la puesta en producción". Este requisito se refiere específicamente al acompañamiento durante la etapa de estabilización y para la atención de problemas derivados de la puesta en producción.

Por otra parte, el pliego establece expresamente que la responsabilidad de ejecutar las actividades de implementación corresponde al contratista. En efecto, el numeral 4 del apartado IMPLEMENTACIÓN dispone que "Todas las actividades de la implementación

asociadas con la intervención de equipos tecnológicos deberán realizarse presencialmente por el personal técnico del Contratista".

Asimismo, el numeral 5 establece que las actividades de la etapa de puesta en producción deberán ejecutarse presencialmente por el personal técnico del Contratista con la asistencia remota del personal especializado del fabricante.

Finalmente, el numeral 6 prevé que, si el SRI considera necesaria la intervención del personal especializado del fabricante en cualquiera de las etapas de implementación, podrá solicitarla formalmente, aplicándose el Acuerdo de Nivel de Servicio para Asistencia Técnica con prioridad 3.

En consecuencia, el requisito previsto en el numeral 11.e no implica que todas las actividades de implementación deban ser ejecutadas por personal del fabricante. La responsabilidad de la implementación corresponde al personal técnico del contratista, con la participación del personal especializado del fabricante únicamente en los casos expresamente previstos en la Solicitud de Oferta (SDO) o cuando el SRI lo requiera conforme al numeral 6.

PREGUNTA 161.-

Estimada entidad, en el punto DESPLIEGUE DEL HARDWARE, entendemos que el soporte de fábrica requerido para los componentes de hardware es por 3 años de servicio y que los mismos deben ser nuevos de fábrica. confirmar.

RESPUESTA 161.-

Estimado oferente, de conformidad con lo establecido en la Solicitud de Ofertas (SDO), los componentes de hardware incluidos en el servicio de gestión de ciberdefensa deberán contar con el licenciamiento, suscripciones, soporte de fábrica y garantía técnica necesarios para garantizar su adecuada operación durante toda la vigencia del contrato, conforme a los numerales 11 y 13 del apartado DESPLIEGUE DEL HARDWARE.

Asimismo, el numeral 10 del mismo apartado establece que el contratista deberá instalar la última versión estable liberada, con el último paquete de parches y actualizaciones del firmware y software de cada componente de hardware desplegado, y el numeral 12 dispone que es responsabilidad del proveedor realizar las actualizaciones periódicas de dichos componentes de acuerdo con las mejores prácticas del fabricante.

En consecuencia, los equipos suministrados podrán ser **nuevos o usados** siempre que garanticen la vigencia de la garantía técnica, el soporte oficial del fabricante y la posibilidad de recibir actualizaciones durante toda la ejecución del contrato. El soporte de fábrica deberá mantenerse por todo el período de vigencia contractual, de acuerdo con lo establecido en la Solicitud de la Oferta (SDO).

PREGUNTA 162.-

Estimada entidad solicitan Los equipos (hardware) incluidos deberán contar con la garantía técnica correspondiente que permita cumplir con los niveles de servicio solicitados por el SRI. Pregunta: la garantía técnica de los componentes de hardware debe estar a nombre del SRI o de la contratista?

RESPUESTA 162.-

De conformidad con lo establecido en el numeral 1 de la sección “DESPLIEGUE DEL HARDWARE”, se dispone que: *“Para la activación y funcionamiento de las licencias de software del componente Network Detection and Response (NDR), el contratista deberá incluir en el servicio de ciberdefensa, en calidad de préstamo, el hardware necesario para su operación, cumpliendo con lo establecido en los PRODUCTOS Y SERVICIOS ESPERADOS.”* En este sentido, considerando que el presente proceso contempla un esquema de provisión de servicio, en el cual el hardware requerido para la operación del componente NDR será entregado en calidad de préstamo durante la vigencia contractual, la garantía técnica podrá constar a nombre del contratista.

PREGUNTA 163.-

Estimada entidad, entendemos que el certificado de garantía técnica del hardware y la póliza de seguro del hardware deben estar a nombre del SRI. Confirmar.

RESPUESTA 163.-

Estimado oferente,

De conformidad con lo establecido en el numeral 1 de la sección “DESPLIEGUE DEL HARDWARE”, se dispone que: *“Para la activación y funcionamiento de las licencias de software del componente Network Detection and Response (NDR), el contratista deberá incluir en el servicio de ciberdefensa, en calidad de préstamo, el hardware necesario para su operación, cumpliendo con lo establecido en los PRODUCTOS Y SERVICIOS ESPERADOS.”* Dado que el hardware opera "en calidad de préstamo", el contratista no transfiere la propiedad al SRI, sino el servicio. En consecuencia, la póliza de seguro de los equipos y su garantía técnica permanecen como resguardo patrimonial del contratista y a su nombre.

PREGUNTA 164.-

Estimada entidad, los equipos deben estar a nombre del SRI o de la entidad contratista?

RESPUESTA 164.-

Estimado oferente,

De conformidad con lo establecido en el numeral 1 de la sección “DESPLIEGUE DEL HARDWARE”, se dispone que: *“Para la activación y funcionamiento de las licencias de*

software del componente Network Detection and Response (NDR), el contratista deberá incluir en el servicio de ciberdefensa, en calidad de préstamo, el hardware necesario para su operación, cumpliendo con lo establecido en los PRODUCTOS Y SERVICIOS ESPERADOS. Asimismo, al término del contrato, el contratista debe ejecutar un procedimiento de borrado seguro de datos “antes de que el contratista retire los equipos instalados” (numeral 15 de DESPLIEGUE DEL HARDWARE), lo cual indica que los equipos deben ser retirados por el contratista al finalizar la vigencia contractual.

En función de lo expuesto, debido a que hardware es ingresado a la institución "en calidad de préstamo", la propiedad legal de los equipos se mantiene bajo el nombre de la entidad contratista.

PREGUNTA 165.-

Estimada entidad, en el punto SERVICIO DE GESTIÓN DE CIBERDEFENSA, entendemos que en caso de un fallo en los elementos de hardware de los componentes tecnológicos que pertenecen al servicio que están desplegados en la red tecnológica del SRI, es necesario coordinar acciones con el administrador del contrato o cual sería el procedimiento para que el fabricante proceda con el cambio de la parte afectada. Confirmar.

RESPUESTA 165.-

El numeral 2 de las CONDICIONES GENERALES de METODOLOGÍA DE TRABAJO establece que *“Todas las actividades que impliquen cambios en la configuración, en la operación o en el nivel de seguridad informática de los sistemas o componentes instalados o desplegados que representen un impacto o afectación a la operación (...) deberán ser informadas al administrador del contrato y deberán ser aplicadas de manera controlada en coordinación con el personal del SRI.”* Adicionalmente, el numeral 7 del apartado SERVICIO DE GESTIÓN DE CIBERDEFENSA (Metodología) establece que *“Es responsabilidad del contratista realizar el mantenimiento periódico de los componentes tecnológicos incluidos en la solución contratada para garantizar su correcto funcionamiento y la entrega del servicio.”*

En función de lo expuesto ante un fallo de hardware, el contratista deberá notificar de inmediato al administrador del contrato conforme al numeral 2 citado, y ejecute el reemplazo de la parte afectada bajo su responsabilidad de mantenimiento (numeral 7 de SERVICIO DE GESTIÓN DE CIBERDEFENSA), coordinando con el fabricante correspondiente en función de la garantía técnica vigente (numeral 13 de DESPLIEGUE DEL HARDWARE).

