BOLETÍN DE ACLARACIONES Nro. 1

ADQUISICIÓN DE FIREWALL NUEVA GENERACIÓN

CÓDIGO: EC-L1253-P00016

PREGUNTA 1.-

Buenas tardes, por favor confirmar si: El Técnico especialista de implementación y migración o Técnico especialista de soporte técnico, puede cumplir el rol de instructor de transferencia de conocimientos, cumpliendo con el perfil que solicitan para dicho cargo.

RESPUESTA 1.-

Únicamente se puede aceptar que el mismo recurso que realice la instalación y migración también realice el trabajo de soporte técnico, conforme lo establecido en la Sección III. Criterios de Evaluación y Calificación, página 60, numeral 4 de La Solicitud de Ofertas.

PREGUNTA 2.-

Me gustaría solicitar una prórroga en la fecha de vencimiento de la propuesta. Dado que somos una empresa que se unió tarde y podríamos usar tiempo adicional para armar una solución integral para su consideración.

RESPUESTA 2.-

Referirse al Boletín de Enmiendas Nro. 1

PREGUNTA 3.-

Estimada Entidad, en la sección 5.2 INSTALACIÓN DEL HARDWARE, se indican que disponen de las siguientes SFPS y conexiones”

MEDIO	TIPO DE CONEXIÓN	FABRICANTE	MODELO
Óptico	40Gbps BASE-SR QSFP+ LC	Cisco	QSFP-40/100-SRBD

Óptico	25Gbps BASE-SR SFP+ LC	Cisco	SFP-25G-SR-S
Óptico	10Gbps BASE-SR SFP+ LC	Cisco	SFP-10G-SR
Óptico	1Gbps BASE-SX SFP LC	Cisco	GLC-SX-MMD

Por favor confirmar que en este proceso no se debe incluir ninguna SFP y estas serán provistas por el SRI. Caso contrario, especificar la cantidad de SFPs requeridas.

RESPUESTA 3.-

En la sección VI. Requisitos de los Bienes y Servicios Conexos, página 105, en los numerales del 9 al 12 se establece que:

"El contratista debe proveer, como parte de la instalación de cada equipo entregado, los transceptores ("transceivers") **que sean necesarios** para su conexión con la infraestructura de red del SRI, en los centros de datos principal y alterno, utilizando los modelos que se indican en la tabla a continuación.

MEDIO	***TIPO DE CONEXIÓN***	***FABRICANTE***	***MODELO***
Óptico	*40Gbps BASE-SR QSFP+ LC*	*Cisco*	*QSFP-40/100-SRBD*
Óptico	*25Gbps BASE-SR SFP+ LC*	*Cisco*	*SFP-25G-SR-S*
Óptico	*10Gbps BASE-SR SFP+ LC*	*Cisco*	*SFP-10G-SR*
Óptico	*1Gbps BASE-SX SFP LC*	*Cisco*	*GLC-SX-MMD*

Tabla 7. *Modelos de transceptores ("transceivers") soportados por el switch de core institucional." (énfasis añadido)*

En virtud de lo expuesto, el contratista debe proveer e instalar la cantidad que sea necesaria de los transceivers de los componentes de hardware que conforman el objeto

de esta contratación (solución ofertada) y los transceivers del switch de core institucional (tabla 7), para la correcta operación del sistema.

PREGUNTA 4.-

Estimada Entidad, en el caso que para realizar integraciones con el Directorio Activo y se requiera un servidor intermedio para esta integración, se entiende que el SRI suministrará la máquina virtual y/o servidor y el oferente deberá solo incluir la configuración y/o software de operación:

"*Si para la instalación y operación de los componentes de software se requiere software base como, por ejemplo, sistemas operativos, bases de datos, etcétera, el contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la instalación, activación y funcionamiento de dichos prerrequisitos siguiendo las mejores prácticas de fábrica, aplicando los estándares tecnológicos institucionales y cumpliendo con los requerimientos técnicos del SRI.*"

Por favor confirmar.

RESPUESTA 4.-

En la sección VI. Requisitos de los Bienes y Servicios Conexos, página 106, numeral 5.3 INSTALACION DE SOFTWARE, en los numerales del 2 al 5 se establece que:

2. *"Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como instancias virtuales (máquina o appliance) en los servidores de gestión de acuerdo con el detalle de la **tabla 6**.*
3. *El contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la instalación, activación y funcionamiento del software de virtualización necesario para el despliegue de las instancias virtuales (máquina o appliance) de los componentes de software, de acuerdo con el estándar del SRI (véase **INFRAESTRUCTURA ACTUAL**).*
4. *El contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la integración del software de virtualización instalado con la infraestructura virtual del SRI.*
5. *Si para la instalación y operación de los componentes de software se requiere software base como, por ejemplo, sistemas operativos, bases de datos, etcétera, el contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la instalación, activación y funcionamiento de dichos prerrequisitos siguiendo las mejores prácticas de fábrica, aplicando los estándares tecnológicos institucionales y cumpliendo con los requerimientos técnicos del SRI."*

En función de lo expuesto, en caso de ser necesario utilizar un servidor adicional para la integración con el Active Directory, deberá incluirse como una máquina virtual adicional dentro de la virtualización solicitada en el numeral 2 y cumpliendo el numeral 5 del texto citado.

PREGUNTA 5.-

Estimada Entidad, para asegurar la continuidad de los productos y considerando la vigencia y vida útil de los equipos, solicitamos que se acepten únicamente modelos lanzados al mercado a partir del año 2023 o en adelante. De esta manera el SRI, asegura una vigencia superior de los equipos. Por favor confirmar.

RESPUESTA 5.-

Por favor referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 118, A. CONDICIONES GENERALES, literal 3 en el que se establece que:

"Para garantizar la vigencia tecnológica, solamente se aceptan equipos cuyo modelo se hayan liberado desde el año 2022 en adelante."

Adicional a esto, en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 134, numeral 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE, numeral 3 se establece que:

"Todos los equipos que conforman el componente de hardware del objeto de contrato deberán ser nuevos y se deberá garantizar que éstos no entren en EOST ("End-of-Support") ni en EOL ("End-of-Life") durante los 5 años posteriores a la fecha de suscripción del contrato."

PREGUNTA 6.-

Estimada Entidad, considerando que los equipos que dispondrán requieren capacidades de almacenamiento para una mejor operación de los equipos, solicitamos que, para beneficio del SRI, se acepte de manera mandatoria discos SSD de 900 GB o superior NVMe configurados en RAID-1. Por favor confirmar.

RESPUESTA 6.-

Por favor referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, B. CLUSTER DE FIREWALL PRINCIPAL Y ALTERNO, página 119, numeral 7 en el que se establece que:

"Almacenamiento:

- *Cada equipo debe tener un volumen de almacenamiento con una capacidad de* ***no menos de 480GB de espacio****;*
- *El volumen de almacenamiento debe estar constituido por un arreglo RAID1, RAID10, RAID5 o RAID6;*
- *El volumen de almacenamiento debe estar conformado por al menos dos (2) unidades de estado sólido (SSD)." (énfasis añadido)*

En función de lo expuesto, es responsabilidad del oferente incluir la capacidad de almacenamiento necesaria para la óptima operación del sistema, tanto para el procesamiento del tráfico como para las operaciones de mantenimiento (ejemplo: respaldos, generación de información de diagnóstico, actualizaciones de versión, etc), de acuerdo con la arquitectura del fabricante, siendo la cantidad mínima 480 GB de espacio para almacenamiento.

PREGUNTA 7.-

Estimada Entidad, solicitan:

Conexión de red para tráfico de datos:

- Cada equipo debe tener no menos de dos (2) interfaces físicas independientes (no compartidas) Ethernet 40 Gbps Base-SR QSFP+ LC;
- Cada equipo debe tener no menos de una (1) interfaz Ethernet 10 Gbps Base-SR SFP+ LC;

Cada equipo debe contar con los transceptores ("transceivers") propios de fábrica necesarios para la operación de las interfaces de tráfico de datos.

Por favor confirmar que la cantidad de transceivers requerido sea correcto:

- Cada equipo deberá tener 2 interfaces Ethernet 40 Gbps Base-SR QSFP+ LC y se debe incluir el transceiver correspondiente, total 2.

- Cada equipo deberá tener 1 interfaz interfaz Ethernet 10 Gbps Base-SR SFP+ LC y se debe incluir el transceiver correspondiente, total 1.

RESPUESTA 7.-

En la sección VI. Requisitos de los Bienes y Servicios Conexos, página 105, en los numerales del 9 al 12 se establece que:

"El contratista debe proveer, como parte de la instalación de cada equipo entregado, los transceptores ("transceivers") **que sean necesarios** para su conexión con la infraestructura de red del SRI, en los centros de datos principal y alterno, utilizando los modelos que se indican en la tabla a continuación.

MEDIO	***TIPO DE CONEXIÓN***	***FABRICANTE***	***MODELO***
Óptico	*40Gbps BASE-SR QSFP+ LC*	*Cisco*	*QSFP-40/100-SRBD*
Óptico	*25Gbps BASE-SR SFP+ LC*	*Cisco*	*SFP-25G-SR-S*
Óptico	*10Gbps BASE-SR SFP+ LC*	*Cisco*	*SFP-10G-SR*
Óptico	*1Gbps BASE-SX SFP LC*	*Cisco*	*GLC-SX-MMD*

Tabla 7. *Modelos de transceptores ("transceivers") soportados por el switch de core institucional." (énfasis añadido)*

En virtud de lo expuesto, el contratista debe proveer e instalar la cantidad que sea necesaria de los transceivers de los componentes de hardware que conforman el objeto de esta contratación (solución ofertada) y los transceivers del switch de core institucional (tabla 7), para la correcta operación del sistema.

PREGUNTA 8.-

Estimada Entidad, solicitan:

La función de inspección SSL/TLS de tráfico saliente debe permitir el descifrado selectivo en base a categorías de navegación, ya sea por tipo de contenido o por nivel de riesgo o por representar contenido sensible, y en base a nombres de host ("hostnames") y dominios.

Esto se refiere al bypass de inspección SSL para sitios definidos por categorías? Es correcto nuestro entendimiento.

RESPUESTA 8.-

No es correcto su entendimiento. No se limita únicamente al bypass de inspección SSL para sitios definidos por categorías.

Se aclara que la función de inspección SSL/TLS debe ser capaz de descifrar y analizar selectivamente el tráfico saliente, tomando decisiones basadas en categorías de navegación, ya sea por el tipo de contenido o por nivel de riesgo o por representar contenido sensible y en base a nombres de host y dominios.

PREGUNTA 9.-

Estimada Entidad, solicitan:

"24. La gestión de políticas debe tener la capacidad de integrarse con el sistema vCenter del SRI (véase INFRAESTRUCTURA ACTUAL) para importar objetos de manera que se puedan utilizar como origen o destino para crear reglas de seguridad."

Por favor confirmar si actualmente disponen del vcenter y como parte de este proyecto es realizar la integración, o la solución propuesta deberá tener la capacidad de integración a futuro. Por favor confirmar.

RESPUESTA 9.-

En la sección VI. Requisitos de los Bienes y Servicios Conexos, página 102, numeral 12, tabla 3 se detalla las versiones de software de los componentes de la plataforma de virtualización que dispone el SRI, en el que se incluye el vcenter.

La necesidad institucional plasmada en la Solicitud de ofertas (SDO). requiere que la gestión de políticas tenga la capacidad de integrarse con el sistema vCenter del SRI en la actualidad; no se trata de una propuesta de integración futura.

PREGUNTA 10.-

Estimada Entidad, solicitan:

"La gestión de políticas debe tener la capacidad de integrarse con el sistema Active Directory del SRI (véase INFRAESTRUCTURA ACTUAL) para importar objetos de manera que se puedan utilizar como origen o destino para crear reglas de seguridad."

Por favor aclarar que objetos correspondan a los usuarios y grupos de usuarios del directorio activo. Por favor confirmar.

RESPUESTA 10.-

Se confirma que los objetos a importarse desde el sistema Active Directory son: usuarios y grupos de usuarios, sin limitarse a otros objetos del Active Directory.

PREGUNTA 11.-

Se solicita: "La transferencia de conocimiento se debe organizar considerando que un (1) funcionario labora en las oficinas del SRI en Guayaquil y que los ocho (8) restantes laboran en las oficinas del SRI en Quito." ¿Para el funcionario de GYE se debe considerar viáticos?

RESPUESTA 11.-

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 111, numeral 2:

"Toda logística asociada con la transferencia de conocimiento correrá por cuenta del Contratista."

PREGUNTA 12.-

Estimada entidad por favor indicar cuantos servidores de identidad disponen actualmente (Radius, AD, etc.) Y cuales de estos deberán ser sincronizados con la solución de seguridad.

RESPUESTA 12.-

Por favor remitirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 101, numerales 7 y 8 :

7. *"El SRI cuenta con un sistema de directorio compuesto por:*
   - ***7.a.*** *Microsoft Active Directory, desplegado en Microsoft Windows Server 2019 en la red informática del SRI;*

7.b. *Microsoft Entra ID (Azure AD), desplegado en los servicios en línea ("cloud") de Microsoft Office 365 E3.*

8. *El sistema de directorio Microsoft Active Directory del SRI está conformado por 12 controladores de dominio, de los cuales 2 se encuentran en el centro de datos principal, 1 en el centro de datos alterno y el resto se encuentra distribuido entre las agencias a nivel nacional."*

PREGUNTA 13.-

Estimada entidad por favor indicar si durante la ejecución del contrato esperan crecer en cantidad de switch leaf con respecto a su solución ACI, si es así indicar el porcentaje de crecimiento durante la ejecución del contrato.

RESPUESTA 13.-

No se tiene considerado un aumento porcentual en la cantidad de switch leaf con respecto a la solución ACI, en al menos un período de 3 años.

PREGUNTA 14.-

Estimada entidad, por favor indicar que retentiva aproximada en tiempo necesitan de sus gestión de logs (1 mes, 3 meses, 6 meses, etc)

RESPUESTA 14.-

El tiempo de retención de registros de eventos ("logs") dependerá del espacio de almacenamiento disponible, en función de lo que se establece en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 107, numeral 15:

"La distribución de los recursos de los servidores físicos, esto es, de la capacidad de procesamiento, de memoria y de espacio de almacenamiento, entre todas las instancias virtuales deberá ser aprobada por el personal técnico del SRI en función de los requerimientos operativos de los componentes de software, los estándares tecnológicos institucionales y los requerimientos técnicos del SRI."

En función de lo expuesto considerar lo siguiente:

SISTEMA DE FIREWALLS:

En el caso específico del sistema de firewalls, además de lo expuesto, el tiempo de retención del **gestor de eventos** dependerá de la densidad de logs que tenga la arquitectura de la solución ofertada.

SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO:

Por favor referirse a:

- La sección VI. Requisitos de los Bienes y Servicios Conexos, B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO, página 148, numeral 97, en la que se establece lo siguiente:
  *"La retención de los registros de eventos ("logs") **debe ser de no menos de 14 días**." (énfasis añadido).*
- La sección VI. Requisitos de los Bienes y Servicios Conexos, página 48, PROTECCIÓN DE DATOS, numeral 99, en el que se estable lo siguiente:
  "El servicio SaaS deberá proveer las facilidades necesarias para descargar o reenviar la información generada, incluyendo los registros de eventos ("logs")."

COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS:

Adicionalmente, se debe considerar que en este componente se van a realizar tanto la recolección y correlación de eventos como el respaldo automático de eventos, lo que también debe ser considerado en la retención.

En la sección VI. Requisitos de los Bienes y Servicios Conexos, RECOLECCIÓN Y CORRELACIÓN DE EVENTOS, página 138, numeral 14, se establece que:

> *"La función de recolección y correlación de logs debe contar con la capacidad y el licenciamiento suficiente para recolectar y correlacionar los registros de eventos ("logs") de:*
>
> - ***El sistema de Firewalls ofertado;***
> - ***El servicio SaaS de protección de correo electrónico ofertado;***
> - *El sistema de Proxy Web del SRI (Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG)." (énfasis añadido)*

Finalmente, en base a lo expuesto, se aclara que la retención de los tres componentes citados (GESTORES DEL SISTEMA DE FIREWALL, COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS, SERVICIO SAAS DE PROTECCIÓN DE CORREO

ELECTRÓNICO) estará determinada por la arquitectura de las soluciones ofertadas y la distribución del espacio de almacenamiento disponible en los SERVIDORES DE GESTIÓN (físicos).

PREGUNTA 15.-

Estimada entidad en la página 121, se solicita incluir características de seguridad tales como: IPS, antimalware, amenazas no basada en firmas, etc, Se ha considerado tal vez proteger a la entidad de vectores de ataques asociados a DNS tales como: Tunelización de DNS y ataques asociados a DGA, considerar colocarlo de manera obligatoría esta protección ya que este tipo de incidentes podrían impactar de manera negativa en la entidad.

RESPUESTA 15.-

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 125, PROTECCIÓN ANTIMALWARE, numeral 49, en el que se establece que:
"El Firewall debe detectar y bloquear ataques de tipo "DNS Tunneling".

Asimismo, en el numeral 52 de la misma página se establece que:
"El Firewall debe detectar y bloquear conexiones hacia sitios maliciosos cuyos nombres fueron creados a través de algoritmos de generación de dominios (DGA)."

PREGUNTA 16.-

Por favor especificar que concurrencia se necesita en la VPN de acceso remoto. Esto con el fin de dimensionar un equipo orientado en estas capacidades.

RESPUESTA 16.-

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 130, numeral 119, en donde se establece que:

"La función de VPN de acceso remoto, tanto en el clúster de firewalls principal como en clúster de firewalls alterno, debe contar con el licenciamiento suficiente para al menos

3129 usuarios totales o 1035 usuarios concurrentes, según sea el modelo de licenciamiento del fabricante"

PREGUNTA 17.-

Por favor confirmar si se puede ofertar un cluster HA activo – pasivo.

RESPUESTA 17.-

Referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 122, numeral 15, en el que se establece que:

"El clúster de firewall debe soportar los siguientes esquemas de alta disponibilidad:

- *Activo-Pasivo, en el que solamente un nodo está activo y soporta toda la carga.*
- *Activo-Activo, en el que todos los nodos están activos y comparten la carga."*

PREGUNTA 18.-

Estimada entidad al buscar compatibilidad con TLS, por favor colocar de manera obligatoria cumplir con compatibilidad a TLS1.3.

RESPUESTA 18.-

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 128, INSPECCIÓN SSL/TLS (A. CLUSTER DE FIREWALL PRINCIPAL Y ALTERNO) , numeral 88, en el que se establece que:

"La función de inspección SSL/TLS debe descifrar el tráfico que utilice el protocolo TLS versiones: 1.3, 1.2, 1.1 y 1.0."

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 141, B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO, numeral 6, en el que se establece que:

"La solución debe integrarse con los componentes del sistema de directorio institucional utilizando protocolos seguros basados en TLS versiones 1.2 o 1.3."

En virtud de lo expuesto, la necesidad institucional plasmada en la Solicitud de ofertas (SDO). ha considerado que la solución de Firewall de Nueva Generación y el Servicio SaaS de Protección de Correo Electrónico soporte TLS versión 1.3

PREGUNTA 19.-

De manera que se pueda garantizar que la inspección SSL/TLS se encuentre en parámetros requeridos, se pide que cada oferente pueda demostrar con documentación técnica liberada por el fabricante y de acceso público al cumplimiento de este parámetro.

RESPUESTA 19.-

Referirse a la Sección III. Criterios de Evaluación y Calificación , página 61, iii Prueba Documental, en la que se establece que:

"…El oferente debe proveer toda la documentación técnica necesaria para validar y verificar el cumplimiento de las especificaciones técnicas de los bienes y servicios ofertados, incluyendo: fichas técnicas, hojas de especificación, catálogos, manuales o similares, arquitecturas propuestas, diseños técnicos propuestos, certificados de fábrica, entre otros"

Asimismo, considerar lo establecido en la Sección I. Instrucciones a los Oferentes (IAO), página 29, numeral 27 Confidencialidad:

"No se divulgará a los Oferentes ni a ninguna persona que no participe oficialmente en el proceso licitatorio información relacionada con la evaluación de las Ofertas o con la recomendación de adjudicación del Contrato hasta que la información sobre la Notificación de la Intención de Adjudicar el Contrato se haya comunicado a todos los Oferentes, con arreglo a la IAO 42."

En función de lo expuesto, todos los parámetros técnicos requeridos en la Solicitud de ofertas (SDO) deberán contar con la respectiva documentación técnica de sustento.

PREGUNTA 20.-

Estimada entidad en el punto 63. de la solución de protección de correo solicitan " La solución debe ser capaz de analizar al menos los siguientes tipos de archivos comprimidos: ZIP, TGZ, 7Z, CAB, LZH, RAR, TNEF.", se solicita colocar de manera opicional los tipos CAB,LZH,RAR y TNEF para permitir la participación de más fabricantes considerados líderes en NGFW.

RESPUESTA 20.-

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 21.-

Indicar si se puede usar directiva GPO de AD para desplegar agente VPN cliente-site de acceso remoto.

RESPUESTA 21.-

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 22.-

Estimada entidad, por favor se sugiere colocar como mandatorio que el mecanismo de sandbox pueda ser capaz de realizar prevención en tiempo real malware de paciente cero (zero day), esto con el fin de repotenciar y asegurar que si existiese un evento de día cero este pueda ser prevenido.

RESPUESTA 22.-

La necesidad institucional plasmada en la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 126, A. CLUSTER DE FIREWALL PRINCIPAL Y ALTERNO, PROTECCIÓN CONTRA AMENAZAS NO BASADA EN FIRMAS, numeral 69, establece que:

"El Firewall debe contar con una función de protección contra amenazas no ***basada en firmas que debe detectar y bloquear malware y amenazas no conocidas mediante el uso de un mecanismo de análisis "inline" del tráfico****." (énfasis añadido)*

Asimismo, la necesidad institucional plasmada en la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 145, B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELETRÓNICO, CONTROL ANTIMALWARE, numeral 52, establece que:
"La solución debe detectar y bloquear malware conocido, ***así como malware de día cero****, esto es, para las que aún no existen firmas." (énfasis añadido)*

En función de lo expuesto, la necesidad institucional plasmada en la Solicitud de Ofertas (SDO) considera la prevención de ataques de día cero.

PREGUNTA 23.-

Estimada entidad por favor confirmar si el mecanismo de sandbox deba ser capaz de emular y extraer archivos embebidos en documentos con malware.

RESPUESTA 23.-

Por favor remitirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, páginas 126 y 127, A. CLUSTER DE FIREWALL PRINCIPAL Y ALTERNO, PROTECCIÓN CONTRA AMENAZAS NO BASADA EN FIRMAS, numeral 69, 74 y 77.

Asimismo, la necesidad institucional plasmada en la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 145, B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELETRÓNICO, CONTROL ANTIMALWARE, numeral 58, establece que:
"La solución debe incluir el uso del análisis de sandboxing para revisar los archivos adjuntos y los recursos web asociados a los hipervínculos incluidos en los mensajes."

Por lo tanto, se solicita regirse a lo solicitado en la Solicitud de Ofertas (SDO).

PREGUNTA 24.-

Estimada entidad por favor confirmar si la solución deba detectar ROP o cualquier técnica de explotación mediante el monitoreo del flujo a nivel de CPU.

RESPUESTA 24.-

La necesidad institucional en este proceso no requiere detectar ROP mediante el monitoreo del flujo a nivel de CPU.

PREGUNTA 25.-

Se solicita "La transferencia de conocimiento deberá impartirse en al menos dos grupos en función de la disponibilidad del personal institucional y la distribución que el SRI establezca." Es decir que se tiene que brindar dos capacitaciones en fechas diferentes para cada grupo, ¿es correcto nuestro entendimiento?

RESPUESTA 25.-

No es correcto su entendimiento, referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 111, numeral 5.4.1.4 TRANSFERENCIA DE CONOCIMIENTO, numero 4, en la que se establece:

*"El calendario y horario de entrega de la transferencia de conocimiento **se acordará con el administrador del contrato** en función de la disponibilidad operativa del personal del SRI." (énfasis añadido)*

PREGUNTA 26.-

Se solicita en el componente de análisis de configuración y eventos "Las funciones y módulos que comprenden el COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS deben desplegarse como máquinas virtuales o appliance virtuales." Por favor confirmar que a entidad facilitará los recursos para la implementación de las máquinas virtuales.

RESPUESTA 26.-

En la sección VI. Requisitos de los Bienes y Servicios Conexos, página 106, numeral 5.3 INSTALACION DE SOFTWARE, en el numeral 2, se establece que:

*"Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como instancias virtuales (máquina o appliance) en los servidores de gestión de acuerdo con el detalle de la **tabla 6**."*

En función de lo expuesto, las máquinas virtuales deben desplegarse como instancias virtuales en los servidores físicos detallados en la tabla 6.

PREGUNTA 27.-

Se solicita "La gestión de políticas debe tener la capacidad de integrarse con el sistema vCenter del SRI" en nuestro entendimiento la herramienta que se debe considerar para virtualización debe ser Vmware. Por favor favor confirmar si es correcto nuestro entendimiento.

RESPUESTA 27.-

No es correcto su entendimiento, referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, GESTIÓN DE POLÍTICAS, página 132, numeral 24, se establece que:

*"La gestión de políticas debe tener la capacidad de integrarse con el sistema vCenter del SRI (véase **INFRAESTRUCTURA ACTUAL**) para importar objetos de manera que se puedan utilizar como origen o destino **para crear reglas de seguridad**." (énfasis añadido)*

Asimismo, considerar la tabla 3 de la página 102, sección VI. Requisitos de los Bienes y Servicios Conexos.

PREGUNTA 28.-

Estimados en el punto 14 de la solución de protección de correo solicitan "La solución, cuando opere en modo ESG, debe tener la capacidad de ser desplegada de las siguientes formas, en función de los requerimientos de seguridad de la arquitectura de correo electrónico institucional:

a. Como servicio SaaS que reciba primero el tráfico de correo electrónico y que lo reenvíe depurado al servicio de Exchange Online institucional. " se refieren a email Security Gateway?

RESPUESTA 28.-

Referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 141, PROTECCIÓN DE CORREO ELECTRÓNICO, numeral 13, en el que se establece que:

"La solución debe tener la capacidad de integrarse con el servicio Microsoft Exchange Online institucional al menos en los siguientes modos de operación:

- *Como gateway de seguridad de correo electrónico **("Email Security Gateway" – ESG);***
- *Mediante integración API con Exchange Online." (énfasis añadido)*

En función de lo expuesto, ESG corresponde a Email Security Gateway

PREGUNTA 29.-

Estimados en el punto 24 de la solución de protección de correo se solicita “La solución debe permitir la adición de etiquetas en el correo electrónico entrante que permitan, al menos, informar al destinatario:

Cuando un correo electrónico es enviado desde un dominio externo,

Si se trata de un remitente desconocido,

Si es un dominio recientemente registrado. “por favor eliminar este punto ya que hace referencia a un fabricante en específico con lo cual no se permite la libre participación de otros oferentes en este servicio.

RESPUESTA 29.-

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 30.-

Estimada entidad en el punto 41 de la solución de protección de correo solicitan “La función de control antispam debe ser al menos de tercera generación, incluyendo análisis por medio de aprendizaje automático (“machine learning”). “Se solicita eliminar este punto ya que hace referencia a términos específicos de un solo fabricante, o quien define la generación del antispam?

RESPUESTA 30.-

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 31.-

Estimada entidad en el punto 47 de la solución de protección de correo solicitan “La solución debe contar con un mecanismo para que los usuarios reporten mensajes maliciosos o no deseados (o sea, declararlos falsos negativos) que han recibido en su bandeja de entrada. “se solicita que se elimine este punto ya que hace referencia a funcionalidades específicas del fabricante Proofpoint dejando por fuera a soluciones líderes en la industria de protección de correo electrónico y también no permitiendo la participación de los mismos.

RESPUESTA 31.-

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 145, numeral 47, donde se establece que:

"La solución debe contar con un mecanismo para que los usuarios reporten mensajes maliciosos o no deseados (o sea, declararlos falsos negativos) que han recibido en su bandeja de entrada."

PREGUNTA 32.-

Estimada entidad en punto 49 de la solución de protección de correo solicitan "La cuarentena debe almacenar los mensajes en carpetas diferenciadas de acuerdo con el tipo motor de detección. "Se solicita que se acepte que la solución funcione colocando una sola cuarentena sin carpetas pero con un motivo de detreccion por cada motor

RESPUESTA 32.-

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 33.-

Estimada entidad en el punto 50 de la solución de protección de correo solicitan "La solución debe permitir al administrador establecer el tiempo máximo que los mensajes pueden permanecer en cada una de las cuarentenas. Los mensajes que superen este periodo deberán ser eliminados definitivamente. se solicita que se elimine este punto ya que hace referencia a funcionalidades específicas del fabricante Proofpoint dejando por fuera a soluciones líderes en la industria de protección de correo electrónico y también no permitiendo la participación de los mismos.

RESPUESTA 33.-

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 145, numeral 50, donde se establece que:

"La solución debe permitir al administrador establecer el tiempo máximo que los mensajes pueden permanecer en cada una de las cuarentenas. Los mensajes que superen este periodo deberán ser eliminados definitivamente."

PREGUNTA 34.-

Estimada entidad en el punto 51 de la solución de protección de correo "La solución debe proporcionar una función de "vista previa segura" para que los administradores puedan ver información detallada de los mensajes en cuarentena y decidir las acciones necesarias. "se solicita que la solución permita descargar el correo en ZIP con contraseña como "Vista Segura"

RESPUESTA 34.-

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 145, numeral 51, donde se establece que:
"La solución debe proporcionar una función de "vista previa segura" para que los administradores puedan ver información detallada de los mensajes en cuarentena y decidir las acciones necesarias."

PREGUNTA 35.-

Estimada entidad en el punto 55 de la solución de protección de correo "La solución debe contar con inteligencia que permita intentar acceder a un archivo protegido con contraseña utilizando información contextual del mensaje utilizado para su envío. "se solicita que se elimine este punto ya que hace referencia a funcionalidades específicas del fabricante Proofpoint dejando por fuera a soluciones líderes en la industria de protección de correo electrónico y también no permitiendo la participación de los mismos.

RESPUESTA 35.-

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 36.-

Estimada entidad en el punto 60 de la solución de protección de correo “Si al momento de realizar análisis de sandboxing de un hipervínculo el recurso web asociado no se encuentra disponible, la solución debe contar con la opción de que el mensaje sea entregado no sin antes reescribir la dirección URL del hipervínculo de manera que, si el usuario hace clic, este se despliegue en un entorno controlado y aislado. “se solicita que se permita participar con el siguiente cumplimiento, hacer el analisis de la URL y el usuario recibe una URL que sino es testeada o conocida por fabrica se blqouea.

RESPUESTA 36.-

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 37.-

Estimada entidad en el punto 63. de la solución de protección de correo solicitan “La solución debe ser capaz de analizar al menos los siguientes tipos de archivos comprimidos: ZIP, TGZ, 7Z, CAB, LZH, RAR, TNEF.”, se solicita eliminar los tipos CAB,LZH,RAR y TNEF para permitir la participación de más fabricantes y considerando que los tipos de comprimidos que quedan son los que se usan día a día.

RESPUESTA 37.-

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 38.-

Estimada entidad en el punto 88 de la solución de protección de correo se solicita “La solución debe contar con paneles (“dashboards”) o reportes que provean al administrador información sobre estadísticas y tendencias de las amenazas de seguridad detectadas, incluyendo:

- Cuentas comprometidas,
- Archivos confidenciales potencialmente expuestos,
- Correos electrónicos filtrados,
- Credenciales de usuarios expuestas,
- Accesos OAuth no seguros,
- Usuarios o cuentas que han sido más atacados,

- Usuarios con comportamientos de alto riesgo,
- Acciones del análisis de caja de arena (“sandbox”),
- Accesos (clics) a direcciones URL,
- Malware detectado,
- Mensajes spam,
- Cómo se atacan esas cuentas,
- Compartición riesgosa de archivos en las aplicaciones de Microsoft Office 365,

Demás amenazas detectadas por la solución. Con que fuentes se necesita integrar la solución ya que para tener los dashboards indicados se necesita tener la integración de varias fuentes.

RESPUESTA 38.-

Se aclara que la fuente necesaria para obtener la información de los paneles (“dashboards”) o reportes requeridos en el numeral 88 deben provenir de la información que recopila el mismo SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO.

Además, se solicita referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 39.-

Estimada entidad en el punto 92 de la solución de protección de correo solicitan, “La solución debe contar con paneles (“dashboards”) o reportes que provean al administrador información sobre la operación del sistema, incluyendo:

- Volumen de tráfico de correo electrónico,
- Mensajes procesados,
- Mensajes rechazados o retenidos en cuarentena,
- Flujos de comunicación.

Se solicita eliminar, Mensajes rechazados o retenidos en cuarentena y Flujos de comunicación, ya que hacen referencia a dashboards específicos de un solo fabricante, lo cual no permite la libre participación en el proceso para marcas líderes.

RESPUESTA 39.-

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 148, GESTIÓN DE EVENTOS, REPORTES Y AUDITORÍA, numeral 92, donde se establece que:

"La solución debe contar con paneles ("dashboards") o reportes que provean al administrador información sobre la operación del sistema, incluyendo:

- *Volumen de tráfico de correo electrónico,*
- *Mensajes procesados,*
- *Mensajes rechazados o retenidos en cuarentena,*
- *Flujos de comunicación."*

PREGUNTA 40.-

En el punto 95 de la solución de protección de correo solicitan "La solución debe emitir alertas en base a condiciones asociadas a las políticas, las carpetas de cuarentena y los umbrales de cola." Por favor su ayuda especificando a que hace referencia con cola?

RESPUESTA 40.-

Esto se refiere a la capacidad de la solución para monitorear la cola de mensajes (los correos que están en espera de ser procesados). Si la cola alcanza un cierto umbral (por ejemplo, un número elevado de mensajes pendientes), la solución debe generar una alerta para que los administradores puedan investigar y resolver el problema.