PREGUNTA 166.-

Estimada entidad en el punto 4 DEL SERVICIO DE GESTION DE CIBERDEFENSA, entendemos que el SRI entregará credenciales al personal del servicio para la apertura del requerimiento en la herramienta de gestión tecnológica ITSM?. Confirmar.

RESPUESTA 166.-

Estimado oferente, su entendimiento es correcto.

PREGUNTA 167.-

Estimada entidad, en el punto 5 del numeral GESTION DE EVENTOS, entendemos que el contratista debe realizar las configuraciones necesarias y apoyar en los trabajos de integración de nuevos sistemas o servicios pero que el funcionamiento correcto de estos nuevos sistemas o servicios estará limitado por las características técnicas o de compatibilidad de estos nuevos componentes, y no es responsabilidad del contratista su funcionamiento.

RESPUESTA 167.-

Estimado oferente, en el numeral 5 de GESTIÓN DE EVENTOS (Metodología) establece que *“El servicio debe colaborar cuando el SRI requiera que otros sistemas o servicios, institucionales o contratados, se integren con los componentes tecnológicos incluidos en la solución contratada objeto de este contrato. Esto es, debe realizar las configuraciones necesarias y participar en los trabajos de integración.”*

Este numeral confirma la obligación del contratista de realizar configuraciones y participar en los trabajos de integración que le correspondan según sus capacidades técnicas y las especificaciones proporcionadas, sin que ello lo exima de reportar oportunamente al SRI cualquier limitación de compatibilidad detectada.

Se entiende razonable que el funcionamiento correcto de un sistema o servicio de terceros integrado dependa de las características técnicas y de compatibilidad propias de dicho componente.

PREGUNTA 168.-

Estimada entidad, los informes de avance de respuesta a incidentes, con que periodicidad se deben entregar; es decir, deben generarse a medida que se avanza con la respuesta al incidente dentro de periodos establecidos de tiempo o solo al final de la respuesta al incidente. Confirmar.

RESPUESTA 168.-

Estimado oferente,

En el apartado GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD numeral 34 para la etapa de **contención** se establece que: *“...Elaborar bajo demanda **los informes de avance de respuesta a incidente** ya sean operativos, tácticos y/o estratégicos, según lo requiera el SRI.”*

En el numeral 35 para la etapa de erradicación se establece que:

“...Elaborar bajo demanda los **informes de avance de respuesta a incidente** ya sean operativos, tácticos y/o estratégicos, según lo requiera el SRI.”

En el numeral 35 en la etapa de acciones posteriores se establece que:

“...Elaborar el(los) **informe(s) de cierre de respuesta a incidente**, operativo(s), táctico(s) y/o estratégico(s), según lo requiera el SRI;”

Asimismo, en el numeral 38 del mismo apartado se establece que:

*“Al final de cada periodo, y además bajo demanda, el servicio debe entregar **informes de gestión de incidentes de ciberseguridad** que demuestren la entrega efectiva del servicio y el beneficio que la institución ha obtenido por este, y que incluyan la información adicional que el SRI requiera en relación con este apartado.”*

En la Sección VIII. Condiciones Especiales de Contrato (CEC) en el apartado SERVICIO DE GESTIÓN DE CIBERDEFENSA - DOCUMENTOS Y ACTIVIDADES en los literales f se establece que: *“El plazo para la entrega de los informes de avance de respuesta a incidente será de hasta 4 horas hábiles contadas a partir de la hora de la solicitud.”* Asimismo, en el literal g se establece que: *“El plazo para la entrega de los informes de cierre de respuesta a incidente será de hasta 2 días hábiles contados a partir del día siguiente de la fecha de cierre del incidente.”*

En consecuencia, los informes de avance de respuesta a incidentes no tienen una periodicidad fija preestablecida, sino que deberán ser elaborados y entregados bajo demanda del SRI durante las etapas correspondientes considerando para su entrega el plazo máximo establecido. Además, el servicio deberá entregar informes de gestión de incidentes de ciberseguridad al final de cada periodo.

PREGUNTA 169.-

Estimada entidad, entendemos que en el punto 2 del numeral ACUERDO DE NIVEL DE SERVICIO, los tiempos indicados en la tabla 2 para contención de ciberamenazas, aplican únicamente para casos que no requieran de procesos, accesos u otro procedimiento sobre sistemas del SRI, y se puedan contener a través de las herramientas propias del servicio de Ciberdefensa.

RESPUESTA 169.-

Estimado oferente, su entendimiento es correcto.

En el numeral 2 del ACUERDO DE NIVEL DE SERVICIO establece textualmente que *“El tiempo de contención de ciberamenazas se define como el intervalo comprendido entre la materialización de una ciberamenaza (...) y el momento en que se logra detener su avance*

o propagación. La tabla 2 aplica únicamente a los casos en los que la contención se efectúa sin requerir intervención sobre los sistemas institucionales.”

PREGUNTA 170.-

Estimada entidad, entendemos que la tabla 2. Escala de tiempo del servicio en función de la prioridad, establece el tiempo máximo que puede transcurrir entre la notificación realizada por el personal del SRI con relación a Incidentes, Eventos y Requerimientos; y el tiempo de inicio de las actividades de análisis técnico por parte del personal del servicio. Confirmar.

RESPUESTA 170.-

Estimado oferente:

La Tabla 2. Escala de tiempo del servicio en función de la prioridad establece los umbrales máximos aceptables de atención para los incidentes, eventos de ciberseguridad, requerimientos de soporte técnico y contención de ciberamenazas, de acuerdo con la prioridad asignada.

Para efectos de interpretación, el tiempo de atención corresponde al intervalo comprendido entre el momento en que el SRI realiza el reporte de seguridad o requerimiento de soporte y el momento en que se inicia el análisis técnico por parte del personal asignado al servicio. En este sentido, la notificación automática de recepción del mensaje o confirmación de ingreso del requerimiento no será considerada como inicio de las actividades de análisis técnico.

Adicionalmente, para el caso específico de la contención de ciberamenazas, el tiempo establecido corresponde al intervalo comprendido entre la materialización de la ciberamenaza, identificada conforme a los registros de los sistemas y controles involucrados, y el momento en que se logra detener su avance o propagación. La escala definida para contención aplica únicamente cuando esta pueda efectuarse sin requerir intervención sobre los sistemas institucionales.

Por lo tanto, los tiempos establecidos en la Tabla 2 corresponden a los tiempos máximos permitidos para el inicio de la atención técnica de incidentes, eventos y requerimientos de soporte, así como para la ejecución de acciones de contención de ciberamenazas, conforme a las definiciones y condiciones establecidas en el apartado correspondiente.

PREGUNTA 171.-

Estimada entidad, en el punto INFORMACION QUE DISPONE LA ENTIDAD, al final tiene una nota que indica: "Toda la información de este apartado ha sido levantada hasta la fecha del presente documento, esta puede variar en función de la operación y..... Es responsabilidad del contratista hacer las validaciones correspondientes previo a la implementación.". Dado que se debe entregar una arquitectura y cotización basado en

los datos actuales entregados por el SRI, solicitamos que se permita realizar un nuevo assessment previo a la entrega de ofertas para dimensionar nuevamente, ya que si hay cambios hacia la implementación, no es posible reaccionar con nueva arquitectura o precios.