PREGUNTA 41.-

Estimada entidad hay varios puntos en la solución de protección de correo en la cual se podría cumplir añadiendo soluciones complementarias como un XDR, es factible este tipo de configuración con el propósito de cumplir todas las especificaciones?

RESPUESTA 41.-

El proceso de contratación no corresponde a la adquisición de una solución XDR.

PREGUNTA 42.-

Estimada entidad en el punto ACONFIGURACIÓN Y EVENTOS, Supervisión , punto 29 “En cuanto a la supervisión del sistema de Firewalls, la función de supervisión debe tener la capacidad de monitorear los parámetros disponibles en los MIB de este sistema, entre los que se debe incluir:

- Firewalls físicos y virtuales monitoreados;
- Tráfico (ancho de banda o “throughput”) de los nodos físicos y sistemas virtuales;
- Conexiones concurrentes de los nodos físicos y sistemas virtuales;
- Procesamiento ocupado de los nodos físicos;
- Memoria RAM ocupada de los nodos físicos;
- Almacenamiento libre y ocupado de los nodos físicos;
- Estado de las conexiones VPN de sitio a sitio (“site-to-site”);
- La cantidad de conexiones VPN activas.”

Se solicita eliminar este punto ya que referencia a una tecnología diferente y no al objeto del proceso de la herramienta solicita

RESPUESTA 42.-

Se aclara que el componente de análisis de configuración y eventos es un sistema independiente del gestor de eventos de la solución de firewalls de nueva generación y del servicio SaaS de protección de correo electrónico.

En cuanto a la función de supervisión, debe tener la capacidad de monitorear los parámetros disponibles en los MIB del sistema de firewalls, entre los que se deben incluir los listados en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 140, numeral 29.

PREGUNTA 43.-

Estimada entidad en el personal técnico se solicitan que en los roles de Técnico especialista de instalación y migración, Instructor de transferencia de conocimiento, Técnico especialista de soporte técnico se solicita que “Estudios o certificado requerido: Certificación Técnica vigente nivel profesional, avanzado o equivalente emitida por el fabricante del sistema de Firewalls y/o el servicio SaaS de protección de correo electrónico ofertados. “Dado que son soluciones diferentes la del FW con la solución de

protección de Correo, se entiende que debe haber un ingeniero certificado en FW y otro diferente para la solución de protección de correo? Es correcto nuestro entendimiento? Es decir 3 ingenieros para correo y 3 ingenieros para FW?

RESPUESTA 43.-

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 44.-

Estimada entidad en personal técnico solicitan 3 Técnico especialista de instalación y migración, 1 Instructor de transferencia de conocimiento es posible que las personas repitan en los 3 roles dado que son servicios que se brindaran en diferente etapa del proyecto?

RESPUESTA 44.-

Conforme lo establecido en la Sección III. Criterios de Evaluación y Calificación, página 60, numerales 4 y 6de La Solicitud de Ofertas.

*"Se puede aceptar que el mismo recurso que **realice la instalación y migración** también realice el trabajo de soporte técnico." (énfasis añadido)*

*"Es responsabilidad del contratista incluir **la cantidad suficiente de recursos de personal** en cada rol para cumplir con los objetivos, entregables y plazos a lo largo de la vigencia del contrato." (énfasis añadido)*

PREGUNTA 45.-

Estimada entidad en el punto 2. Lista de Servicios / Servicios Conexos y Cronograma de Cumplimiento, en Fechas finales de cumplimiento de los servicios, se especifica " El plazo de la vigencia del licenciamiento de todos los elementos del componente de software será de 1.095 días calendario contados a partir de la fecha de la culminación de la instalación del hardware." Por favor especificar que se entiende por instalación del hardware, es solamente el rackeo y prendido del equipo, o una vez finalizadas las configuraciones?

RESPUESTA 45.-

Referirse a la sección VIII. Condiciones Especiales de Contrato (CEC), página 174, BIENES REQUERIDOS, numeral 1, en el que se establece que:

"El plazo de la entrega de los bienes instalados será de hasta 90 días calendario contados a partir de la notificación del administrador del contrato. ***Para el efecto, el contratista deberá entregar el oficio de culminación de la instalación del hardware."*** *(énfasis añadido)*

Además, se solicita referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, 5.2 INSTALACIÓN DEL HARDWARE, páginas 105 y 106, numerales del 15 al 17.

Se aclara que la vigencia del licenciamiento de todos los elementos del componente de software será de 1.095 días calendario, comenzando a contarse a partir de la aceptación, por parte del Administrador del Contrato, del oficio de culminación de la instalación del hardware.

PREGUNTA 46.-

Estimada entidad en el punto 2. Lista de Servicios / Servicios Conexos y Cronograma de Cumplimiento, GESTORES DEL SISTEMA DE FIREWALL, en Fechas finales de cumplimiento de los servicios, se especifica " El plazo de la vigencia del licenciamiento de todos los elementos del componente de software será de 1.095 días calendario contados a partir de la fecha de la culminación de la instalación del hardware." Por favor especificar que se entiende por instalación del hardware, es solamente el rackeo y prendido del equipo, o una vez finalizadas las configuraciones?

RESPUESTA 46.-

Referirse a la sección VIII. Condiciones Especiales de Contrato (CEC), página 174, BIENES REQUERIDOS, numeral 1, en el que se establece que:

"El plazo de la entrega de los bienes instalados será de hasta 90 días calendario contados a partir de la notificación del administrador del contrato. ***Para el efecto, el contratista deberá entregar el oficio de culminación de la instalación del hardware."*** *(énfasis añadido)*

Además, se solicita referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, 5.2 INSTALACIÓN DEL HARDWARE, páginas 105 y 106, numerales del 15 al 17.

Se aclara que la vigencia del licenciamiento de todos los elementos del componente de software será de 1.095 días calendario, comenzando a contarse a partir de la aceptación, por parte del Administrador del Contrato, del oficio de culminación de la instalación del hardware.

PREGUNTA 47.-

Estimada entidad en e punto 2. Lista de Servicios / Servicios Conexos y Cronograma de Cumplimiento, COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS, en Fechas finales de cumplimiento de los servicios, se especifica " El plazo de la vigencia del licenciamiento de todos los elementos del componente de software será de 1.095 días calendario contados a partir de la fecha de la culminación de la instalación del hardware." Por favor especificar que se entiende por instalación del hardware, es solamente el rackeo y prendido del equipo, o una vez finalizadas las configuraciones?

RESPUESTA 47.-

Referirse a la sección VIII. Condiciones Especiales de Contrato (CEC), página 174, BIENES REQUERIDOS, numeral 1, en el que se establece que:

"El plazo de la entrega de los bienes instalados será de hasta 90 días calendario contados a partir de la notificación del administrador del contrato. ***Para el efecto, el contratista deberá entregar el oficio de culminación de la instalación del hardware."*** *(énfasis añadido)*

Además, se solicita referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, 5.2 INSTALACIÓN DEL HARDWARE, páginas 105 y 106, numerales del 15 al 17.

Se aclara que la vigencia del licenciamiento de todos los elementos del componente de software será de 1.095 días calendario, comenzando a contarse a partir de la aceptación, por parte del Administrador del Contrato, del oficio de culminación de la instalación del hardware.

PREGUNTA 48.-

Estimada entidad en e punto 2. Lista de Servicios / Servicios Conexos y Cronograma de Cumplimiento, SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO, POR AÑO,en Fechas finales de cumplimiento de los servicios, se especifica " El plazo de la vigencia del licenciamiento de todos los elementos del componente de software será de 1.095 días calendario contados a partir de la fecha de la culminación de la instalación del hardware." Por favor especificar que se entiende por instalación del hardware, es solamente el rackeo y prendido del equipo, o una vez finalizadas las configuraciones, y como se aceptará en este caso la instalación si es tipo SAAS?

RESPUESTA 48.-

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, 2. Lista de Servicios / Servicios Conexos y Cronograma de Cumplimiento, página 95, SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO, POR AÑO, Columna "Fechas finales de cumplimiento de los servicios" , donde se establece que:

*"El plazo de la vigencia del licenciamiento de todos los elementos del componente de software será de **1.095 días calendario** contados a partir de la fecha de la culminación de la instalación del hardware. "*

Además, se solicita referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, 5.3 INSTALACIÓN DEL SOFTWARE, páginas 106 y-107.

Se aclara que la vigencia del licenciamiento de todos los elementos del componente de software será de 1.095 días calendario, comenzando a contarse a partir de la aceptación, por parte del Administrador del Contrato, del oficio de culminación de la instalación del hardware.

PREGUNTA 49.-

Estimada entidad en el punto 2. Lista de Servicios / Servicios Conexos y Cronograma de Cumplimiento, Migración, en Fechas finales de cumplimiento de los servicios, se especifica " El plazo de la entrega del servicio de migración, mediante el oficio de culminación de migración, será de hasta 210 días calendario, contados a partir del día siguiente de la culminación de la instalación del hardware" Por favor clarificar que durante estos 210 días ya está corriendo la vigencia de la licencias de los FW

RESPUESTA 49.-

Se aclara que la vigencia del licenciamiento de todos los elementos del componente de software será de 1.095 días calendario, comenzando a contarse a partir de la aceptación por parte del Administrador del Contrato del oficio de culminación de la instalación del hardware.

Por lo tanto, al iniciar el servicio conexo de MIGRACIÓN, el licenciamiento de los elementos del componente de software deberá estar vigente.

PREGUNTA 50.-

Estimada entidad, en la experiencia de la empresa, como medio de comprobación es suficiente con un certificado simple donde se indique la fecha de ejecución del proyecto, el nombre de la empresa y el monto del valor del proyecto?

RESPUESTA 50.-

El certificado de experiencia del oferente deberá estar en concordancia con lo establecido en la sección III. Criterios de Evaluación y Calificación, (ii)Experiencia y capacidad técnica, página 56.

PREGUNTA 51.-

Estimada entidad dado que es un proyecto complejo que involucra varias soluciones de diferentes tecnologías y que se requiere realizar bastante documentación se solicita que se pueda ampliar el plazo de entrega de las ofertas técnicas 20 días más a la fecha estipulada

RESPUESTA 51.-

Referirse al Boletín de Enmiendas Nro. 1

PREGUNTA 52.-

La sección "5.2 INSTALACIÓN DEL HARDWARE" al igual que la sección "5.3 INSTALACIÓN DEL SOFTWARE" de la Solicitud de Ofertas (SDO), indican que los gestores de firewall deben instalarse como appliance virtual o como máquina virtual dentro de servidores físicos principal y alterno. Mientras que en la "Sección VIII. Condiciones Especiales de Contrato", fila "CGC 16.1" se define a los Gestores del

Sistema de Firewall como componentes de Hardware. Adicionalmente al final de dicha sección, existe una "Nota" que indica que:

Los GESTORES DEL SISTEMA DE FIREWALL constituyen una función indispensable para la operación de los GATEWAYS DEL SISTEMA DE FIREWALL, siendo estos interdependientes. Por este motivo este ítem es considerado como componente de hardware.

A nuestro entendimiento, este componente de Gestión Centralizada de Firewalls, al ser importante e indispensable, puede ser implementado a través de equipos físicos o como una solución de appliances virtuales o máquinas virtuales. Por favor aclarar este particular indicando si se aceptará como solución válida cualquiera de los dos escenarios.

RESPUESTA 52.-

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 53.-

En la sección "6.2. COMPONENTE DE SOFTWARE", apartado "A. COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS", numerales 13, 15 y 18 se indica que el almacenamiento debe ser en base al periodo de retención".

A nuestro entendimiento, el período de retención a la que se refieren los numerales mencionados anteriormente, es el indicado en el numeral 97 del apartado "B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO", que indica que la retención debe ser de no menos 14 días. Por favor confirmar si nuestra apreciación es correcta.

RESPUESTA 53.-

El tiempo de retención de registros de eventos (“logs”) dependerá del espacio de almacenamiento disponible, en función de lo que se establece en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 107, numeral 15:

“La distribución de los recursos de los servidores físicos, esto es, de la capacidad de procesamiento, de memoria y de espacio de almacenamiento, entre todas las instancias virtuales deberá ser aprobada por el personal técnico del SRI en función de los requerimientos operativos de los componentes de software, los estándares tecnológicos institucionales y los requerimientos técnicos del SRI.”

En función de lo expuesto considerar lo siguiente:

SISTEMA DE FIREWALLS:

En el caso específico del sistema de firewalls, además de lo expuesto, el tiempo de retención del **gestor de eventos** dependerá de la densidad de logs que tenga la arquitectura de la solución ofertada.

SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO:

Por favor referirse a:

- La sección VI. Requisitos de los Bienes y Servicios Conexos, B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO, página 148, numeral 97, en la que se establece lo siguiente:
  *"La retención de los registros de eventos ("logs") **debe ser de no menos de 14 días**." (énfasis añadido).*
- La sección VI. Requisitos de los Bienes y Servicios Conexos, página 48, PROTECCIÓN DE DATOS, numeral 99, en el que se estable lo siguiente:
  "El servicio SaaS deberá proveer las facilidades necesarias para descargar o reenviar la información generada, incluyendo los registros de eventos ("logs")."

COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS:

Adicionalmente, se debe considerar que en este componente se van a realizar tanto la recolección y correlación de eventos como el respaldo automático de eventos, lo que también debe ser considerado en la retención.

En la sección VI. Requisitos de los Bienes y Servicios Conexos, RECOLECCIÓN Y CORRELACIÓN DE EVENTOS, página 138, numeral 14, se establece que:

> *"La función de recolección y correlación de logs debe contar con la capacidad y el licenciamiento suficiente para recolectar y correlacionar los registros de eventos ("logs") de:*
>
> - ***El sistema de Firewalls ofertado;***
> - ***El servicio SaaS de protección de correo electrónico ofertado;***
> - *El sistema de Proxy Web del SRI (Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG)." (énfasis añadido)*

Finalmente, en base a lo expuesto, se aclara que la retención de los tres componentes citados (GESTORES DEL SISTEMA DE FIREWALL, COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS, SERVICIO SAAS DE PROTECCIÓN DE CORREO

ELECTRÓNICO) estará determinada por la arquitectura de las soluciones ofertadas y la distribución del espacio de almacenamiento disponible en los SERVIDORES DE GESTIÓN (físicos).

PREGUNTA 54.-

En la sección "6.2. COMPONENTE DE SOFTWARE", apartado "A. COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS", numeral 31 indica que la función de supervisión debe emitir alertas al menos por correo electrónico y por mensajería instantánea Telegram. La integración con Telegram podría necesitar costos adicionales en base a la cantidad de usuarios que se requiera que reciban dichas alertas.

Se solicita cordialmente que la integración con Telegram sea opcional y en su lugar se acepte el envío de alertas por SMS, considerando que Telegram es un servicio de mensajería externa que no está bajo el control directo del SRI y que los SMS son una solución más comercial, dependen de la entidad y se encuentran regulados por el Gobierno.

RESPUESTA 54.-

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 55.-

En la Sección II. Datos de la Licitación dentro de las Instrucciones a los Oferentes (IAO), en el literal C. Preparación de las Ofertas, IAO 11.1 señala: "*El idioma de la Oferta es: Español. Todo el intercambio de correspondencia se hará en el idioma Español. El idioma utilizado para la traducción de los documentos justificativos y el material impreso que formen parte de la Oferta es Español.*"

En vista de que este tipo de soluciones tecnológicas son fabricadas en países donde el lenguaje oficial no es español, solicitamos se acepte que la oferta incluya manuales de fábrica en inglés.

RESPUESTA 55-

Favor regirse a lo señalado en la Sección I. Instrucciones a los Oferentes (IAO), literal C, Preparación de las Ofertas, numeral 11.1, que indica:

"La Oferta, toda la correspondencia y los documentos relativos a ella que intercambien el Oferente y el Comprador deberán redactarse en el idioma que se indica ***en los DDL****.* ***Los documentos de respaldo y el material impreso que formen parte de la Oferta podrán***

estar escritos en otro idioma, *siempre que vayan acompañados de* ***una traducción fidedigna de las secciones pertinentes al idioma que se especifica en los DDL****, en cuyo caso la traducción prevalecerá en lo que respecta a la interpretación de la Oferta*". (El resaltado y subrayado me pertenece).

PREGUNTA 56.-

Con respecto a la garantía bancaria que solicitan en el caso que se adjudique el contrato, se solicita que pueda ser válida una garantía emitida por una empresa de seguros (aseguradora).

RESPUESTA 56.-

El SRI, no solicita Garantía Bancaria. Conforme lo señalado en la Solicitud de Ofertas (SDO) de la Sección VIII. Condiciones Especiales de Contrato (CEC), pág. 175, en las CGC 19.1 y CGC 19.3, se establece las condiciones de la garantía para el cumplimiento del contrato, que señalan:

"(…)

CGC 19.1	***Garantía de Cumplimiento del Contrato:*** *Para seguridad del cumplimiento de este Contrato y para responder de las obligaciones que se contrajeren a favor de terceros, relacionados con el mismo, el Proveedor rinde una garantía a satisfacción del Servicio de Rentas Internas, equivalente al cinco por ciento (5%) del monto total del Contrato.*
CGC 19.3	*Se requiera una Garantía de Cumplimiento, la misma que deberá de presentarse en la forma de fianza o póliza de cumplimiento previo a la suscripción del Contrato.* *Las fianza o póliza estarán denominadas en dólares de los Estados Unidos de América.*

(…)

PREGUNTA 57.-

En la sección VI, Personal Técnico mínimo, pág. 57 se solicita en la titulación académica Ingeniero en sistemas, informática o afín, en este sentido entendemos que otros títulos de tercer nivel debidamente avalados por la SENESCYT como Licenciado en Redes y Sistemas Operativos, Tecnólogos en Electrónica y Telecomunicaciones y otros afines serán considerados como válidos para el proceso, por favor confirmar que nuestra interpretación es correcta.

RESPUESTA 57.-

Es correcto su entendimiento.

PREGUNTA 58.-

En la página 85 en la sección V. Formularios de la Oferta el documento denominado Autorización del Fabricante, se indica un formato para dicho certificado, en la práctica, los fabricantes tienen formatos preestablecidos para este tipo de certificado que indican en esencia lo mismo, pero en un formato distinto denominado Distribuidor Autorizado, que por ejemplo en el caso de uno de los fabricantes dice:

"*DISTRIBUIDOR AUTORIZADO"*

Estimados Señores

Por medio de la presente comunicamos a ustedes que la empresa xxxxxx es parte del programa de partners xxxxxx, lo cual les permite comercializar, soportar y administrar nuestras soluciones en el territorio de Ecuador.

La presente confirmación de estatus de Distribuidor Autorizado será válida durante la vigencia del contrato o hasta que el estatus de Distribuidor Autorizado cambie, lo que suceda primero.

Solicitamos que el Banco Interamericano / Servicio de Rentas Internas, en la presentación de la oferta acepte este tipo de formato realizado por el fabricante en lugar del establecido en los DDL – Formulario Autorización del Fabricante.

RESPUESTA 58.-

Conforme lo determinado en la Solicitud de Ofertas (SDO), Sección V. Formularios de la Oferta, pág. 85, el Formulario "Autorización del Fabricante", deberá estar escrito en papel membretado del fabricante, suscrito por una persona debidamente autorizada para firmar documentos que comprometan jurídicamente al fabricante; y, el fabricante deberá declarar que sus compromisos de prácticas de responsabilidad ambiental y social – ASSS, están alineadas al cumplimiento de las políticas ambientales y sociales, determinadas por el Banco Interamericano de Desarrollo.

PREGUNTA 59.-

Buen día, en base a la licitación **EC-L1253-P00016** xxxx se encuentra muy interesada en participar, por tal motivo solicitamos muy comedidamente se extienda el plazo de entrega

de la oferta debido a la complejidad de la misma, lo que nos tomará más tiempo de lo estipulado en el cronograma de entrega.

RESPUESTA 59.

Referirse al Boletín de Enmiendas Nro. 1

PREGUNTA 60.-

Estimados, en la sección Bienes requeridos, en el punto B. CLÚSTER DE FIREWALL PRINCIAL Y ALTERNO, en el punto 8. se indica : cada equipo debetener no menos de dos (2) interfaces físicas independientes (no compartidas) Ethernet 40 Gbps Base-SR QSFP+ LC; En relación a no compartidas, favor confirmar que la no compartición aplica solo a los puertos solicitados y que se aceptara un modelo, que en caso utilicen más puertos a futuro maneje compartición si se utiliza la capacidad de todos suspuertos.

RESPUESTA 60.

Referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 119 en la que se establece que:

"Conexión de red para tráfico de datos:

- *Cada equipo debe* ***tener no menos de dos (2) interfaces físicas independientes*** *(no compartidas) Ethernet 40 Gbps Base-SR QSFP+ LC;…" (énfasis añadido)*

Se solicita regirse a la Solicitud de Ofertas (SDO). para dar cumplimiento a las necesidades mínimas de puertos requeridos.

PREGUNTA 61.-

Estimados, en la sección Bienes requeridos, en el punto B. CLÚSTER DE FIREWALL PRINCIAL Y ALTERNO, en el punto 9. se indica: Cada equipo debe tener no menos de una (1) interfaz para sincronización; Favor confirmar que esta interfaz ser una de las interfaces de datos quetambién puede cumplir esta función.

RESPUESTA 61.

La necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 119, numeral 9 "Conexión de red para sincronización", establece que:

"Cada equipo debe tener ***no menos de una (1) interfaz para sincronización****…" (énfasis añadido)*

En función de lo expuesto, se solicita regirse a lo solicitado en la Solicitud de Ofertas (SDO). en la que indica que cada equipo debe tener no menos de una interfaz para sincronización independiente.

PREGUNTA 62.-

Estimados, en la sección Bienes requeridos, en el punto C. Servidores de Gestión Principal y Alterno (2 Equipos). Se detalla una solución de procesamiento y almacenamiento que no es dedicada y estandarizada para proyectos de Ciber Seguridad. Favor confirmar que se aceptará equipos dedicados para gestión, monitoreo y almacenamiento de logs con las siguientes características:

2x Plataforma de Gestión:

- 2 Puertos Fijos de gestión SFP+
- Memoria de 128 GB
- Procesador AMD de 24 cores
- 3.2 TB para eventos
- 10 Discos de 1.2 TB en raid 6
- 2 x 10/25 Gbps

SFP+2x Plataforma de Logs

- Procesador 2 AMD de 28 Core
- Memoria 16 x 32 GB DDR4 3200
- Almacenamiento 10x1.2 TB
- 2 Puertos de 10 Gigas

Las dos plataformas adecuadas para trabajar en ambientes de Datacenter, con

eficiencia de fuentes (80PlusPlatinum certified)

RESPUESTA 62.

La necesidad institucional se encuentra plasmada en la Solicitud de Ofertas (SDO), se solicita remitirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 120.

PREGUNTA 63.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto A. CLUSTER DE FIREWALL PRINCIPAL Y ALTERNO. *Se indica: Virtualización de Sistemas*, entendemos que esto se refiere a la virtualización de firewalls en conextos dentro del firewall. Favor confirmar.

RESPUESTA 63.

Es correcto su entendimiento, referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, VIRTUALIZACIÓN DE SISTEMAS, página 131, numeral 138, donde se establece lo siguiente:

"La función de sistemas virtuales debe ser de tecnología propietaria del fabricante del sistema de Firewalls de Nueva Generación. No se admiten tecnologías de virtualización de servidores (ej. VMware, Citrix, Microsoft, KVM y similares)."

PREGUNTA 64.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO. *Se indica: El Firewall debe contar con la opción de utilizar la negación como parte de la lógica de la condición de origen o de destino de las reglas de seguridad.* Favor confirmar que esta característica
se refiere al bloqueo de tráfico, dependiendo de origen y destino y no como tal una negación de política como tal que no es práctico en la lógica de ejecución del tráfico.

RESPUESTA 64.

No es correcto su entendimiento, se refiere a la capacidad que debe tener el firewall de aplicar reglas de seguridad que incluyan la negación, lo que significa que se pueda establecer condiciones para excluir ciertos orígenes o destinos en las comunicaciones de red, conforme a lo solicitado en la sección VI. Requisitos de los Bienes y Servicios Conexos, FIREWALL, página 123, numeral 21.

PREGUNTA 65.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO. *Se indica: El Firewall debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.* Favorconfirmar que se aceptara soluciones donde se indique solo la última fecha

de modificación ya que en la práctica las políticas tienen algunas modificaciones y si alguna no se modifica quedaría con la fecha inicial

RESPUESTA 65.

Referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, FIREWALL, página 123, numeral 27, donde se establece que:

"El Firewall debe mostrar la ***fecha de creación y última fecha de modificación*** *de la regla de seguridad" (énfasis añadido)*

En función de lo expuesto, se solicita referirse a la Solicitud de Oferta (SDO).

PREGUNTA 66.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO. *Se indica: El Firewall debe contar con la capacidad de insertar o modificar los valores en la cabecera HTTP del tráfico de aplicaciones SaaS.* Favor confirmar que este requerimiento es opcional yaque no es una funcional especifica de NGFW, además modificar las cabeceras HTTP puede afectar la integridad del tráfico y generar problemas en el funcionamiento de aplicaciones, especialmente SaaS.

RESPUESTA 66.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 124, numeral 41, donde se establece que:

"El Firewall debe contar con la capacidad de insertar o modificar los valores en la cabecera HTTP del tráfico de aplicaciones SaaS."

Se aclara que la capacidad de insertar o modificar los valores en la cabera HTTP del tráfico de aplicaciones SaaS es una función de firewalls de nueva generación.

PREGUNTA 67.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO. *Se indica: El ambiente de caja de arena ("sandbox")debe soportar la ejecución o detonación de al menos los tipos de archivosque se indican a continuación para su análisis. DMG, PKG.* Favor confimarque el soporte de archivos DMG, PKG es opcionales ya que el análisis de estos archivos en sandboxing no se ejecutan comúnmente en este tipo desistemas

y se restringe solo a un par de fabricantes.

RESPUESTA 67.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, PROTECCIÓN CONTRA AMENAZAS NO BASADA EN FIRMAS, página 127, numeral 74, establece que:

"El ambiente de caja de arena ("sandbox") debe soportar la ejecución o detonación de al menos los tipos de archivos que se indican a continuación para su análisis.

- *Archivos ejecutables, incluyendo: EXE, DLL, JAR, DMG, PKG;*
- *Archivos de Microsoft Office, incluyendo: DOC, DOCX, XLS, XLSX, PPT, PPTX;*
- *Archivos de formato portable, incluyendo: PDF;*
- *Archivos comprimidos, incluyendo: ZIP, RAR, 7Z;*
- *Archivos de scripts, incluyendo: VBS, PS1, JS."*

En función de lo expuesto, se solicita regirse a la necesidad institucional plasmada en la Solicitud de la Oferta (SDO)

PREGUNTA 68.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2Funcionalidad de Hardware. En el punto A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO. *Se indica: 80. La función de protección contra amenazas no basada en firmas debe emplear mecanismo basados en aprendizaje automático ("machine learning") para analizar imágenes enpáginas web y determinar si están imitando marcas conocidas como parte de una campaña phishing*. Estimados, favor confirmar que esta característica es opcional ya que corresponde a un funcionalidad de una marca especifica, y adicional este tiempo de controles se realiza con otrasherramientas y no con NGFW.

RESPUESTA 68.

Favor se solicita referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 127, numeral 80, en la que se establece que:

"La función de protección contra amenazas no basada en firmas debe emplear mecanismo basados en aprendizaje automático ("machine learning") para analizar imágenes en páginas web y determinar si están imitando marcas conocidas como parte de una campaña phishing."

PREGUNTA 69.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO. *Se indica: La función de protección contra amenazas no basada en firmas debe utilizar aprendizaje automático ("machine learning") para identificar las conexiones que utilizan DGA (algoritmos de generación de dominios).* Estimados, favor confirmar queesta característica es opcional ya que corresponde a una funcionalidad de una marca especifica,

RESPUESTA 69.

Favor se solicita referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 127, numeral 82, en la que se establece que:

"La función de protección contra amenazas no basada en firmas debe utilizar aprendizaje automático ("machine learning") para identificar las conexiones que utilizan DGA (algoritmos de generación de dominios)."

PREGUNTA 70.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO. *Se indica: 83. La función de protección contra amenazas no basada en firmas debe permitir reportar al fabricante los falsospositivos y los falsos negativos.* Estimados, favor confirmar que este requerimiento es opcional ya que en amenazas no basas en firmas se basamas en indicadores de compromiso donde no se indica un veredicto hastacuando ya se tiene una disposición de la posible amenaza.

RESPUESTA 70.

La necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 127, numeral 83, establece que:

"La función de protección contra amenazas no basada en firmas debe permitir reportar al fabricante los falsos positivos y los falsos negativos."

Se solicita regirse a lo solicitado en la Solicitud de la Oferta (SDO).

PREGUNTA 71.-

De acuerdo con lo solicitado en la página 59 del Personal Técnico Mínimo: Instructor de transferencia de conocimiento, teniendo en cuenta que la transferencia de conocimientos

debe ser impartida por una persona que tenga pleno conocimiento de la solución implementada, solicitamos que se acepte que uno de los técnicos de implementación pueda ser asignado para el rol mencionado.

RESPUESTA 71.

Conforme lo establecido en la Sección III. Criterios de Evaluación y Calificación, página 60, numerales 4 y 6de La Solicitud de Ofertas.

*"Se puede aceptar que el mismo recurso que **realice la instalación y migración** también realice el trabajo de soporte técnico." (énfasis añadido)*

*"Es responsabilidad del contratista incluir **la cantidad suficiente de recursos de personal** en cada rol para cumplir con los objetivos, entregables y plazos a lo largo de la vigencia del contrato." (énfasis añadido)*

PREGUNTA 72.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2Funcionalidad de Hardware. En el punto A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO. *Se indica: 95. La función de inspección SSL/TLS debe soportar la opción de integrarse con sistemas HSM ("Hardware Security Module") para almacenar claves criptográficas y certificados SSL/TLS.* Favor confirmar que este requerimiento es opción ya que este tipo de funciones se puede realizar en equipos dedicados para desencriptar.

RESPUESTA 72.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 128, numeral 95, donde se establece que:

*"La función de inspección SSL/TLS **debe soportar la opción de integrarse con sistemas HSM** ("Hardware Security Module") para almacenar claves criptográficas y certificados SSL/TLS." (énfasis añadido)*

Se aclara que este requisito debe incluir la capacidad de que la función de inspección SSL/TLS se integre con un sistema HSM.

PREGUNTA 73.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO. *Se indica:* 101. *La función de identificación de usuarios debe soportar ser desplegada al menos de las siguientes formas:Instalando un agente en los puntos finales.* Favor

confirmar que este requerimiento es opcional ya que para esta funcionalidad se debería incluir un agente de protección de endpoint en cada uno de los puntos finales y encarecería la solución. Adicional, esta es una funcionalidad que solo cumple un fabricante.

RESPUESTA 73.

Se solicita remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 129, numeral 101, donde se establece que:

"La función de identificación de usuarios debe soportar ser desplegada al menos de las siguientes formas:

- *Sin agente ("agentless");*
- *Instalando un agente en los puntos finales."*

PREGUNTA 74.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO. *Se indica: 104. La función de identificación de usuarios debe tener la capacidad de leer las cabeceras XFF ("X-Forward-For") para obtener información de la identidad del usuario que está navegando mediante un proxy web.* Favor confirmar que este requerimiento es opcional ya que cierra la participación solo a dos fabricantes.

RESPUESTA 74.

Se confirma que no es un requerimiento opcional, se solicita regirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 129, numeral 104.

"La función de identificación de usuarios debe tener la capacidad de leer las cabeceras XFF ("X-Forward-For") para obtener información de la identidad del usuario que está navegando mediante un proxy web."

PREGUNTA 75.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO. *Se indica: 105. La función de identificación de usuarios debe tener la capacidad de eliminar en el tráfico saliente a Internet las cabeceras XFF ("X-Forward-For") introducidas por el proxy web.* Favor confirmar que este requerimiento es opcional ya que cierra la participación solo a dos fabricantes.

RESPUESTA 75.

Se confirma que no es un requerimiento opcional, se solicita regirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 129, numeral 105.

"La función de identificación de usuarios debe tener la capacidad de eliminar en el tráfico saliente a Internet las cabeceras XFF ("X-Forward-For") introducidas por el proxy web."

PREGUNTA 76.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto B. GESTORES PRINCIPAL Y ALTERNO *Se indica: La gestión debe tener la capacidad de funcionar comoentidad certificadora subalterna de una entidad certificadora externa al sistema de Firewalls.* Favor confirmar que este requerimiento es opcionaldebido a que las mejores prácticas indican que la entidad certificadora debería estar localiza, en el equipo que recibe los enlaces de conectividadcomo balanceadores.

RESPUESTA 76.

Se aclara que la gestión del sistema de Firewalls debe ser capaz de actuar como una entidad certificadora subordinada a otra entidad certificadora externa. Esto implica que la gestión debe verificar y validar la autenticidad y la integridad de las comunicaciones o transacciones que se realicen a través de los firewalls, siguiendo las directrices y estándares establecidos por una entidad certificadora principal.

En función de lo expuesto, se solicita remitirse a la necesidad plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 132, numeral 11, que establece:

"La gestión debe tener la capacidad de funcionar como entidad certificadora subalterna de una entidad certificadora externa al sistema de Firewalls."

PREGUNTA 77.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto B. GESTORES PRINCIPAL Y ALTERNO *Se indica: 25. La gestión de políticas debe tener la capacidad deintegrarse con el sistema Active Directory del SRI (véase INFRAESTRUCTURA ACTUAL) para importar objetos de manera que se puedan utilizar comoorigen o destino para crear reglas de seguridad.* Favor confirmar que la integración con el Directorio activo es para importar los usuarios (Objetos) ypoder manejar políticas específicas de usuarios.

RESPUESTA 77.

Se aclara que los objetos a importarse desde el sistema Active Directory son: usuarios y grupos de usuarios, sin limitarse a otros objetos del Active Directory.