RESPUESTA 171.-

Estimado oferente, acorde a los plazos previstos, no están autorizadas las evaluaciones in-situ (assessments) en el transcurso de la etapa precontractual. Las especificaciones de tráfico actual (y la estimación del 5% anual estipulada) componen el insumo central suficiente para un dimensionamiento referencial y escalable que asuma la variabilidad regular del mercado.

PREGUNTA 173.-

Estimada entidad, EN EL ítem SERVICIOS CONEXOS REQUERIDOS en el punto 3 del literal A. CONDICIONES GENERALES, los componentes de hardware y de software que se requieran desplegar en la red tecnológica del SRI serán provistos por el contratista. Pregunta: Estos equipos deben ser nuevos y con soporte del fabricante o pueden ser refurbished?. En caso de que deban ser nuevos, el soporte debe estar a nombre del contratista o del SRI.

RESPUESTA 173.-

Estimado oferente, de conformidad con lo establecido en la Solicitud de Ofertas (SDO), los componentes de hardware incluidos en el servicio de gestión de ciberdefensa deberán contar con el licenciamiento, suscripciones, soporte de fábrica y garantía técnica necesarios para garantizar su adecuada operación durante toda la vigencia del contrato, conforme a los numerales 11 y 13 del apartado DESPLIEGUE DEL HARDWARE. Asimismo, el numeral 10 del mismo apartado establece que el contratista deberá instalar la última versión estable liberada, con el último paquete de parches y actualizaciones del firmware y software de cada componente de hardware desplegado, y el numeral 12 dispone que es responsabilidad del proveedor realizar las actualizaciones periódicas de dichos componentes de acuerdo con las mejores prácticas del fabricante.

En consecuencia, los equipos suministrados podrán ser **nuevos o usados** siempre que garanticen la vigencia de la garantía técnica, el soporte oficial del fabricante y la posibilidad de recibir actualizaciones durante toda la ejecución del contrato. El soporte de fábrica deberá mantenerse por todo el período de vigencia contractual, de acuerdo con lo establecido en la Solicitud de la Oferta (SDO).

PREGUNTA 174.-

Estimada entidad, entendemos que para realizar el servicio de ciberdefensa, las funciones tecnológicas solicitadas en el punto SERVICIO DE GESTIÓN DE CIBERDEFENSA, se requiere que el EDR, NDR y todos los elementos de hardware y software usados para Gestión de amenazas, Inteligencia unificada y respuesta unificada; cuenten con equipos nuevos de fábrica y licenciamiento activo durante el periodo de servicio a ser entregado? o es posible usar equipos refurbished para entregar el servicio?

RESPUESTA 174.-

Estimado oferente, de conformidad con lo establecido en la Solicitud de Ofertas (SDO), los componentes de hardware incluidos en el servicio de gestión de ciberdefensa deberán contar con el licenciamiento, suscripciones, soporte de fábrica y garantía técnica necesarios para garantizar su adecuada operación durante toda la vigencia del contrato, conforme a los numerales 11 y 13 del apartado DESPLIEGUE DEL HARDWARE.

Asimismo, el numeral 10 del mismo apartado establece que el contratista deberá instalar la última versión estable liberada, con el último paquete de parches y actualizaciones del firmware y software de cada componente de hardware desplegado, y el numeral 12 dispone que es responsabilidad del proveedor realizar las actualizaciones periódicas de dichos componentes de acuerdo con las mejores prácticas del fabricante.

En consecuencia, los equipos suministrados podrán ser **nuevos o usados** siempre que garanticen la vigencia de la garantía técnica, el soporte oficial del fabricante y la posibilidad de recibir actualizaciones durante toda la ejecución del contrato. El soporte de fábrica deberá mantenerse por todo el período de vigencia contractual, de acuerdo con lo establecido en la Solicitud de la Oferta (SDO).

PREGUNTA 175.-

Estimada Entidad, dado que en el literal B. PRESTACIONES DEL SERVICIO DE GESTIÓN DE CIBERDEFENSA, se indica que el equipo MDR del fabricante debe realizar la gestión de ciberdefensa, entendemos que todo el hardware y software que se utilice debe ser adquirido al fabricante con licenciamiento por el tiempo del servicio y debe ser nuevo de fábrica. Confirmar

RESPUESTA 175.-

Estimado oferente, de conformidad con lo establecido en la Solicitud de Ofertas (SDO), los componentes de hardware incluidos en el servicio de gestión de ciberdefensa deberán contar con el licenciamiento, suscripciones, soporte de fábrica y garantía técnica necesarios para garantizar su adecuada operación durante toda la vigencia del contrato, conforme a los numerales 11 y 13 del apartado DESPLIEGUE DEL HARDWARE.

Asimismo, el numeral 10 del mismo apartado establece que el contratista deberá instalar la última versión estable liberada, con el último paquete de parches y actualizaciones del firmware y software de cada componente de hardware desplegado, y el numeral 12 dispone que es responsabilidad del proveedor realizar las actualizaciones periódicas de dichos componentes de acuerdo con las mejores prácticas del fabricante.

En consecuencia, los equipos suministrados podrán ser **nuevos o usados** siempre que garanticen la vigencia de la garantía técnica, el soporte oficial del fabricante y la posibilidad de recibir actualizaciones durante toda la ejecución del contrato. El soporte de fábrica deberá mantenerse por todo el período de vigencia contractual, de acuerdo con lo establecido en la Solicitud de la Oferta (SDO).

PREGUNTA 176.-

Estimada entidad, en el punto 6 del literal B PRESTACIONES DEL SERVICIO DE GESTIÓN DE CIBERDEFENSA, entendemos que el SRI nos entregará como insumo el análisis de riesgos para la clasificación de incidentes. Confirmar.

RESPUESTA 176.-

Estimado oferente,

El numeral 6 del literal B. Monitoreo de Amenazas de Ciberseguridad establece expresamente que *"el servicio debe realizar la clasificación de las alertas de amenazas en eventos e incidentes de ciberseguridad en función de una escala común acordada con el SRI"*.

En consecuencia, la responsabilidad de realizar la clasificación de las alertas corresponde al servicio de gestión de ciberdefensa, utilizando una escala común que será acordada entre el contratista y el SRI durante la ejecución del contrato. La Solicitud de Ofertas (SDO) no establece que el SRI deba proporcionar un análisis de riesgos institucional preexistente como insumo para efectuar dicha clasificación.

Por tanto, el oferente deberá considerar en su propuesta los recursos, metodologías y capacidades necesarias para efectuar la clasificación de eventos e incidentes conforme a los requisitos establecidos en la Solicitud de Oferta (SDO), en coordinación con el SRI para la definición de la escala común aplicable.

PREGUNTA 177.-

Estimada entidad, en GESTIÓN DE EVENTOS DE CIBERSEGURIDAD punto 20, dado que las tareas pueden ser ilimitadas y de cualquier índole, solicitamos se pueda aclarar la cantidad estimada y tipo de tarea, para poder realizar un costeo ajustado a realidad de mercado, caso contrario para los oferentes sería difícil estimar un costo para este rubro

RESPUESTA 177.-

Estimado oferente, el numeral 20 de GESTIÓN DE EVENTOS DE CIBERSEGURIDAD establece que *“El servicio debe configurar, probar y estabilizar la automatización de las tareas que el personal de SRI solicite mediante la función central de respuesta unificada de ciberdefensa incluida en el servicio.”*

La Solicitud de Oferta (SDO) no establece una cantidad estimada de tareas para el cumplimiento del numeral 20 del apartado GESTIÓN DE EVENTOS DE CIBERSEGURIDAD, debido a que estas dependerán de la naturaleza, volumen y complejidad de los eventos de ciberseguridad que se presenten durante la ejecución del contrato.

En consecuencia, el oferente deberá dimensionar su propuesta considerando la prestación integral del servicio y el cumplimiento de todos los requerimientos técnicos y niveles de servicio establecidos en la SDO. Las tareas que se ejecuten estarán relacionadas con el objeto del contrato y con las actividades previstas en los documentos del proceso para la gestión de eventos de ciberseguridad.

PREGUNTA 178.-

Estimada entidad, en NETWORK DETECTION AND RESPONSE (NDR) en el punto 26 se indica que la función NDR puede operar en modo SaaS o localmente, entendemos que en caso de operar en modo SaaS, los motores de análisis y detección deben funcionar de forma local, para garantizar la capacidad de detección de amenazas en todos los componentes locales, inclusive en caso de fallas de conexión a la nube.

RESPUESTA 178.-

Estimado oferente,

La SDO no establece como requisito que, para soluciones con operación en modalidad SaaS, los motores de análisis y detección deban continuar operando localmente ante una pérdida de conectividad con la nube. Por tanto, corresponde a los oferentes diseñar y proponer la arquitectura de su solución, siempre que esta cumpla íntegramente con los requisitos funcionales, técnicos y de niveles de servicio establecidos en la Solicitud de Oferta (SDO), considerando que independientemente de cómo se distribuyan los componentes de la solución NDR los equipos de propósito específico desplegados en los centros de cómputo deben tener la capacidad de detectar y contener las ciberamenazas aún cuando se pierda el acceso a internet.

PREGUNTA 179.-

Estimada entidad, en NETWORK DETECTION AND RESPONSE (NDR) en el punto 27 se indica que la función NDR debe desplegarse en equipos de propósito específico. Entendemos por tanto que se debe colocar equipos catalogados por el fabricante como

especializados para realizar tareas de NDR y no máquinas virtuales sobre servidores para ejecutar esta función. Por favor confirmar

RESPUESTA 179.-

Estimado oferente, el numeral 27 de NETWORK DETECTION AND RESPONSE (NDR) establece que: *“La función NDR debe desplegarse en los dos centros de cómputo del SRI (‘on-premise’), mediante la instalación de equipos de propósito específico.”*

Se solicita la instalación de equipos (hardware) de propósito específico.

PREGUNTA 180.-

Estimada entidad, en NETWORK DETECTION AND RESPONSE (NDR) en el punto 27 se indica que la función NDR debe desplegarse en equipos de propósito específico. Entendemos por tanto que se debe colocar equipos nuevos y con soporte del fabricante, por favor confirmar.

RESPUESTA 180.-

Estimado oferente, de conformidad con lo establecido en la Solicitud de Ofertas (SDO), los componentes de hardware incluidos en el servicio de gestión de ciberdefensa deberán contar con el licenciamiento, suscripciones, soporte de fábrica y garantía técnica necesarios para garantizar su adecuada operación durante toda la vigencia del contrato, conforme a los numerales 11 y 13 del apartado DESPLIEGUE DEL HARDWARE.

Asimismo, el numeral 10 del mismo apartado establece que el contratista deberá instalar la última versión estable liberada, con el último paquete de parches y actualizaciones del firmware y software de cada componente de hardware desplegado, y el numeral 12 dispone que es responsabilidad del proveedor realizar las actualizaciones periódicas de dichos componentes de acuerdo con las mejores prácticas del fabricante.

En consecuencia, los equipos suministrados podrán ser **nuevos o usados** siempre que garanticen la vigencia de la garantía técnica, el soporte oficial del fabricante y la posibilidad de recibir actualizaciones durante toda la ejecución del contrato. El soporte de fábrica deberá mantenerse por todo el período de vigencia contractual, de acuerdo con lo establecido en la Solicitud de la Oferta (SDO).

PREGUNTA 181.-

Estimada entidad, en el punto 29 de NETWORK DETECTION AND RESPONSE (NDR), entendemos que varios de los dispositivos listados en la tabla 6, tienen ambiente virtualizado con VmWare y tráfico que se mueve en este entorno, por tanto, sería necesario que la herramienta NDR pueda inspeccionar el tráfico dentro de estos ambientes.

RESPUESTA 181.-

Estimado oferente,

La SDO no establece como requisito específico que la función NDR deba inspeccionar el tráfico interno de los entornos virtualizados VMware, ni exige una tecnología o mecanismo particular para lograr dicho monitoreo.

PREGUNTA 182.-

Estimada entidad, entendemos que el SRI cuenta con un directorio activo donde está claramente identificable las cuentas privilegiadas y las cuentas de servicio y se podrá contar con el acceso al AD. Por favor confirmar.

RESPUESTA 182.-

Estimado oferente, el numeral 74 del apartado GESTIÓN DE AMENAZAS DE IDENTIDAD establece que: *“La gestión de amenazas de identidad debe identificar automáticamente cuentas de servicio o cuentas privilegiadas mediante aprendizaje automático (ML).”*

Asimismo, el numeral 63 dispone: *“La gestión de amenazas de identidad debe integrarse al sistema de directorio Microsoft del SRI (ver **INFRAESTRUCTURA ACTUAL**).”*

En consecuencia, el componente ofertado debe cumplir con la capacidad de identificación automática prevista en la Solicitud de Ofertas (SDO) utilizando la información obtenida mediante dicha integración.

La información adicional será proporcionada por el administrador de contrato en la fase correspondiente.

PREGUNTA 183.-

Estimada entidad, en el punto 96 de INTELIGENCIA UNIFICADA DE CIBERDEFENSA, se indica: “NOTA: Es responsabilidad del contratista incluir la cantidad de espacio SaaS necesario en el componente central de inteligencia unificada de ciberdefensa para que este opere adecuadamente, en función de la cantidad efectiva de datos que reciba del entorno institucional.”, entendemos que en este punto se validará que el contratista cumpla con la cantidad de espacio SaaS necesario, en base a la tabla 9, donde se indica las cantidades estimadas actuales y el crecimiento de tráfico estimado anual del 5%.

RESPUESTA 183.-

Estimado oferente, su entendimiento es correcto, el numeral 96 de INTELIGENCIA UNIFICADA DE CIBERDEFENSA establece que:

“La capacidad de almacenamiento y de procesamiento del componente central de inteligencia unificada de ciberdefensa debe estar dimensionada para soportar la carga y análisis AI y ML de eventos de los componentes de detección y respuesta (“DR”) incluidos

en la solución contratada y de los componentes tecnológicos institucionales en relación con lo estimado en la **tabla 9**.