PREGUNTA 78.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto B. GESTORES PRINCIPAL Y ALTERNO *Se indica: 31. La gestión de políticas debe soportar el uso de etiquetas en los objetos de la política para facilitar su búsqueda o paraestablecer asociaciones entre estos.* Favor confirmar que se aceptara soluciones que permitan buscar políticas a través de filtros, y que las etiquetas en objetos es opcional, debido a que los filtros específicos permite una búsqueda efectiva de políticas.

RESPUESTA 78.

Se solicita regirse a la necesidad institucional plasmada en la Solicitud de Oferta (SDO). en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 133, numeral 31, donde se establece que:

"La gestión de políticas debe soportar el uso de etiquetas en los objetos de la política para facilitar su búsqueda o para establecer asociaciones entre estos."

PREGUNTA 79.-

Estimados, en la sección Bienes requeridos, en el numeral 6.1.2 Funcionalidad de Hardware. En el punto B. GESTORES PRINCIPAL Y ALTERNO *Se indica: 47. La gestión de los eventos debe permitir al administrador configurar el tamaño del archivo para rotación de los archivosde registros de eventos ("logs").* Favor confirmar que este requerimiento es opcional ya que cada fabricante maneja el registro de eventos de la formamas eficiente según su arquitectura, y no se usan necesariamente archivospara registros de eventos, sino bases de datos.

RESPUESTA 79.

Se solicita remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 134, numeral 47:

"La gestión de los eventos debe permitir al administrador configurar el tamaño del archivo para rotación de los archivos de registros de eventos ("logs")."

PREGUNTA 80.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO *Se indica: 23. La solución debe detectar la manipulación sospechosa de buzones de usuarios y reglas de correo en Exchange Online, por parte de un perfil administrador, y debe tomar accionesde respuesta, tales como, la eliminación de la regla identificada como riesgosa.* Favor confirmar que este requerimiento es opcional debido a quees muy específico y cerrado a una sola marca.

RESPUESTA 80.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, PROTECCIÓN DE CORREO ELECTRÓNICO, numeral 23, donde se establece que:

"La solución debe detectar la manipulación sospechosa de buzones de usuarios y reglas de correo en Exchange Online, por parte de un perfil administrador, y debe tomar acciones de respuesta, tales como, la eliminación de la regla identificada como riesgosa."

PREGUNTA 81.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO *Se indica: 24. La solución debe permitir la adición de etiquetas en el correo electrónico entrante que permitan al menos informar al destinatario: Si es un dominio recientemente registrado.* Favor confirmar que este es un requerimiento opcional ya que no da ningúnvalor al destinatario saber si un dominio ha sido recientemente registrado.

RESPUESTA 81.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 82.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de

Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO Se indica: *38. La solución debe permitir al administrador configurar las reglas de protección de correo electrónico en base de al menos los siguientes parámetros:*

- *Cantidad de archivos contenidos en un solo archivo comprimido,*
- *Metadatos de archivo adjuntos*
- *Número de restantes,*
- *Tiempo de registro de dominio utilizado en los campos de o MFROM,*
- *Antigüedad del dominio utilizado en el campo desde y/o MFROM.*

Favor confirmar que estos parámetros son opcionales debido que son muyespecíficos, no generan valor en la protección de correo electrónico y estan dirigidos solo a un fabricante.

RESPUESTA 82.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 83.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO Se indica: *51. La solución debe proporcionaruna función de "vista previa segura" para que los administradores puedan verinformación detallada de los mensajes en cuarentena y decidir las acciones necesarias.* Estimados, este requerimiento es redundante debido a que unmensaje en cuarentena va a ser analizado por todos los motores de inspección de los cuales cuenta la solución y entregar un veredicto. Debido a esto favor confirmar que la vista previa segura es opcional.

RESPUESTA 83.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 145, numeral 51, donde se establece que:

“La solución debe proporcionar una función de "vista previa segura" para que los administradores puedan ver información detallada de los mensajes en cuarentena y decidir las acciones necesarias.”

PREGUNTA 84.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de

Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO Se indica: *54. La solución debe soportar el análisis y la aplicación de acciones específicas para archivos cifrados o protegidos por contraseña o con compresión múltiple.* Favor confirmar que este requerimiento es opcional debido a que es muy específico y solo lo cumple un fabricante.

RESPUESTA 84.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 85.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO Se indica: *55. La solución debe contar con inteligencia que permita intentar acceder a un archivo protegido con contraseña utilizando información contextual del mensaje utilizado para suenvío.* Favor confirmar que este requerimiento es opcional debido a que esmuy específico y solo lo cumple un fabricante.

RESPUESTA 85.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 86.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO Se indica: *60. Si al momento de realizar análisisde sandboxing de un hipervínculo el recurso web asociado no se encuentra disponible, la solución debe contar con la opción de que el mensaje seaentregado no sin antes reescribir la dirección URL del hipervínculo de manera que, si el usuario hace clic, este se despliegue en un entorno controlado y aislado.* Favor confirmar que este requerimiento es opcional debido a que es muy específico y solo lo cumple un fabricante.

RESPUESTA 86.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 87.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO Se indica: *63. La solución debe ser capaz deanalizar al menos los siguientes tipos de archivos comprimidos: ZIP, TGZ, 7Z,CAB, LZH, RAR, TNEF.* Favor confirmar que el tipo de archivo TNEF es opcional debido a que no es común en el manejo de archivos comprimidosy solo lo soporta un fabricante

RESPUESTA 87.-

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 88.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO Se indica: 67 *.La solución debe contar con protecciones especializadas para amenazas de tipo: "delay exploits"* . Favorconfirmar que este tipo de amenazas es opcional debido que son muy específicas y las cumple solo un fabricante.

RESPUESTA 88.-

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 146 ,CONTROL DE PHISHING, numeral 67, donde se establece que:

"La solución debe contar con protecciones especializadas para amenazas de tipo:

- *"Email Account Compromise" (EAC),*
- *"Business Email Compromise" (BEC),*
- *"spear phishing",*
- *"whaling",*
- *"delayed exploits"."*

PREGUNTA 89.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO Se indica: *68 .La solución debe ser capaz de analizar tanto el encabezado como el contenido del mensaje para detectar e identificar ataques de suplantación de dominio, suplantación de nombre para mostrar y estrategias de "typosquatting".* Favor confirmar que esterequerimiento es opcional debido a que es muy específico y solo lo cumpleun fabricante.

RESPUESTA 89.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 146 ,CONTROL DE PHISHING, numeral 68, donde se establece que:

"La solución debe ser capaz de analizar tanto el encabezado como el contenido del mensaje para detectar e identificar ataques de suplantación de dominio, suplantación de nombre para mostrar y estrategias de "typosquatting"."

PREGUNTA 90.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO Se indica: *74. La solución debe tener la capacidad de reescribir la dirección URL del hipervínculo de manera que, siel usuario hace clic, este se despliegue en un entorno controlado y aislado.*Favor confirmar que este requerimiento es opcional debido a que es muyespecífico y solo lo cumple un fabricante.

RESPUESTA 90.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 91.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO Se indica: *75. La solución debe ser capazde retener la entrega de los mensajes de correo electrónico mientras seanalizan todas las direcciones URL que contienen.* Favor confirmar que esterequerimiento es opcional debido a que es muy específico y solo lo cumpleun fabricante.

RESPUESTA 91.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 146, CONTROL DE PHISHING, numeral 75, donde se establece que:

"La solución debe ser capaz de retener la entrega de los mensajes de correo electrónico mientras se analizan todas las direcciones URL que contienen."

PREGUNTA 92.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO Se indica: *76. La solución debediscriminar a los usuarios que estadísticamente han recibido más mensajes de phishing o con direcciones URL maliciosas para aplicarle proteccionesde seguridad más rigurosas.* Favor confirmar que este requerimiento es opcional debido a que es muy específico y solo lo cumple un fabricante.

RESPUESTA 92.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 146, CONTROL DE PHISHING, numeral 76, donde se establece que:

"La solución debe discriminar a los usuarios que estadísticamente han recibido más mensajes de phishing o con direcciones URL maliciosas para aplicarle protecciones de seguridad más rigurosas."

PREGUNTA 93.-

Estimados, en la sección Bienes requeridos, en el numeral 6.2 Componentes de Software. En el punto B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO Se indica: *88. La solución debe contarcon paneles ("dashboards") o reportes que provean al administrador información sobre estadísticas y tendencias de las amenazas de seguridad detectadas, incluyendo:*

- *Correos electrónicos filtrados,*
- *Credenciales de usuarios expuestas,*
- *Accesos OAuth no seguros,*
- *Compartición riesgosa de archivos en las aplicaciones de Microsoft Office 365,*

Favor confirmar que esos Dashbords o reporters, son opcionales para garantizar la participación debido a que son muy específicos y solo losmaneja un fabricante.

RESPUESTA 93.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 94.-

Estimados por favor su ayuda extiendo en tiempo de entrega de los equipos, puesto que están solicitando un tiempo de 90 días incluido lainstalación, lo que se dificulta para equipos de importación.

RESPUESTA 94.

Por favor remitirse a lo solicitado en la Sección VIII. Condiciones Especiales de Contrato (CEC), BIENES REQUERIDOS, numeral1, donde se establece que:

"El plazo de la entrega de los bienes instalados será de hasta 90 días calendario contados a partir de la notificación del administrador del contrato. Para el efecto, el contratista deberá entregar el oficio de culminación de la instalación del hardware."

PREGUNTA 95.-

Estimados en la sección de **Certificación Bancaria del Proveedor**, por favor confirmar que la misma no aplica, debido a que este proceso no contempla anticipo.
Por favor confirmar nuestro entendimiento.

RESPUESTA 95.

La certificación bancaria solicitada, únicamente aplica para el oferente adjudicado. Dicha certificación servirá para el registro de la cuenta donde se realizarán los pagos del presente proceso.

PREGUNTA 96.-

Estimados solicitamos muy comedidamente se extienda el plazo de entregade la oferta debido a la complejidad de la misma, lo que nos tomará mástiempo de lo estipulado en el cronograma de entrega. Gracias

RESPUESTA 96.

Referirse al Boletín de Enmiendas Nro. 1

PREGUNTA 97.-

en base a la licitación **EC-L1253-P00016,** uno de los posibles oferentes. quiere realizar una aclaración, solicitando que se pueda presentar una Póliza de Fiel Cumplimiento en reemplazo de una garantía de fiel cumplimiento (garantía bancaria).

RESPUESTA 97.

El SRI, no solicita Garantía Bancaria. Conforme lo señalado en la SDO de la Sección VIII. Condiciones Especiales de Contrato (CEC), pág. 175, en las CGC 19.1 y CGC 19.3, se establece las condiciones de la garantía para el cumplimiento del contrato, que señalan:

"(…)

CGC 19.1	Garantía de Cumplimiento del Contrato: Para seguridad del cumplimiento de este Contrato y para responder de las obligaciones que se contrajeren a favor de terceros, relacionados con el mismo, el Proveedor rinde una garantía a satisfacción del Servicio de Rentas Internas, equivalente al cinco por ciento (5%) del monto total del Contrato.
CGC 19.3	Se requiera una Garantía de Cumplimiento, la misma que deberá de presentarse en la forma de fianza o póliza de cumplimiento previo a la suscripción del Contrato. Las fianza o póliza estarán denominadas en dólares de los Estados Unidos de América.

(…)

PREGUNTA 98.-

Condiciones Generales

Montaje de los Equipos

Se sugiere cambiar la especificación "*4. Todos los equipos deben ser servidores de bastidor ("rack-mounted servers") compatibles con las condiciones físicas de los centros de datos del SRIque constan en la INFRAESTRUCTURA ACTUAL.*" por "*4. Todos los equipos deben ser del tipo "rack-mounted", compatibles con las condiciones físicas de los centros de datos del SRI que constan en laINFRAESTRUCTURA ACTUAL.*"

RESPUESTA 98.

Referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 118, MONTAJE DE LOS EQUIPOS, 6.1.1 CONDICIONES GENERALES, numeral 4, donde se establece que:

*"Todos los equipos deben ser servidores de bastidor ("rack-mounted servers") compatibles con las condiciones físicas de los centros de datos del SRI que constan en la **INFRAESTRUCTURA ACTUAL**."*

No se acepta la sugerencia, ya que la especificación técnica del numeral 4, MONTAJE DE LOS EQUIPOS, responde a una necesidad institucional claramente definida.

PREGUNTA 99.-

CLUSTER DE FIREWALL PRINCIPAL Y ALTERNO

Para el **punto de cumplimiento 8**, se sugiere cambiar la especificación "*...dos (2) interfaces físicas independientes (no compartidas)...*" por "*...dos (2) interfaces físicas...*".

RESPUESTA 99.

No se acepta la sugerencia, ya que la especificación técnica del numeral 8, Sección VI, Requisitos de los Bienes y Servicios Conexos, en la página 119, responde a una necesidad institucional claramente definida.

PREGUNTA 100.-

CLUSTER DE FIREWALL PRINCIPAL Y ALTERNO

Para el **punto de cumplimiento 9**, se sugiere cambiar la especificación "*Cada equipo debe tenerno menos de una (1) interfaz para sincronización*" por "*Cada equipo debe permitir la sincronización con su par en alta disponibilidad*", debido a que, asícomo se encuentra planteada, la consideramos como restrictiva, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 100.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 119, numeral 9, donde se establece que:

"Conexión de red para sincronización:

- *Cada equipo debe tener no menos de una (1) interfaz para sincronización;*
- *La interfaz de sincronización puede ser de tecnología propietaria (ej. factor de forma, protocolo, estándar, etc.), en cuyo caso el contratista deberá proveer todos los componentes físicos y lógicos para su operación;*
- *Si la interfaz de sincronización es de tecnología abierta, cada equipo debe tener una (1) interfaz Ethernet 10 Gbps Base-SR SFP+ LC;*

- *Cada equipo debe contar con los transceptores ("transceivers") propios de fábrica necesarios para la operación de las interfaces de sincronización."*

PREGUNTA 101.-

SERVIDORES DE GESTIÓN PRINCIPAL Y ALTERNO

Los equipos para la gestión de Firewalls, principal yalterno, **¿podrían ser appliances de propósito específico?**

RESPUESTA 101.

Referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 104, 5.2 INSTALACIÓN DEL HARDWARE, numeral 5, donde se establece que:

"Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como appliance virtual o como máquina virtual (VM) en su respectivo servidor de gestión tal como se indica en la tabla a continuación.

COMPONENTE DE SOFTWARE	***SERVIDOR FÍSICO***	***SITIO***
Gestor de firewall principal	*Servidor de gestión principal*	*CD Principal*
Componente de análisis de configuración y eventos principal	*Servidor de gestión principal*	*CD Principal*
Gestor de firewall alterno	*Servidor de gestión alterno*	*CD Alterno*
Componente de análisis de configuración y eventos alterno	*Servidor de gestión alterno*	*CD Alterno*

Tabla 6. *Correspondencia entre instancias virtuales y servidores físicos."*

En función de lo expuesto, los servidores de gestión principal y alterno no pueden ser appliance de propósito específico.

PREGUNTA 102.-

SERVIDORES DE GESTIÓN PRINCIPAL Y ALTERNO

Para el **punto de cumplimiento 4**, en el caso de que se acepten soluciones de propósito específico,se sugiere cambiar la especificación "*…48 núcleos…*"por"*…24 núcleos…*"y la especificación"*…2.6 GHz…*" por "*…2.3 GHz…*", debido a que, así como se encuentran planteadas, las consideramoscomo restrictivas, lo que impide la libreparticipación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 102.

Referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 104, 5.2 INSTALACIÓN DEL HARDWARE, numeral 5, donde se establece que:

"Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como appliance virtual o como máquina virtual (VM) en su respectivo servidor de gestión tal como se indica en la tabla a continuación.

COMPONENTE DE SOFTWARE	***SERVIDOR FÍSICO***	***SITIO***
Gestor de firewall principal	*Servidor de gestión principal*	*CD Principal*
Componente de análisis de configuración y eventos principal	*Servidor de gestión principal*	*CD Principal*
Gestor de firewall alterno	*Servidor de gestión alterno*	*CD Alterno*
Componente de análisis de configuración y eventos alterno	*Servidor de gestión alterno*	*CD Alterno*

Tabla 6. *Correspondencia entre instancias virtuales y servidores físicos."*

En función de lo expuesto, los servidores de gestión principal y alterno no pueden ser appliance de propósito específico, por lo tanto, no se acoge su sugerencia.

PREGUNTA 103.-

SERVIDORES DE GESTIÓN PRINCIPAL Y ALTERNO

Para el **punto de cumplimiento 5**, en el caso de que se acepten soluciones de propósito específico,se sugiere cambiar las especificaciones "*…256 GB…*" por "*…128 GB…*", "*…DDR5…*" por "*…DDR4/DDR5…*" y "*…4400 MHz…*" por "*…3200 MHz…*", debido a que, así como se encuentran planteadas, las consideramos como restrictivas, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 103.

Referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 104, 5.2 INSTALACIÓN DEL HARDWARE, numeral 5, donde se establece que:

"Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como appliance virtual o como máquina virtual (VM) en su respectivo servidor de gestión tal como se indica en la tabla a continuación.

COMPONENTE DE SOFTWARE	*SERVIDOR FÍSICO*	*SITIO*
Gestor de firewall principal	*Servidor de gestión principal*	*CD Principal*
Componente de análisis de configuración y eventos principal	*Servidor de gestión principal*	*CD Principal*
Gestor de firewall alterno	*Servidor de gestión alterno*	*CD Alterno*
Componente de análisis de configuración y eventos alterno	*Servidor de gestión alterno*	*CD Alterno*

Tabla 6. *Correspondencia entre instancias virtuales y servidores físicos."*

En función de lo expuesto, los servidores de gestión principal y alterno no pueden ser appliance de propósito específico, por lo tanto, no se acoge su sugerencia.

PREGUNTA 104.-

SERVIDORES DE GESTIÓN PRINCIPAL Y ALTERNO

En el caso de que se acepten soluciones depropósito específico, siempre garantizando una alta disponibilidad del servicio de gestión deFirewalls, **¿se podrían omitir los puntos de cumplimiento 6 y 7?**, los mismos que se encuentran orientados a soluciones basadas en servidores de cómputo genéricos con recursos de procesamiento, memoria y almacenamiento específicos.

RESPUESTA 104.

Referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 104, 5.2 INSTALACIÓN DEL HARDWARE, numeral 5, donde se establece que:

"Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como appliance virtual o como máquina virtual (VM) en su respectivo servidor de gestión tal como se indica en la tabla a continuación.

COMPONENTE DE SOFTWARE	*SERVIDOR FÍSICO*	*SITIO*
Gestor de firewall principal	*Servidor de gestión principal*	*CD Principal*
Componente de análisis de configuración y eventos principal	*Servidor de gestión principal*	*CD Principal*
Gestor de firewall alterno	*Servidor de gestión alterno*	*CD Alterno*
Componente de análisis de configuración y eventos alterno	*Servidor de gestión alterno*	*CD Alterno*

Tabla 6. *Correspondencia entre instancias virtuales y servidores físicos."*

En función de lo expuesto, los servidores de gestión principal y alterno no pueden ser appliance de propósito específico, por lo tanto, no se acoge su sugerencia.

PREGUNTA 105.-

SERVIDORES DE GESTIÓN PRINCIPAL Y ALTERNO

Para el **punto de cumplimiento 5**, en el caso de que se acepten soluciones de propósito específico,se sugiere cambiar la especificación "*Mediosvirtuales (ej. CD's, DVD's, etc.)*" por "*Medios virtuales (ej. CD's, DVD's, etc.) o USB 3.0 Tipo A.*".

RESPUESTA 105.

Referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 104, 5.2 INSTALACIÓN DEL HARDWARE, numeral 5, donde se establece que:

"Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como appliance virtual o como máquina virtual (VM) en su respectivo servidor de gestión tal como se indica en la tabla a continuación.

COMPONENTE DE SOFTWARE	***SERVIDOR FÍSICO***	***SITIO***
Gestor de firewall principal	*Servidor de gestión principal*	*CD Principal*
Componente de análisis de configuración y eventos principal	*Servidor de gestión principal*	*CD Principal*
Gestor de firewall alterno	*Servidor de gestión alterno*	*CD Alterno*
Componente de análisis de configuración y eventos alterno	*Servidor de gestión alterno*	*CD Alterno*

Tabla 6. *Correspondencia entre instancias virtuales y servidores físicos."*

En función de lo expuesto, los servidores de gestión principal y alterno no pueden ser appliance de propósito específico, por lo tanto, no se acoge su sugerencia.

PREGUNTA 106.-

SERVIDORES DE GESTIÓN PRINCIPAL Y ALTERNO

Se sugiere considerar como **opcional** el **punto de cumplimiento 10**, debido a que, así como se encuentra planteado, la consideramos como restrictiva, lo que impide la libre participación de oferentes con soluciones de otras marcas concapacidades similares.

RESPUESTA 106.

Favor referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 121, numeral 10, donde se establece que:

"Configuración de Alto Desempeño:

- *El firmware de cada equipo debe tener la funcionalidad de alto desempeño ("high performance") o equivalente;*

Cada equipo debe contar con los módulos de disipación de calor, ventiladores y fuentes de alimentación (PSU) dimensionados para soportar la operación de este en modo alto desempeño ("high performance") o equivalente."

PREGUNTA 107.-

SERVIDORES DE GESTIÓN PRINCIPAL Y ALTERNO

Para el **punto de cumplimiento 11**, en el caso deque se acepten soluciones de propósito específico, se sugiere considerar como **opcional** la especificación "*Cada fuente de alimentación debetener una eficiencia de no menos del 90%*", debidoa que, así como se encuentra planteada, la consideramos como restrictiva, lo que impide lalibre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 107.

Referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 104, 5.2 INSTALACIÓN DEL HARDWARE, numeral 5, donde se establece que:

"Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como appliance virtual o como máquina virtual (VM) en su respectivo servidor de gestión tal como se indica en la tabla a continuación.

COMPONENTE DE SOFTWARE	***SERVIDOR FÍSICO***	***SITIO***
Gestor de firewall principal	*Servidor de gestión principal*	*CD Principal*
Componente de análisis de configuración y eventos principal	*Servidor de gestión principal*	*CD Principal*
Gestor de firewall alterno	*Servidor de gestión alterno*	*CD Alterno*
Componente de análisis de configuración y eventos alterno	*Servidor de gestión alterno*	*CD Alterno*

Tabla 6. *Correspondencia entre instancias virtuales y servidores físicos."*

En función de lo expuesto, los servidores de gestión principal y alterno no pueden ser appliance de propósito específico, por lo tanto, no se acoge su sugerencia.

PREGUNTA 108.-

CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO

Para el **punto de cumplimiento 20**, se sugierecambiar la especificación "*El Firewall debe soportar el uso de etiquetas en los objetos para sureferenciación o agrupación*" por "*El Firewall debesoportar el uso de etiquetas o categorías en los objetos o políticas para su referenciación o agrupación*", debido a que, así como se encuentra planteada, la consideramos como restrictiva, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 108.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 109.-

CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO

Se sugiere considerar como **opcional** el **punto de cumplimiento 21**, debido a que, así como se encuentra planteado, lo consideramos como restrictivo, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 109.

Favor referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 123, FIREWALL (FW), numeral 21, donde se establece que:

"El Firewall debe contar con la opción de utilizar la negación como parte de la lógica de la condición de origen o de destino de las reglas de seguridad."

PREGUNTA 110.-

CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO

Para el **punto de cumplimiento 27**, se sugierecambiar la especificación "*El Firewall debe mostrarla fecha de creación y última fecha de modificaciónde la regla de seguridad*" por "*El Firewall debe mostrar la última fecha de modificación de la reglade seguridad*", debido a que, así como se encuentraplanteada, la consideramos como restrictiva, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 110.

Favor referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, FIREWALL, página 123, numeral 27, donde se establece que:

*"El Firewall debe mostrar la **fecha de creación y última fecha de modificación** de la regla de seguridad" (énfasis añadido)*

PREGUNTA 111.-

CONTROL DE NAVEGACIÓN

Se sugiere considerar como **opcional** el **punto de cumplimiento 41**, debido a que, así como se encuentra planteado, lo consideramos como restrictivo, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 111.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 124, numeral 41, donde se establece que:

"El Firewall debe contar con la capacidad de insertar o modificar los valores en la cabecera HTTP del tráfico de aplicaciones SaaS."

Se aclara que la capacidad de insertar o modificar los valores en la cabera HTTP del tráfico de aplicaciones SaaS es una función de firewalls de nueva generación.

PREGUNTA 112.-

PROTECCIÓN CONTRA AMENAZAS NO BASADA EN FIRMAS

Para el **punto de cumplimiento 71**, se sugierecambiar la especificación "*La función de protección contra amenazas no basada en firmasdebe incluir el uso del análisis de caja de arena ("sandboxing") y de aprendizaje automático ("machine learning")*" por "*La función de protección contra amenazas no basada en firmasdebe incluir el uso del análisis de caja de arena ("sandboxing")*", debido a que, así como se encuentra planteada, la consideramos como restrictiva, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 112.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 126, PROTECCIÓN CONTRA AMENAZAS NO BASADA EN FIRMAS, numeral 71, donde se establece que:

"La función de protección contra amenazas no basada en firmas debe incluir el uso del análisis de caja de arena ("sandboxing") y de aprendizaje automático ("machine learning")."

PREGUNTA 113.-

PROTECCIÓN CONTRA AMENAZAS NO BASADA EN FIRMAS

Para el **punto de cumplimiento 74**, se sugiere considerar como **opcionales** los formatos de archivos ejecutables **DMG** y **PKG**, debido a que, así como se encuentran planteados, los consideramos como restrictivos, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 113.

Los archivos con extensiones DMG y PKG, son ejecutables comunes en sistemas macOS con los que cuenta el SRI.

Favor referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, PROTECCIÓN CONTRA AMENAZAS NO BASADA EN FIRMAS, página 127, numeral 74, establece que:

"El ambiente de caja de arena ("sandbox") debe soportar la ejecución o detonación de al menos los tipos de archivos que se indican a continuación para su análisis.

- *Archivos ejecutables, incluyendo: EXE, DLL, JAR, DMG, PKG;*
- *Archivos de Microsoft Office, incluyendo: DOC, DOCX, XLS, XLSX, PPT, PPTX;*
- *Archivos de formato portable, incluyendo: PDF;*
- *Archivos comprimidos, incluyendo: ZIP, RAR, 7Z;*
- *Archivos de scripts, incluyendo: VBS, PS1, JS."*

PREGUNTA 114.-

PROTECCIÓN CONTRA AMENAZAS NO BASADA EN FIRMAS

Se sugiere considerar como **opcionales** los **puntos de cumplimiento 80 y 82**, debido a que, así como se encuentra planteados, los consideramos como restrictivos, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 114.

Favor se solicita referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 127, numeral 80, en la que se establece que:

"La función de protección contra amenazas no basada en firmas debe emplear mecanismo basados en aprendizaje automático ("machine learning") para analizar imágenes en páginas web y determinar si están imitando marcas conocidas como parte de una campaña phishing."

Asimismo, favor se solicita referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 127, numeral 82, en la que se establece que:

"La función de protección contra amenazas no basada en firmas debe utilizar aprendizaje automático ("machine learning") para identificar las conexiones que utilizan DGA (algoritmos de generación de dominios)."

PREGUNTA 115.-

PROTECCIÓN CONTRA AMENAZAS NO BASADA EN FIRMAS

Para el **punto de cumplimiento 83**, se sugierecambiar la especificación "*La función de protección contra amenazas no basada en firmas debe permitir reportar al fabricante los falsos positivos y los falsos negativos*" por "*La función deprotección contra amenazas no basada en firmasdebe permitir reportar al fabricante los falsos positivos y los falsos negativos. También, se aceptan soluciones que permitan realizar esta funcionalidad desde un portal del fabricante*", debido a que, así como se encuentra planteada, la consideramos como restrictiva, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 115.

Referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 127, numeral 83, donde se establece que:

"La función de protección contra amenazas no basada en firmas debe permitir reportar al fabricante los falsos positivos y los falsos negativos."

PREGUNTA 116.-

INSPECCIÓN SSL/TLS

Para el **punto de cumplimiento 95**, se sugierecambiar la especificación "*La función de inspección SSL/TLS debe soportar la opción de integrarse con sistemas HSM ("Hardware Security Module") para almacenar claves criptográficas y certificados SSL/TLS*" por "*La función de inspección SSL/TLS debe soportar la opción de integrarse con sistemas HSM ("Hardware Security Module") para almacenar claves criptográficas y certificados SSL/TLS, o el equipo ofertado debecumplir con el estandar FIPS140-2*", debido a que, así como se encuentra planteada, la consideramoscomo restrictiva, lo que

impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 116.

El estándar FIPS140-2 no es una necesidad institucional, por lo tanto, regirse a lo solicitado en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 128, numeral 95: *"La función de inspección SSL/TLS debe soportar la opción de integrarse con sistemas HSM ("Hardware Security Module") para almacenar claves criptográficas y certificados SSL/TLS."*

PREGUNTA 117.-

IDENTIFICACIÓN DE USUARIOS

Para el **punto de cumplimiento 101**, se sugiere cambiar la especificación "*Instalando un agente enlos puntos finales*" por "*Instalando un agente en lospuntos finales o en servidores del dominio*", debidoa que, así como se encuentra planteada, la consideramos como restrictiva, lo que impide lalibre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 117.

Se solicita remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 129, numeral 101, donde se establece que:

"La función de identificación de usuarios debe soportar ser desplegada al menos de las siguientes formas:

- *Sin agente ("agentless");*
- *Instalando un agente en los puntos finales."*

PREGUNTA 118.-

IDENTIFICACIÓN DE USUARIOS

Para el **punto de cumplimiento 104**, se sugiere cambiar la especificación "*La función de identificación de usuarios...*" por "*La función de identificación de usuarios o dispositivos…*", debidoa que, así como se encuentra planteada, la consideramos como restrictiva, lo que impide lalibre participación de oferentes con soluciones deotras marcas con capacidades similares.

RESPUESTA 118.

Se solicita regirse a la necesidad institucional plasmada en la sección VI. Requisitos de

los Bienes y Servicios Conexos, página 129, numeral 104.

"La función de identificación de usuarios debe tener la capacidad de leer las cabeceras XFF ("X-Forward-For") para obtener información de la identidad del usuario que está navegando mediante un proxy web."

PREGUNTA 119.-

IDENTIFICACIÓN DE USUARIOS

Se sugiere considerar como **opcional** el **punto de cumplimiento 105**, debido a que, así como se encuentra planteado, lo consideramos como restrictivo, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 119.

Se confirma que no es un requerimiento opcional, se solicita regirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 129, numeral 105.

"La función de identificación de usuarios debe tener la capacidad de eliminar en el tráfico saliente a Internet las cabeceras XFF ("X-Forward-For") introducidas por el proxy web."

PREGUNTA 120.-

GESTORES PRINCIPAL Y ALTERNO

Se sugiere considerar como **opcional** el **punto de cumplimiento 11**, debido a que, así como se encuentra planteado, lo consideramos como restrictivo, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 120.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 121, numeral 11, donde se establece que:

"Alimentación:

- *Cada equipo debe tener instaladas dos fuentes de alimentación (PSU) redundantes tipo "hot-swap";*
- *Cada fuente de alimentación debe soportar un rango de entrada de 110-220 VAC o más amplio;*
- *Cada fuente de alimentación debe tener una eficiencia de no menos del 90%."*

PREGUNTA 121.-

GESTIÓN DE POLÍTICAS

Se sugiere considerar como **opcionales** los **puntosde cumplimiento 25 y 31**, debido a que, así comose encuentran planteados, los consideramos comorestrictivos, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 121.

Referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 123, CONTROL DE NAVEGACIÓN, numeral 25, donde se establece que:

"El Firewall debe soportar que se añada un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y control de cambios."

Referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 123, CONTROL DE NAVEGACIÓN, numeral 31, donde se establece que:

"El Firewall debe aplicar la función de control de navegación mediante acciones tales como: permitir, bloquear, aplicar control por tiempo."

PREGUNTA 122.-

GESTIÓN DE EVENTOS

Se sugiere considerar como **opcional** el **punto de cumplimiento 47**, debido a que, así como se encuentra planteado, lo consideramos como restrictivo, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 122.

Referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 134, donde se establece que:

"La gestión de los eventos debe permitir al administrador configurar el tamaño del archivo para rotación de los archivos de registros de eventos ("logs")."

PREGUNTA 123.-

GARANTÍA TÉCNICA

Para soluciones que se ofrezcan con hardware dedicado o de propósito específico, **¿se podría omitir el cumplimiento del punto 5?**

RESPUESTA 123.

Referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 104, 5.2 INSTALACIÓN DEL HARDWARE, numeral 5, donde se establece que:

"Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como appliance virtual o como máquina virtual (VM) en su respectivo servidor de gestión tal como se indica en la tabla a continuación.

COMPONENTE DE SOFTWARE	***SERVIDOR FÍSICO***	***SITIO***
Gestor de firewall principal	*Servidor de gestión principal*	*CD Principal*
Componente de análisis de configuración y eventos principal	*Servidor de gestión principal*	*CD Principal*
Gestor de firewall alterno	*Servidor de gestión alterno*	*CD Alterno*
Componente de análisis de configuración y eventos alterno	*Servidor de gestión alterno*	*CD Alterno*

Tabla 6. *Correspondencia entre instancias virtuales y servidores físicos."*

En función de lo expuesto, los servidores de gestión principal y alterno no pueden ser appliance de propósito específico, por lo tanto, no se acoge su sugerencia con respecto al numeral 5 correspondiente a la sección 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE.