NOTA: Es responsabilidad del contratista incluir la cantidad de espacio SaaS necesario en el componente central de inteligencia unificada de ciberdefensa para que este opere adecuadamente, en función de la cantidad efectiva de datos que reciba del entorno institucional.”

La Tabla 9 (numeral 12 de INFRAESTRUCTURA ACTUAL) presenta las cantidades estimadas por componente tecnológico e incluye la nota de que *"Se estima que el crecimiento del tráfico puede llegar al 5% anual"*. Esta información constituye un insumo para el dimensionamiento de la solución. En concordancia con el numeral 96 de INTELIGENCIA UNIFICADA DE CIBERDEFENSA, corresponde al contratista dimensionar el espacio SaaS necesario para garantizar la correcta operación del componente central, considerando la cantidad efectiva de datos del entorno institucional y la información referencial proporcionada por el SRI, incluida la estimación de crecimiento contenida en la Tabla 9.

PREGUNTA 184.-

Estimada entidad, en el punto 95 de INTELIGENCIA UNIFICADA DE CIBERDEFENSA, se indica: El componente central de inteligencia, entendemos que en este punto se validará que el contratista cumpla con retención al menos 6 meses de los datos acopiados, dado que en el punto PROTECCION DE DATOS INSTITUCIONALES EN COMPONENTE SAAS del literal A CONDICIONES GENERALES ya solicitan que los logs para auditoria del SRI deben tener mínimo seis meses.

RESPUESTA 184.-

Estimado oferente, el numeral 95 de INTELIGENCIA UNIFICADA DE CIBERDEFENSA establece que:

*"El componente central de inteligencia unificada de ciberdefensa puede ser de tipo **Extended Detection and Response (XDR)** o **Next Generation SIEM (NGSIEM)** o una combinación de estos."*

Este numeral no se refiere a la retención de datos.

En el numeral 97 de la misma sección se establece que:

"El componente central de inteligencia unificada de ciberdefensa debe garantizar la retención de los datos de acuerdo con la siguiente priorización:

- *Datos acopiados: un (1) mes,*
- *Datos producidos por el análisis: seis (6) meses."*

En función de lo expuesto, los datos acopiados deben retenerse un mínimo de un (1) mes, y no de seis (6) meses; el periodo de seis (6) meses aplica a los “datos producidos por el análisis”, es decir, a los resultados del procesamiento (alertas, correlaciones, investigaciones, etc), no a los datos acopiados.

La referencia realizada en la pregunta con respecto al periodo de seis meses de retención de logs de auditoría que registren las acciones de administración en las interfaces gráficas de gestión (numeral 11 de PROTECCIÓN DE DATOS INSTITUCIONALES EN COMPONENTES SAAS) corresponde a un requisito distinto.

PREGUNTA 185.-

Estimada entidad, en RESPUESTA UNIFICADA DE CIBERDEFENSA en el punto 134, se solicita: “La función central de respuesta unificada de ciberdefensa debe operar en modo SaaS ...”, entendemos que aun cuando la función central de respuesta unificada opere en modo SaaS, y dado que la infraestructura a monitorear está OnPremise; la función debe garantizar la operación de forma local, aun cuando exista una desconexión de internet o de la nube.

RESPUESTA 185.-

Estimado oferente,

En atención a su consulta, se aclara que el requerimiento establecido en el punto 134 de RESPUESTA UNIFICADA DE CIBERDEFENSA establece que la función central de respuesta unificada de ciberdefensa deberá operar en modo SaaS.

El requerimiento no establece ni implica que la función deba garantizar una operación local o autónoma ante una eventual desconexión de Internet o de la plataforma en la nube.

Por lo tanto, no es correcto el entendimiento planteado. Lo solicitado por la entidad es que la función central de respuesta unificada de ciberdefensa opere bajo un modelo SaaS, conforme a las demás especificaciones técnicas establecidas para este componente.

PREGUNTA 186.-

Estimada entidad, en el punto SERVICIO DE GESTIÓN DE CIBERDEFENSA, entendemos que la multa aplicada a excesos en resolver incidentes de ciberseguridad se refiere a los tiempos establecidos en la Tabla 2, para atención y respuesta a incidentes y eventos de ciberseguridad, más no a tiempos de resolución ya que estos dependerán de intervención en dispositivos y componentes del SRI que requieren permisos de acceso y configuraciones a cargo de personal del SRI u otros fabricantes, sobre los cuales no tenemos control de su disponibilidad.

RESPUESTA 186.-

Estimado oferente:

Se aclara que, para **INCIDENTES DE CIBERSEGURIDAD, EVENTOS DE CIBERSEGURIDAD y REQUERIMIENTOS DE SOPORTE TÉCNICO** se aplica los tiempos establecidos para cada prioridad en la “Tabla 2. Escala de tiempo del servicio en función de la prioridad.”, considerando que *“El tiempo de atención se define como el intervalo comprendido entre el momento en que el SRI realiza un reporte de seguridad o requerimiento de soporte y el momento en que se inicia el análisis técnico por parte del personal del servicio. La notificación automática de recepción del mensaje no es aceptada como el inicio del análisis técnico.”*

Por lo tanto, el contratista deberá iniciar la atención de la solicitud realizada por el SRI en los tiempos correspondientes a cada prioridad, dejando constancia de que se inició el análisis técnico con evidencia verificable y auditable que permita determinar la fecha y hora en la que el personal especializado del servicio inició las actividades de análisis, investigación o gestión correspondientes.

Para tal efecto, será responsabilidad del contratista mantener una bitácora o registro de las actividades realizadas, la cual deberá contener la información y los respaldos, documentos, registros, evidencias técnicas o cualquier otro material pertinente que permita verificar y acreditar de manera objetiva las actividades ejecutadas, así como el cumplimiento de los tiempos establecidos en la tabla de niveles de servicio.

Respecto al tiempo de resolución de incidentes, este deberá entenderse como el tiempo requerido para ejecutar las actividades de contención de ciberamenazas, cuyo plazo máximo establecido es de cuatro (4) horas, conforme a lo indicado en la Tabla 2 del Acuerdo de Nivel de Servicio.

Este tiempo de contención será aplicable de manera uniforme, independientemente de la prioridad asignada al incidente.

Considerando que:

*“El tiempo de contención de ciberamenazas se define como el intervalo comprendido entre la materialización de una ciberamenaza –según los registros de los sistemas y controles involucrados– y el momento en que se logra detener su avance o propagación. La **tabla 2** aplica únicamente a los casos en los que la contención se efectúa sin requerir intervención sobre los sistemas institucionales.”*

PREGUNTA 187.-

Estimada entidad, en el punto SERVICIO DE GESTIÓN DE CIBERDEFENSA, entendemos que la multa aplicada a excesos en resolver incidentes de ciberseguridad se refiere a los tiempos establecidos en la Tabla 2, para Contención de Amenazas usando las herramientas del servicio adquirido, siempre que no involucren dispositivos y

componentes del SRI que requieren permisos de acceso y configuraciones a cargo de personal del SRI u otros fabricantes, sobre los cuales no tenemos control de su disponibilidad.

RESPUESTA 187.-

Estimado oferente:

Se aclara que, para **INCIDENTES DE CIBERSEGURIDAD, EVENTOS DE CIBERSEGURIDAD y REQUERIMIENTOS DE SOPORTE TÉCNICO** se aplica los tiempos establecidos para cada prioridad en la “Tabla 2. Escala de tiempo del servicio en función de la prioridad.”, considerando que *“El tiempo de atención se define como el intervalo comprendido entre el momento en que el SRI realiza un reporte de seguridad o requerimiento de soporte y el momento en que se inicia el análisis técnico por parte del personal del servicio. La notificación automática de recepción del mensaje no es aceptada como el inicio del análisis técnico.”*

Por lo tanto, el contratista deberá iniciar la atención de la solicitud realizada por el SRI en los tiempos correspondientes a cada prioridad, dejando constancia de que se inició el análisis técnico con evidencia verificable y auditable que permita determinar la fecha y hora en la que el personal especializado del servicio inició las actividades de análisis, investigación o gestión correspondientes.

Para tal efecto, será responsabilidad del contratista mantener una bitácora o registro de las actividades realizadas, la cual deberá contener la información y los respaldos, documentos, registros, evidencias técnicas o cualquier otro material pertinente que permita verificar y acreditar de manera objetiva las actividades ejecutadas, así como el cumplimiento de los tiempos establecidos en la tabla de niveles de servicio.

Respecto al tiempo de resolución de incidentes, este deberá entenderse como el tiempo requerido para ejecutar las actividades de contención de ciberamenazas, cuyo plazo máximo establecido es de cuatro (4) horas, conforme a lo indicado en la Tabla 2 del Acuerdo de Nivel de Servicio.

Este tiempo de contención será aplicable de manera uniforme, independientemente de la prioridad asignada al incidente.

Considerando que:

*“El tiempo de contención de ciberamenazas se define como el intervalo comprendido entre la materialización de una ciberamenaza –según los registros de los sistemas y controles involucrados– y el momento en que se logra detener su avance o propagación. La **tabla 2** aplica únicamente a los casos en los que la contención se efectúa sin requerir intervención sobre los sistemas institucionales.”*

Por lo tanto, los tiempos asociados a la atención y respuesta de incidentes contemplados en dicha tabla serán considerados únicamente cuando las actividades de contención puedan ser ejecutadas directamente dentro del alcance operativo del servicio contratado.

PREGUNTA 188.-

Estimada entidad, se solicita de la manera mas comedida se permita presentar en el personal técnico ingeniero o tecnólogo, ya que tecnólogo también es reconocido como título de tercer nivel. Por favor confirmar

RESPUESTA 188.-

Estimado oferente,

Para la validación del personal técnico mínimo, se deberá presentar la documentación que respalde que el título de Tecnólogo corresponda a un nivel de estudio de tercer nivel, adicional deberá cumplir con el requisito de titulación académica solicitada para cada rol.

PREGUNTA 189.-

Estimada entidad, en el documento términos de referencia en el punto 149 solicitan: La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes controles de ciberseguridad institucionales: Check Point VSX, Proofpoint Core Email protection, Broadcom/Symantec ProxySG, Otros controles de ciberseguridad existentes con los que el servicio requiera integrarse para realizar acciones de contención. Se entiende que el servicio integrará las tecnologías mencionadas, y que si se necesita apoyo por parte del administrador o proveedor de cada componente a integrar, para garantizar un adecuado proceso el SRI lo gestionará. Por favor confirmar

RESPUESTA 189.-

Estimado oferente,

Dependiendo de la naturaleza y funciones del componente tecnológico al que se tenga que integrar el SRI proveerá la asistencia o acompañamiento del administrador del componente, del proveedor o del fabricante según corresponda en cada caso.

PREGUNTA 190.-

Estimada entidad, en el documento términos de referencia en el punto 149 solicitan: La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes controles de ciberseguridad institucionales: Check Point VSX, Proofpoint Core Email protection, Broadcom/Symantec ProxySG, Otros controles de ciberseguridad existentes con los que el servicio requiera integrarse para realizar acciones de contención. Se entiende que el soporte de las tecnologías a integrar

no son alcance del servicio actual, y que cualquier configuración o soporte requerido en las tecnologías que no hacen parte del contrato, el SRI debe garantizar que se realice a través de sus respectivos proveedores. Por favor confirmar

RESPUESTA 190.-

Estimado oferente,

El soporte de las herramientas institucionales no es parte del objeto de contratación, sin embargo, el oferente que resulte adjudicado debe dar las instrucciones necesarias para lograr la integración de los controles y componentes tecnológicos del SRI con la solución ofertada.

PREGUNTA 191.-

Estimada entidad, en el documento términos de referencia en el punto 149 solicitan: La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes controles de ciberseguridad institucionales: Check Point VSX, Proofpoint Core Email protection, Broadcom/Symantec ProxySG, Otros controles de ciberseguridad existentes con los que el servicio requiera integrarse para realizar acciones de contención. Se entiende que toda la documentación necesaria de los componentes a integrar será suministrada por el proveedor. Por favor confirmar

RESPUESTA 191.-

Estimado oferente,

En el numeral 149 del apartado RESPUESTA UNIFICADA DE CIBERDEFENSA se solicita que:

“La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes controles de ciberseguridad institucionales:

- *Check Point VSX,*
- *Proofpoint Core Email protection,*
- *Broadcom/Symantec ProxySG,*
- *Otros controles de ciberseguridad existentes con los que el servicio requiera integrarse para realizar acciones de contención.*

NOTAS:

1. *Es responsabilidad del contratista incluir en la función central de respuesta unificada de ciberdefensa las integraciones y las acciones de respuesta necesarias para lograr una respuesta efectiva y oportuna ante amenazas de ciberseguridad en el entorno institucional.*

2. *El alcance de cada integración puede variar a medida que los fabricantes involucrados liberen nuevas versiones.”*

En función de lo expuesto, el componente central de inteligencia unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los controles de ciberseguridad detallados en el requerimiento, para este fin se admite desarrollos personalizados y el uso de protocolos estándar (SYSLOG, API).
Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 192.-

Estimada entidad, en el documento términos de referencia en el punto 153 solicitan: La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes componentes tecnológicos institucionales: Microsoft Exchange (local y online), Palo Alto Networks ION SDWAN, IBM Verify Identity Governance, VMware vCenter/vSphere, Otros componentes tecnológicos existentes con los que el servicio requiera integrarse para realizar acciones de contención. Se entiende que el servicio integrará las tecnologías mencionadas, y que, si se necesita apoyo por parte del administrador o proveedor de cada componente a integrar, para garantizar un adecuado proceso el SRI lo gestionará. Por favor confirmar

RESPUESTA 192.-

Estimado oferente,
En el numeral 153 del apartado RESPUESTA UNIFICADA DE CIBERDEFENSA se solicita que:

“La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes componentes tecnológicos institucionales:

- *Microsoft Exchange (local y online),*
- *Palo Alto Networks ION SDWAN,*
- *IBM Verify Identity Governance,*
- *VMware vCenter/vSphere,*
- *Otros componentes tecnológicos existentes con los que el servicio requiera integrarse para realizar acciones de contención.*

NOTAS:

- 1. Es responsabilidad del contratista incluir en la función central de respuesta unificada de ciberdefensa las integraciones y las acciones de respuesta necesarias para lograr una respuesta efectiva y oportuna ante amenazas de ciberseguridad en el entorno institucional.*
- 2. El alcance de cada integración puede variar a medida que los fabricantes involucrados liberen nuevas versiones.”*