PREGUNTA 124.-

COMPONENTES DE SOFTWARE

COMPONENTES DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS

ANÁLISIS AUTOMÁTICO DE CONFIGURACIÓN

Para el **punto de cumplimiento 6**, se sugiere considerar como **opcionales** las especificaciones"*Número de reglas de tráfico de entrada*" y "*Número de reglas de tráfico de salida*", debido a que, así como se encuentran planteadas, lasconsideramos como restrictivas, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 124.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 136, ANÁLISIS AUTOMÁTICO DE CONFIGURACIÓN, numeral 6, donde se establece que:

"La función de análisis automático de configuración debe ser capaz de proveer al menos las siguientes estadísticas generales de reglas:

- *Número total de reglas;*
- *Número de reglas permitidas;*
- *Número de reglas denegadas;*
- *Número de reglas de tráfico de entrada;*
- *Número de reglas de tráfico de salida;*
- *Número de reglas inactivas;*
- *Número de reglas deshabilitadas;*
- *Número de reglas permitidas con origen y destino "ANY";*
- *Número de reglas permitidas con servicio "ANY"."*

PREGUNTA 125.-

ANÁLISIS AUTOMÁTICO DE CONFIGURACIÓN

Para el **punto de cumplimiento 8**, se sugiere considerar como **opcionales** las especificaciones "*Detalles de reglas excesivamente permisivas*", "*Amenazas de seguridad en servicios o aplicaciones*", "*Análisis de direcciones IP en listas negras*" y "*Análisis de puertos riesgosos*", debido aque, así como se encuentran planteadas, las consideramos como restrictivas, lo que impide lalibre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 125.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 137, numeral 8, donde se establece que:

"La función de análisis automático de configuración debe ser capaz de proveer la siguiente información en los reportes de análisis de reglas:

- *Irregularidades en reglas;*
- *Reglas sugeridas;*
- *Reglas no utilizadas;*
- *Afinamiento de política;*
- *Utilización de objetos;*

- *Objetos duplicados;*
- *Detalles de irregularidades;*
- *Sugerencias de reordenación de reglas;*
- *Detalles de reglas excesivamente permisivas;*
- *Amenazas de seguridad en servicios o aplicaciones;*
- *Análisis de direcciones IP en listas negras;*
- *Análisis de puertos riesgosos."*

PREGUNTA 126.-

ANÁLISIS AUTOMÁTICO DE CONFIGURACIÓN

Para el **punto de cumplimiento 9**, se sugiere considerar como **opcionales** las especificaciones"*Detalles de todas las reglas temporizadas*" y "*Lasreglas temporizadas próximas a activarse*", debido a que, así como se encuentran planteadas, las consideramos como restrictivas, lo que impide lalibre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 126.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 137, numeral 9, donde se establece que:

"La función de análisis automático de configuración debe ser capaz de proveer la siguiente información en los reportes de reglas temporizadas:

- Detalles de todas las reglas temporizadas;
- Las reglas temporizadas activas;
- Las reglas temporizadas próximas a activarse;
- Las reglas temporizadas expiradas;
- Las reglas temporizadas recurrentes."

PREGUNTA 127.-

ANÁLISIS AUTOMÁTICO DE CONFIGURACIÓN

Para el **punto de cumplimiento 11**, se sugiere considerar como **opcionales** las especificaciones"*Versión del cambio de configuración*", "*Número denuevas adiciones de reglas*", "*Número de nuevas modificaciones de reglas*", "*Número de nuevas*

eliminaciones de reglas" y "*Estadística histórica decambios*", debido a que, así como se encuentran planteadas, las consideramos como restrictivas, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidadessimilares.

RESPUESTA 127.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 137, numeral 11, donde se establece que:

"La función de análisis automático de configuración debe ser capaz de proveer la siguiente información en los reportes de análisis de cambio de reglas:

- *Fecha y hora del cambio de regla;*
- *Usuario que realizó el cambio;*
- *Dirección IP del usuario que realizó el cambio;*
- *Versión del cambio de configuración;*
- *Número de nuevas adiciones de reglas;*
- *Número de nuevas modificaciones de reglas;*
- *Número de nuevas eliminaciones de reglas;*
- *Estadística histórica de cambios."*

PREGUNTA 128.-

SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO

PROTECCIÓN DE CORREO ELECTRÓNICO

Se sugiere considerar como **opcional** el **punto de cumplimiento 23**, debido a que, así como se encuentra planteado, lo consideramos como restrictivo, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 128.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, PROTECCIÓN DE CORREO ELECTRÓNICO, numeral 23, donde se establece que:

"La solución debe detectar la manipulación sospechosa de buzones de usuarios y reglas de correo en Exchange Online, por parte de un perfil administrador, y debe tomar acciones de respuesta, tales como, la eliminación de la regla identificada como riesgosa."

PREGUNTA 129.-

SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO

PROTECCIÓN DE CORREO ELECTRÓNICO

Para el **punto de cumplimiento 24**, se sugiere considerar como **opcional** la especificación "*Si es un dominio recientemente registrado*", debido aque, así como se encuentra planteada, la consideramos como restrictiva, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 129.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 130.-

SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO

PROTECCIÓN DE PROCOLO SMTP

Para el **punto de cumplimiento 38**, se sugiere considerar como **opcionales** las especificaciones"*Cantidad de archivos contenidos en un solo archivo comprimido*", "*Metadatos de archivo adjuntos", "Número de restantes*", "*Tiempo de registro de dominio utilizado en los campos de oMFROM*" y "*Antigüedad del dominio utilizado en el campo desde y/o MFROM*", debido a que, así como se encuentran planteadas, las consideramos como restrictivas, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 130.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 131.-

Se sugiere considerar como **opcional** el **punto de cumplimiento 51**, debido a que, así como se encuentra planteado, lo consideramos como restrictivo, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 131.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 145, numeral 51, donde se establece que:

“La solución debe proporcionar una función de "vista previa segura" para que los administradores puedan ver información detallada de los mensajes en cuarentena y decidir las acciones necesarias.”

PREGUNTA 132.-

Se sugiere considerar como **opcionales** los **puntosde cumplimiento 54 y 55**, debido a que, así comose encuentran planteados, los consideramos comorestrictivos, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 132.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 133.-

Para el **punto de cumplimiento 60**, se sugiere cambiar la especificación “*Si al momento derealizar análisis de sandboxing de un hipervínculo el recurso web asociado no se encuentra disponible, la solución debe contar con la opciónde que el mensaje sea entregado no sin antes reescribir la dirección URL del hipervínculo de manera que, si el usuario hace clic, este se despliegue en un entorno controlado y aislado*” por“*Si al momento de realizar análisis de sandboxing de un hipervínculo el recurso web asociado no seencuentra disponible, la solución debe contar con la opción de que el mensaje sea entregado no sinantes reescribir la dirección URL del hipervínculo*”,debido a que, así como se encuentra planteada, la consideramos como restrictiva, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 133.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 134.-

Para el **punto de cumplimiento 63**, se sugiereconsiderar como **opcional** el tipo de archivo comprimido **TNEF**, debido a que, así como se encuentra planteado, lo consideramos como restrictivo, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 134.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 135.-

Para el **punto de cumplimiento 67**, se sugiere considerar como **opcional** la especificación "*delayed exploits*", debido a que, así como se encuentra planteada, la consideramos como restrictiva, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 135.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 146 ,CONTROL DE PHISHING, numeral 67, donde se establece que:

"La solución debe contar con protecciones especializadas para amenazas de tipo:

- "Email Account Compromise" (EAC),
- "Business Email Compromise" (BEC),
- "spear phishing",
- "whaling",
- "delayed exploits"."

PREGUNTA 136.-

Se sugiere considerar como **opcional** el **punto de cumplimiento 68**, debido a que, así como se encuentra planteado, lo consideramos como restrictivo, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 136.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 146 ,CONTROL DE PHISHING, numeral 68, donde se establece que:

"La solución debe ser capaz de analizar tanto el encabezado como el contenido del mensaje para detectar e identificar ataques de suplantación de dominio, suplantación de nombre para mostrar y estrategias de "typosquatting"."

PREGUNTA 137.-

Para el **punto de cumplimiento 70**, se sugierecambiar la especificación "*La solución debe detectar y bloquear los ataques de phishing quesuplantan las páginas de inicio de sesión*" por "*La solución debe detectar y bloquear los ataques dephishing*", debido a que, así como se encuentra planteada, la consideramos como restrictiva, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 137.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 146 ,CONTROL DE PHISHING, numeral 70, donde se establece que:

"La solución debe detectar y bloquear los ataques de phishing que suplantan las páginas de inicio de sesión."

PREGUNTA 138.-

Para el **punto de cumplimiento 74**, se sugierecambiar la especificación "*La solución debe tener la capacidad de reescribir la dirección URL del hipervínculo de manera que, si el usuario hace clic,este se despliegue en un entorno controlado y aislado*" por "*La solución debe tener la capacidad de reescribir la dirección URL del hipervínculo*",debido a que, así como se encuentra planteada, laconsideramos como restrictiva, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 138.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 139.-

Se sugiere considerar como **opcionales** los **puntosde cumplimiento 75 y 76**, debido a que, así comose encuentran planteados, los consideramos comorestrictivos, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 139.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 146, CONTROL DE PHISHING, numeral 75, donde se establece que:

"La solución debe ser capaz de retener la entrega de los mensajes de correo electrónico mientras se analizan todas las direcciones URL que contienen."

Asimismo, remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 146, CONTROL DE PHISHING, numeral 76, donde se establece que:

"La solución debe discriminar a los usuarios que estadísticamente han recibido más mensajes de phishing o con direcciones URL maliciosas para aplicarle protecciones de seguridad más rigurosas."

PREGUNTA 140.-

Se sugiere considerar como **opcional** el **punto de cumplimiento 85**, debido a que, así como se encuentra planteado, lo consideramos como restrictivo, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 140.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 147, ACCIONES DE REMEDIACIÓN, numeral 85, donde se establece que:

"Una vez recuperado el mensaje desde la bandeja del usuario, la solución debe permitir a los administradores analizarlo y eliminarlo o retenerlo en cuarentena."

PREGUNTA 141-

Para el **punto de cumplimiento 88**, se sugiere considerar como **opcionales** las especificaciones "*Correos electrónicos filtrados*", "*Credenciales de usuarios expuestas*", "*Accesos OAuth no seguros*", y "*Compartición riesgosa de archivos en las aplicaciones de Microsoft Office 365*", debido a que, así como se encuentran planteadas, las consideramos como restrictivas, lo que impide la libre participación de oferentes con soluciones de otras marcas con capacidades similares.

RESPUESTA 141.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 142.-

Estimada Entidad en la "Sección III. en la especificación "Cantidad Mínima" de "Técnico especialista de instalación y migración" Actualmente, se solicita una cantidad mínima de 3 especialistas. Solicitamos amablemente reconsiderar y modificar esta especificación, reduciendo la cantidad mínima a 2 especialistas, debido a que, de acuerdo a nuestro análisis, esta cantidad es suficiente para garantizar la correcta prestación del servicio técnico, optimizando los recursos sin comprometer la calidad del soporte.

RESPUESTA 142.

Al considerar los componentes que deben desplegarse en la etapa de instalación y migración, así como la necesidad de que el personal técnico cuente con las certificaciones adecuadas, se determinó que se requieren al menos tres especialistas para satisfacer las necesidades institucionales en esta fase. Por lo tanto, no se acepta su sugerencia.

PREGUNTA 143.-

Estimada Entidad en la “Sección III.se pide cambiar la especificación “Cantidad Mínima” de “Técnico especialista de soporte técnico” Actualmente, se solicita una cantidad mínima de 3 especialistas. Solicitamos amablemente reconsiderar y modificar esta especificación, reduciendo la cantidad mínima a 2 especialistas, debido a que, de acuerdo a nuestro análisis, esta cantidad es suficiente para garantizar la correcta prestación del servicio técnico, optimizando los recursos sin comprometer la calidad del soporte.

RESPUESTA 143.

Al evaluar los componentes que requieren soporte técnico y la necesidad de que el personal técnico cuente con las certificaciones correspondientes, se concluyó que se necesitan al menos tres especialistas para atender las necesidades institucionales en esta fase. Por lo tanto, no se acepta su sugerencia.

PREGUNTA 144.-

Estimada Entidad en la “Sección III. Criterios de Evaluación y Calificación” el Técnico especialista de instalación y migración y Técnico especialista de soporte técnico pueden ser la misma persona?

RESPUESTA 144.

Únicamente se puede aceptar que el mismo recurso que realice la instalación y migración también realice el trabajo de soporte técnico, conforme lo establecido en la Sección III. Criterios de Evaluación y Calificación, página 60, numeral 4 de La Solicitud de Ofertas.

"*Se puede aceptar que el* ***mismo recurso que realice la instalación y migración también realice el trabajo de soporte técnico***." (énfasis añadido).

PREGUNTA 145.-

Estimada Entidad en la "Sección III. Criterios de Evaluación y Calificación" el Técnico especialista de instalación y migración y el Instructor de transferencia de conocimiento pueden ser la misma persona?

RESPUESTA 145.

Únicamente se puede aceptar que el mismo recurso que realice la instalación y migración también realice el trabajo de soporte técnico, conforme lo establecido en la Sección III. Criterios de Evaluación y Calificación, página 60, numeral 4 de La Solicitud de Ofertas.

"*Se puede aceptar que el* ***mismo recurso que realice la instalación y migración también realice el trabajo de soporte técnico***." (énfasis añadido).

PREGUNTA 146.-

Estimada entidad en el literal 5.3. se dice textualmente "Si para la instalación y operación de los componentes de software se requiere software base como, por ejemplo, sistemas operativos, bases de datos, etcétera, el contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la instalación, activación y funcionamiento de dichos prerrequisitos siguiendo las mejores prácticas de fábrica, aplicando los estándares tecnológicos institucionales y cumpliendo con los requerimientos técnicos del SRI." ¿es de nuestro entendimiento que es responsabilidad del SRI proveer el licenciamiento de VMware para la virtualización de los componentes de software es nuestro entendimiento correcto?

RESPUESTA 146.

No es correcto su entendimiento, referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, GESTIÓN DE POLÍTICAS, página 132, numeral 24, se establece que:

*"La gestión de políticas **debe tener la capacidad de integrarse con el sistema vCenter** del SRI (véase **INFRAESTRUCTURA ACTUAL**) para importar objetos de manera que se puedan utilizar como origen o destino **para crear reglas de seguridad**." (énfasis añadido)*

Con base en lo anterior, la información sobre VMware, detallada en la tabla 3 "Detalle de las versiones de software de los componentes de la plataforma de virtualización del SRI", se presenta para cumplir con los requisitos técnicos relacionados a la integración con VCenter, como por ejemplo el requisito mencionado en el párrafo anterior.

Por lo que se solicita referirse a la necesidad institucional plasmada en la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 106, numeral 5.3 INSTALACIÓN DEL SOFTWARE.

PREGUNTA 147.-

Estimada entidad por favor aclarar que equipos dispone actualmente la entidad en cada clúster y en cada localización con el fin de conocer a detalle los servicios de MIGRACIÓN explicados en el literal "5.4.1.MIGRACION"

RESPUESTA 147.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 100, INFRAESTRUCTURA ACTUAL.

PREGUNTA 148-

Estimada entidad en el punto "5.4.1.1 SISTEMAS DE FIREWALLS" dice textualmente "La migración del sistema de firewalls debe incluir los siguientes aspectos particulares: 1.Las políticas del sistema de firewalls deberán ser transcritas desde el sistema actual al nuevo sistema." Por favor aclarar el número de reglas que serán migradas.

RESPUESTA 148.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, 4 INFRAESTRUCTURA ACTUAL, página 101, numeral 5, donde se detalla que:

*"**El sistema de firewalls del SRI cuenta con alrededor de 1.200 reglas de seguridad** distribuidas en 5 paquetes de políticas, uno por cada sistema (firewall) virtual." (énfasis añadido)*

Sin embargo, de acuerdo con la nota que se encuentra en la misma sección, página 103, en la que se establece que:

*"**NOTA**: Toda la información de este apartado ha sido levantada a la fecha del presente documento. Esta puede variar en función de la operación y las necesidades institucionales y de las nuevas liberaciones de los fabricantes. **Es responsabilidad del contratista hacer las validaciones correspondientes oportunamente**." (énfasis añadido)*

PREGUNTA 149.-

Estimada Entidad en la "Sección ACUERDO DE NIVEL DE SERVICIO" en el literal 4 se establece para mantenimiento correctivo en el tiempo destinado para prioridad 1 mantenimiento correctivo 1 hora solicitamos amablemente reconsiderar y modificar esta especificación a 2 horas, esta solicitud se basa en nuestra experiencia operativa, donde generalmente se requiere una primera hora para realizar un diagnóstico adecuado antes de proceder con las acciones correctivas.

RESPUESTA 149.

No se acoge su solicitud, referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 115, 5.5 ACUERDO DE NIVEL DE SERVICIO, numeral 1, en el que se establece que:

"El tiempo de respuesta se define como el lapso entre el momento en que el SRI hace la solicitud de servicio y el momento en que inicia el análisis técnico por parte del ingeniero especialista designado a dicho requerimiento. Aplica a los servicios de mantenimiento correctivo y de asistencia técnica."

PREGUNTA 150.-

Estimada Entidad en la "Sección ACUERDO DE NIVEL DE SERVICIO" en el literal 4 se establece para mantenimiento correctivo en el tiempo destinado para prioridad 2 mantenimiento correctivo 3 hora solicitamos amablemente reconsiderar y modificar esta especificación a 4 horas, esta solicitud se basa en nuestra experiencia operativa, donde

generalmente se requiere una primera hora para realizar un diagnóstico adecuado antes de proceder con las acciones correctivas.

RESPUESTA 150.