En función de lo expuesto, el componente central de inteligencia unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los controles de ciberseguridad detallados en el requerimiento, para este fin se admite desarrollos

personalizados y el uso de protocolos estándar (SYSLOG, API).
Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 193.-

Estimada entidad, en el documento términos de referencia en el punto 153 solicitan: La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes componentes tecnológicos institucionales: Microsoft Exchange (local y online), Palo Alto Networks ION SDWAN, IBM Verify Identity Governance, VMware vCenter/vSphere, Otros componentes tecnológicos existentes con los que el servicio requiera integrarse para realizar acciones de contención. Se entiende que el soporte de las tecnologías a integrar no son alcance del servicio actual, y que cualquier configuración o soporte requerido en las tecnologías que no hacen parte del contrato, el SRI debe garantizar que se realice a través de sus respectivos proveedores. Por favor confirmar

RESPUESTA 193.-

Estimado oferente,
El soporte de las herramientas institucionales no es parte del objeto de contratación, sin embargo, el oferente que resulte adjudicado debe dar las instrucciones necesarias para lograr la integración de los controles y componentes tecnológicos del SRI con la solución ofertada.

PREGUNTA 194.-

Estimada entidad, en el documento términos de referencia en el punto 153 solicitan: La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes componentes tecnológicos institucionales: Microsoft Exchange (local y online), Palo Alto Networks ION SDWAN, IBM Verify Identity Governance, VMware vCenter/vSphere, Otros componentes tecnológicos existentes con los que el servicio requiera integrarse para realizar acciones de contención. Se entiende que toda la documentación necesaria de los componentes a integrar será suministrada por el proveedor. Por favor confirmar

RESPUESTA 194.-

Estimado oferente,
En el numeral 153 del apartado RESPUESTA UNIFICADA DE CIBERDEFENSA se solicita que:

“La función central de respuesta unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los siguientes componentes tecnológicos institucionales:

- *Microsoft Exchange (local y online),*

- Palo Alto Networks ION SDWAN,
- IBM Verify Identity Governance,
- VMware vCenter/vSphere,
- Otros componentes tecnológicos existentes con los que el servicio requiera integrarse para realizar acciones de contención.

NOTAS:

1. Es responsabilidad del contratista incluir en la función central de respuesta unificada de ciberdefensa las integraciones y las acciones de respuesta necesarias para lograr una respuesta efectiva y oportuna ante amenazas de ciberseguridad en el entorno institucional.

2. El alcance de cada integración puede variar a medida que los fabricantes involucrados liberen nuevas versiones.”

En función de lo expuesto, el componente central de inteligencia unificada de ciberdefensa debe ser capaz de realizar tareas automáticas a través de los controles de ciberseguridad detallados en el requerimiento, para este fin se admite desarrollos personalizados y el uso de protocolos estándar (SYSLOG, API).

Es responsabilidad del oferente mantener actualizado y funcional este desarrollo.

PREGUNTA 195.-

Estimada entidad, en el ítem 86, solicitan: Para determinar anomalías de comportamiento, la gestión de amenazas de identidad debe detectar accesos sospechosos a servidores críticos. Pregunta: "Teniendo en cuenta que la definición de servidores críticos depende de los procesos internos de la compañía y su definición precede de un análisis de riesgos y criticidad de los procesos y aplicaciones internas, se entiende que el SRI entregará la información relevante sobre los servidores críticos." Por favor confirmar

RESPUESTA 195.-

Estimado oferente, el SRI suministrará al proveedor adjudicado la información correspondiente para el desarrollo del contrato.

PREGUNTA 196.-

Por favor solicitamos se permita justificar los requerimientos técnicos con manuales del fabricante en idioma inglés, ya que los fabricantes publican la información técnica y actualizada en este idioma y no se dispone de toda la documentación en español. Adicionalmente las traducciones de palabras técnicas del inglés al español no siempre son correctas gramaticalmente, ejemplo: tracer – tracear, ping – pingear, multitenant – inquilino múltiple.

RESPUESTA 196.-

Estimado oferente, no es posible acoger su requerimiento. La documentación técnica deberá contar con su respectiva traducción fidedigna al idioma español, y el oferente deberá garantizar que las traducciones de los términos técnicos sean gramaticalmente correctas, a fin de asegurar un adecuado entendimiento por parte del Comité Técnico de Evaluación y Selección.

PREGUNTA 197.-

Estimada entidad, solicitan en el ítem IAO 11.1 Idioma de la oferta que la oferta sea en idioma español, se solicita de la manera más comedida se permita presentar la parte de la documentación técnica del fabricante (datasheets) en idioma inglés ya que es el idioma que manejan la mayoría de fabricantes y se pierde contexto en las traducciones.

RESPUESTA 197.-

Estimado oferente, no es posible acoger su requerimiento. La documentación técnica del fabricante (datasheets) deberá contar con su respectiva traducción fidedigna al idioma español, y el oferente deberá garantizar que las traducciones de los términos técnicos sean gramaticalmente correctas, a fin de asegurar un adecuado entendimiento por parte del Comité Técnico de Evaluación y Selección.

PREGUNTA 198.-

Estimada entidad en el apartado IAO 12.1(j) en el ítem b) Solicitan: Copia simple de la constancia de inscripción del documento de constitución en los registros públicos del país de origen. Por favor mencionar que documento se debe entregar para este cumplimiento. Gracias

RESPUESTA 198.-

Estimado oferente, el documento que deberá presentarse corresponde a la inscripción de la compañía en el Registro Mercantil y la de su representante legal, o, en su defecto, ante la entidad competente del país de origen de la compañía.

PREGUNTA 200.-

Estimada entidad, en el ítem Capacidad Financiera: en la facturación promedio anual solicitan i. El contratista deberá demostrar su capacidad financiera para llevar a cabo el cumplimiento de sus obligaciones contractuales, sus ventas deben ser el promedio anual de los últimos 5 años con cierre fiscal cuyo resultado debe ser mayor o igual a USD 888.524,75 (25%) del presupuesto referencial sin incluir impuestos. Si la oferta es presentada en consorcio el resultado del cierre fiscal sería la suma de las 2 empresas que conformen el consorcio? Por favor confirmar

RESPUESTA 200.-

Estimado Oferente, las 2 empresas que conformen el consorcio deben cumplir de manera conjunta el parámetro establecido, de acuerdo con los parámetros descritos en los DDL en la Sección III. Criterios de Evaluación y Calificación de los DDL que indican:

“Para oferentes en Asociación en participación, consorcio o asociación (APCA), se sumará el valor de todos los integrantes que deberán cumplir con el parámetro establecido, de la siguiente manera:

Integrante líder: Al menos el 50% del parámetro establecido

Otros participantes del APCA: Al menos el 10% del parámetro establecido”.

“La evidencia documentada que se requiere para acreditar el cumplimiento de estos requisitos es:

En relación con los últimos 5 años con cierre fiscal, se deberá entregar copia simple de los estados financieros, declaraciones de impuestos anuales, facturas por la venta y/o servicios de tecnología o documentación equivalente en el país de origen, presentados ante autoridad competente...”.

PREGUNTA 201.-

Estimada entidad, en el ítem 5.1 Criterios de Calificación (IAO 39.1) en el literal b) Experiencia Específica, solicitan Experiencia Requerida Se deberá acreditar experiencia en al menos una de las siguientes categorías: Comercialización de bienes, o de garantía técnica, o de licenciamiento de: soluciones de detección y respuesta de amenazas, o de ciberseguridad, o de ciberdefensa. Comercialización de servicios, tales como implementación, o configuración, o migración, o mantenimiento, o soporte técnico especializado, o consultoría, o gestión de soluciones o sistemas de detección y respuesta de amenazas, o de ciberseguridad, o de ciberdefensa. Solicitamos que se permita la presentación de Comercialización de servicios, tales como implementación, o configuración, o migración, o mantenimiento, o soporte técnico especializado, o consultoría, o gestión de soluciones o sistemas de detección y respuesta de amenazas, o de ciberseguridad, o de ciberdefensa o soluciones tecnológicas, permitiendo así la libre participación a más canales con experiencia. Por favor confirmar que se acepte nuestra solicitud

RESPUESTA 201.-

Estimado oferente, no es posible acoger su requerimiento.

PREGUNTA 202.-

Estimada entidad, en el ítem personal Técnico Mínimo Gestor del proyecto (PM) solicitan Estudios o certificado requerido: Certificación vigente en Gestión de Proyectos o Postgrado en Gestión de Proyectos o Especialización en Gestión de Proyectos. Se solicita de la manera más comedida que se acepte Certificación vigente en Gestión de Proyectos o Postgrado en Gestión de Proyectos o Especialización en Gestión de Proyectos o certificación vigente de PMP. Por favor mencionar si se acepta nuestra solicitud

RESPUESTA 202.-

Estimado oferente, se aclara que el requisito "Certificación vigente en Gestión de Proyectos" corresponde a un término genérico que comprende diversas certificaciones reconocidas en esta disciplina, entre las cuales se encuentra la certificación PMP (Project Management Professional). En consecuencia, se aceptarán las certificaciones en Gestión de Proyectos que cumplan con dicho requisito, siempre que se encuentren vigentes al momento de la presentación de la oferta.

PREGUNTA 203.-

Estimada entidad para el personal técnico se solicita para el Nivel de estudio Título universitario de tercer nivel o superior, entendemos que al decir Título de tercer Nivel se acepta el título de ingeniero o tecnólogo tomando en cuenta que el título de tecnólogo ya es avalado como título de tercer Nivel. Por favor confirmar.

RESPUESTA 203.-

Estimado oferente,

Para la validación del personal técnico mínimo, se deberá presentar la documentación que respalde que el título de Tecnólogo corresponda a un nivel de estudio de tercer nivel, adicional deberá cumplir con el requisito de titulación académica solicitada para cada rol.

PREGUNTA 204.-

Estimada entidad, en la evidencia documental en el ítem Experiencia de fabricación y Capacidad Técnica: Para los ítems bajo el Contrato que el Oferente es un fabricante, el Oferente deberá proporcionar prueba documental para demostrar que..... Entendemos que esto aplica cuando el oferente es fabricante, por favor confirmar

RESPUESTA 204.-

Estimado oferente, es correcto su entendimiento.

PREGUNTA 205.-

Estimada entidad, en el presente proceso se entiende que el certificado Autorización del fabricante no es necesario presentar ya que mencionan que no aplica y solo se debe

presentar los certificados vigentes emitidos por los fabricantes que avalen que el oferente es un distribuidor autorizado de los componentes ofertados. Por favor confirmar

RESPUESTA 205.-

Estimado oferente, para el presente proceso no aplica el formulario Autorización del Fabricante.

PREGUNTA 206.-

Estimada entidad en el formulario Carta de Oferta solicitan que se llene el ítem **Solicitud de Oferta n.º** Por favor mencionar que el número que se debe colocar es EC-L1253-P00075, por favor confirmar.

RESPUESTA 206.-

Estimado oferente, el número correspondiente es EC-L1253-P00075.

PREGUNTA 207.-

Estimada entidad en el documento especificaciones técnicas en el punto 27. Solicitan La función NDR debe desplegarse en los dos centros de cómputo del SRI (“on-premise”), mediante la instalación de equipos de propósito específico. En base a lo solicitado, entendemos que si se debe llenar uno de los formularios Lista de Precios: Bienes de acuerdo con la modalidad que aplique. Por favor confirmar

RESPUESTA 207.-

Estimado oferente, los formularios lista de precio no aplican para la presente licitación.

El formulario que deberá ser presentado es: “PRECIO Y CRONOGRAMA DE CUMPLIMIENTO: SERVICIOS / SERVICIOS CONEXOS” de la Sección V, Formularios de la Oferta, página 85.

PREGUNTA 208.-

Estimada entidad, si la oferta se entrega como APCA, entendemos que en esta fase no es necesaria la constitución del APCA, sino se debe presentar un documento de compromiso que se va a constituir el APCA. Por favor confirmar

RESPUESTA 208.-

Estimado oferente, es correcto su entendimiento.

PREGUNTA 209.-

Estimada entidad, entendemos que el licenciamiento ofertando debe quedar a nombre del SRI que es la entidad contratante, por favor confirmar

RESPUESTA 209.-

Estimado oferente, su entendimiento es correcto.

El apartado LICENCIAMIENTO de la Sección VI. Requisitos de los Bienes y Servicios Conexos, páginas 112 y 113 establece:

1. *“El contratista debe entregar y activar a nombre del SRI:*
 - 1.a.** *Licenciamiento Endpoint Detection and Response (EDR)*
 - 1.b.** *Licenciamiento del(os) equipo(s) Network Detection and Response (NDR)*
 - 1.c.** *Licenciamiento de la Gestión de amenazas de identidad*
 - 1.d.** *Licenciamiento de la Inteligencia unificada de ciberdefensa*
 - 1.e.** *Licenciamiento de la Respuesta unificada de ciberdefensa”*

PREGUNTA 211.-

Estimada entidad, en el punto Despliegue de Hardware en el ítem 10. El contratista deberá instalar la última versión estable liberada y con el último paquete de parches y actualizaciones del firmware y software de cada componente de hardware desplegado. Es responsabilidad del oferente mantener actualizadas las versiones de firmware y software del hardware entregado a la institución en forma de préstamo para entregar el servicio.

RESPUESTA 211.-

Estimado oferente,
Es correcto su entendimiento.

PREGUNTA 212.-

Estimada entidad, por favor mencionar si el oferente adjudicado para la firma del contrato debe presentar póliza de buen uso de anticipo

RESPUESTA 212.-

Estimado oferente, el presente proceso no contempla anticipo, razón por la cual no se deberá presentar dicha póliza.

PREGUNTA 213.-

Estimada entidad, por favor mencionar si el oferente adjudicado para la firma del contrato debe presentar póliza de fiel cumplimiento del contrato

RESPUESTA 213.-

Estimado oferente, el presente proceso si contempla la presentación de póliza de fiel cumplimiento del contrato.

PREGUNTA 214.-

Estimada entidad, por favor mencionar si el oferente adjudicado para la firma del contrato debe presentar garantía bancaria para la firma del contrato

RESPUESTA 214.-

Estimado oferente, el presente proceso no contempla la presentación de una garantía bancaria.