No se acoge su solicitud, referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 115, 5.5 ACUERDO DE NIVEL DE SERVICIO, numeral 1, en el que se establece que:

"El tiempo de respuesta se define como el lapso entre el momento en que el SRI hace la solicitud de servicio y el momento en que inicia el análisis técnico por parte del ingeniero especialista designado a dicho requerimiento. Aplica a los servicios de mantenimiento correctivo y de asistencia técnica."

PREGUNTA 151.-

De acuerdo con el item *"La función de respaldo automático de configuración debe contar con la capacidad y el licenciamiento suficiente para respaldar la configuración de: El sistema de Firewalls ofertado; El sistema de Proxy Web del SRI(Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG).",* Solicitamos a la entidad eliminar la inclusión del componente del sistema Proxy del fabricante Broadcom, teniendo en cuenta que dentro de nuestra solución firewall, la funcionalidad de filtrado web, ya viene incluida contando con un sistema para el control de navegación y de paquetes.

RESPUESTA 151.

No se acoge su solicitud, debido a que el sistema de Proxy Web que actualmente dispone el SRI en producción es Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG.

PREGUNTA 152.-

De acuerdo con el ítem "La función de respaldo automático de logs debe contar con la capacidad y el licenciamiento suficiente para respaldar los registros de eventos ("logs") de: El sistema de Firewalls ofertado; El servicio SaaS de protección de correo electrónico ofertado; El sistema de Proxy Web del SRI (Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG).", Solicitamos a la entidad eliminar la inclusión del componente del sistema Proxy del fabricante Broadcom, teniendo en cuenta que el control de la navegación estará asumido por los firewall ofertados y que únicamente desde estos se generarían logs relacionados a la navegación web de los usuarios.

RESPUESTA 152.

No se acoge su solicitud, debido a que el sistema de Proxy Web que actualmente dispone el SRI en producción es Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG.

PREGUNTA 153.-

De acuerdo con el ítem "La función de recolección y correlación de logs debe contar con la capacidad y el licenciamiento suficiente para recolectar y correlacionar los registros de eventos ("logs") de: El sistema de Firewalls ofertado; El servicio SaaS de protección de correo electrónico ofertado; El sistema de Proxy Web del SRI (Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG).", Solicitamos a la entidad eliminar el requerimiento del componente del sistema Proxy fabricante Broadcom, teniendo en cuenta que el control de la navegación estará asumido por los firewall ofertados y que únicamente desde estos se generarían eventos relacionados a la navegación web de los usuarios.

RESPUESTA 153.

No se acoge su solicitud, debido a que el sistema de Proxy Web que actualmente dispone el SRI en producción es Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG.

PREGUNTA 154.-

Estimada entidad en el apartado PROTECCIÓN DE CORREO ELECTRÓNICO, solicitan: "***La solución debe detectar la manipulación sospechosa de buzones de usuarios y reglas de correo en Exchange Online, por parte de un perfil administrador, y debe tomar acciones de respuesta, tales como, la eliminación de la regla identificada como riesgosa***." solicitamos que se permita la inspección de actividad sospechosa sobre el tráfico de correo de los usuarios que pasa por la solución de correo electrónico, y donde la respuesta sea el bloqueo del tráfico malicioso y la puesta en cuarentena de la dirección IP y dirección de correo del remitente. Confirmar?

RESPUESTA 154.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, PROTECCIÓN DE CORREO ELECTRÓNICO, numeral 23, donde se establece que:

"La solución debe detectar la manipulación sospechosa de buzones de usuarios y reglas de correo en Exchange Online, por parte de un perfil administrador, y debe tomar acciones de respuesta, tales como, la eliminación de la regla identificada como riesgosa."

PREGUNTA 155.-

Estimada entidad, en la sección 6. BIENES REQUERIDOS, item 6.1.1 CAPACIDADDEL HARDWARE en A.CONDICIONES GENERALES, solicitan: La infraestructura del sistema de Firewalls de Nueva Generación (NGFW) debe estar constituida por hardware para centros de datos. Entendemos que el hardware ofertado debe ser de propósito específico para la solución ofertada. Por favor confirmar

RESPUESTA 155.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 118, 6.1.1 CAPACIDAD DEL HARDWARE, A. CONDICIONES GENERALES, donde se establece:

"La infraestructura del sistema de Firewalls de Nueva Generación (NGFW) debe estar ***constituida por hardware para centros de datos****." (énfasis añadido)*

Se aclara que la frase "constituida por hardware para centro de datos" significa que esté diseñado específicamente para funcionar en entornos de alta capacidad y rendimiento, como los centros de datos.

PREGUNTA 156.-

Estimada entidad, se solicita de la manera más comedida se permita en esta etapade la licitación realizar una inspección en sitio para revisar la infraestructura a ser reemplazada. Por favor mencionar el día, la persona y la hora de la inspección.

RESPUESTA 156.

Conforme a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 150, 5. INSPECCIONES Y PRUEBAS, no aplica realizar inspecciones y pruebas, por lo que no se acoge su solicitud.

PREGUNTA 157.-

Estimada entidad al momento de realizar la implementación de la solución se necesita el personal a cargo de la plataforma existente dentro de la institución, como apoyo para el proceso de migración, optimización y reconfiguración de la plataforma a ser instalada. Por favor mencionar que se contará con el recurso solicitado durante este proceso

RESPUESTA 157.

En la fase de implementación de la solución, el Administrador de Contrato gestionará los recursos técnicos del SRI con los que se trabajará en esta fase en conjunto con el contratista.

PREGUNTA 158.-

Estimada Entidad para la sección “CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO”entendemos que es importante incluir **el soporte a reglas basadas en servicioscloud** populares de Internet, en donde se tiene una base de datos que se actualiza dinámicamente. Esta base de datos puede usarse también en enrutamiento y balanceo de enlaces o SD-WAN. **Y el enrutamiento Inteligente para las diferentesaplicaciones**, la solución debe estar en capacidad de enrutar el tráfico teniendo en cuenta requerimientos mínimos como Jitter (variación del retardo), retardo y pérdida de paquetes. Esto con el fin de mejorar la experiencia de los usuarios internos respecto al uso de aplicaciones tipo SAAS (Office 365, teams, Zoom, etc) en un escenario donde se tiene conexión a internet dual y que se puede desplegarsin licencias y costos adicionales para la entidad contratante.

RESPUESTA 158.

Se solicita regirse a la necesidad institucional plasmada en la Solicitud de Oferta (SDO).

PREGUNTA 159.-

Estimada entidad, Solicitamos a la entidad aclarar el tiempo de retención de los log

para los firewall de siguiente generación.

RESPUESTA 159.

El tiempo de retención de registros de eventos (“logs”) dependerá del espacio de almacenamiento disponible, en función de lo que se establece en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 107, numeral 15:

“La distribución de los recursos de los servidores físicos, esto es, de la capacidad de procesamiento, de memoria y de espacio de almacenamiento, entre todas las instancias virtuales deberá ser aprobada por el personal técnico del SRI en función de los requerimientos operativos de los componentes de software, los estándares tecnológicos institucionales y los requerimientos técnicos del SRI.”

En función de lo expuesto considerar lo siguiente:

SISTEMA DE FIREWALLS:

En el caso específico del sistema de firewalls, además de lo expuesto, el tiempo de retención del **gestor de eventos** dependerá de la densidad de logs que tenga la arquitectura de la solución ofertada.

SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO:

Por favor referirse a:

- La sección VI. Requisitos de los Bienes y Servicios Conexos, B. SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO, página 148, numeral 97, en la que se establece lo siguiente:
  *“La retención de los registros de eventos (“logs”) **debe ser de no menos de 14 días**.” (énfasis añadido).*
- La sección VI. Requisitos de los Bienes y Servicios Conexos, página 48, PROTECCIÓN DE DATOS, numeral 99, en el que se estable lo siguiente:
  “El servicio SaaS deberá proveer las facilidades necesarias para descargar o reenviar la información generada, incluyendo los registros de eventos (“logs”).”

COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS:

Adicionalmente, se debe considerar que en este componente se van a realizar tanto la recolección y correlación de eventos como el respaldo automático de eventos, lo que también debe ser considerado en la retención.

En la sección VI. Requisitos de los Bienes y Servicios Conexos, RECOLECCIÓN Y CORRELACIÓN DE EVENTOS, página 138, numeral 14, se establece que:

> *"La función de recolección y correlación de logs debe contar con la capacidad y el licenciamiento suficiente para recolectar y correlacionar los registros de eventos ("logs") de:*
>
> - ***El sistema de Firewalls ofertado;***
> - ***El servicio SaaS de protección de correo electrónico ofertado****;*
> - *El sistema de Proxy Web del SRI (Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG)." (énfasis añadido)*

Finalmente, en base a lo expuesto, se aclara que la retención de los tres componentes citados (GESTORES DEL SISTEMA DE FIREWALL, COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS, SERVICIO SAAS DE PROTECCIÓN DE CORREO ELECTRÓNICO) estará determinada por la arquitectura de las soluciones ofertadas y la distribución del espacio de almacenamiento disponible en los SERVIDORES DE GESTIÓN (físicos).

PREGUNTA 160.-

Estimada entidad, entendemos que para el presente proceso no existe la posibilidad de entregar una oferta alternativa, favor confirmar

RESPUESTA 160.

Conforme la IAO 14.1 de los DDL y en concordancia con la sección III. Criterios de Evaluación y Calificación, página 54, numeral 3.3. Ofertas Alternativas (IAO 14.1), no aplican las ofertas alternativas para el presente proceso.

PREGUNTA 161.-

Estimada entidad, solicitan en el item preparación de ofertas lo siguiente: IAO 11.1 El idioma de la Oferta es: Español. Al elaborar las especiaciones técnicas hay datasheets del fabricante que vienen en idioma universal inglés y es ingles técnico, por lo que se solicita que se acepte entregar documentos del fabricante en idioma inglés.

RESPUESTA 161.

Conforme establece la IAO 11 el idioma de entrega de la oferta debe ser en español. Podrá presentarse en la oferta documentos escritos en otro idioma, siempre que vayan acompañados de una traducción fidedigna de las secciones pertinentes.

PREGUNTA 162.-

Estimada entidad por favor confirma si la oferta debe ser entregada DDP con todos los gastos de importación e impuestos pagados en las instalaciones del cliente, o si se requiere que se entregue CIP antes de aduana y la institución se encarga de nacionalizar los equipos y nosotros nos encargamos de llevar los equipos desde aduana hacia la instalación del cliente. Favor confirmar

RESPUESTA 162.

Conforme a la IAO 15.7 de la sección II. Datos de Licitación (DDL), página 45, la evaluación de las ofertas se efectuará en CIP y para la adjudicación en DDP.

En consecuencia, en el caso que los bienes sean fabricados fuera del país del comprador y deban ser importados, se deberá llenar los datos solicitados dentro de los formularios de la sección V, página 74 y 75; y, en el caso que los bienes fabricados fuera del país hayan sido previamente importados se deberá llenar los datos solicitados dentro del formulario de la sección V, página 76.

PREGUNTA 163.-

Estimada entidad en el documento solicitud de oferta en el item IAO 19.3 (a) solicitan: El factor es de hasta 1.15% anual acumulado para las Ofertas en moneda nacional, no se ha considerado la presentación de las ofertas en otro tipo de moneda. Para definir el factor de hasta 1.15% será sobre la base del análisis que se constituya en ese momento. Por favor mencionar y detallar a que se refiere este punto.

RESPUESTA 163.

Favor remitirse a las instrucciones a los oferentes (IAO) 19.3 (a) que señala: *"19.3 Si la adjudicación se demora más de cincuenta y seis (56) días a partir del vencimiento del*

Período de Validez inicial de la Oferta, el precio del Contrato se determinará de la manera siguiente:

(a) *en el caso de los Contratos de precio fijo, el precio contractual será el de la Oferta, ajustado por un factor especificado en los DDL;"*

En este sentido, el factor que la entidad contratante a definido en el caso que ocurrirá lo determinado en la IAO 19.3 (a) es de hasta el 1.15% sobre el análisis que se constituya en el momento que se requiera ejecutar dicha condición.

PREGUNTA 164.-

Estimada entidad en el documento solicitud de oferta en el item **IAO 17.4** solicitan: Período de tiempo estimado de funcionamiento de los Bienes (para efectos de repuestos): 5 años, entendemos que esto aplica siempre y cuando el SRI extienda el soporte del fabricante, ya que actualmente el requerimiento es de 3 años de soporte del fabricante desde la firma del acta entrega recepción y no por 5 años. Por favor confirmar

RESPUESTA 164.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 134, 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE, numeral 3, donde se establece que:

"Todos los equipos que conforman el componente de hardware del objeto de contrato deberán ser nuevos y se deberá garantizar que éstos no entren en EOST ("End-of-Support") ni en EOL ("End-of-Life") durante los 5 años posteriores a la fecha de suscripción del contrato."

PREGUNTA 165.-

Estimada entidad en el documento solicitud de oferta en el ítem **IAO 21.1** solicitan: La documentación de la oferta serán copias simples, sin embargo, para la suscripción del contrato se requerirá los documentos que sean otorgados en territorio extranjero, debidamente legalizados ante agente diplomático o cónsul de Ecuador, acreditado en su territorio apostillados. Entendemos que esto hace referencia a certificados de los fabricantes que son emitidos en el extranjero, tanto para el personal técnico como para el oferente.

RESPUESTA 165.

Es correcto su entendimiento. Los documentos legalizados deberán ser entregados únicamente por el oferente que sea adjudicado.

PREGUNTA 166.-

Estimada entidad en el documento solicitud de oferta en el item **IAO 21.1** solicitan: Documentación técnica en formato digital (formato pdf, no imágenes) como: fichas técnicas, hojas de especificación, catálogos, manuales o similares, de los productos y servicios ofertados, deberá cumplir las siguientes características; Permitir la búsqueda de texto, Resaltar las secciones que permitan verificar el cumplimiento de las especificaciones técnicas. Estimada entidad, se entiende que en el CD donde se entregará una copia escaneada de la oferta, adicional se debe subir los datasheet en formato PDF donde se pueda realizar la búsqueda de texto y resaltar las secciones que permitan verificar el cumplimiento de las especificaciones técnicas. Por favor confirmar.

RESPUESTA 166.

Es correcto su entendimiento.

PREGUNTA 167.-

Estimada entidad, en el ítem Calificación del Oferente (IAO 39) solicitan (a) Si el Oferente es fabricante: (i) Capacidad financiera:…. Al ser un canal que es distribuidor autorizado y no es el fabricante, entendemos que no hay que cumplir con la capacidad financiera solicitada, favor confirmar

RESPUESTA 167.-

Remitirse a la sección III. Criterios de Evaluación y Calificación, página 61, literal b que menciona:

"(b) Si el Oferente no es fabricante:

Si el Oferente no es fabricante, pero está ofertando los Bienes en nombre del fabricante de acuerdo con el Formulario de Autorización del Fabricante (Sección V, "Formularios de la Oferta"), el oferente deberá demostrar las calificaciones (i), (ii) y (iii) referidas en el literal a"

PREGUNTA 168.-

Estimada entidad en el item Calificación del Oferente (IAO 39) solicitan: 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. Por favor detallar a que se refiere con integrante líder.

RESPUESTA 168.

El integrante líder es el miembro de la Asociación en participación, consorcio o asociación (APCA), que deberá tener al menos el 50% de participación en el APCA. Esto deberá constar en el acuerdo de APCA de conformidad a la IAO 12.2

PREGUNTA 169.-

Estimada entidad en el ítem Calificación del Oferente (IAO 39) solicitan en Experiencia y capacidad técnica, Experiencia requerida Comercialización de bienes, o comercialización de garantía técnica, o comercialización de licenciamiento, o comercialización de servicios, tales como, implementación, o configuración, o migración, o mantenimiento, o soporte técnico especializado de soluciones de Firewall de Nueva Generación (NGFW). Solicitamos de la manera más comedida, se acepte Experiencia requerida Comercialización de bienes, o comercialización de garantía técnica, o comercialización de licenciamiento, o comercialización de servicios, tales como, implementación, o configuración, o migración, o mantenimiento, o soporte técnico especializado de soluciones de Firewall de Nueva Generación (NGFW) o soluciones tecnológicas de datacenter, permitiendo la libre participación a más canales que tenemos experiencia en el mercado. Por favor mencionar si se acepta nuestra solicitud

RESPUESTA 169.

No se acoge su solicitud, por favor remitirse a la experiencia requerida en la sección III. Criterios de Evaluación y Calificación, página 56.

PREGUNTA 170.-

Estimada entidad en el ítem Capacidad Técnica en el PERSONAL TÉCNICO MÍNIMOsolicitamos que se permita que un técnico pueda cumplir más de 2 roles. Por favorconfirmar.

RESPUESTA 170.

Únicamente se puede aceptar que el mismo recurso que realice la instalación y migración también realice el trabajo de soporte técnico, conforme lo establecido en la Sección III. Criterios de Evaluación y Calificación, página 60, numeral 4 de La Solicitud de Ofertas.

PREGUNTA 171.-

Estimada entidad en la página 61 en el item (iii) Prueba documental, solicitan: El Oferente deberá proporcionar prueba documental que demuestre que los Bienes cumplen los siguientes requisitos en materia de experiencia: Certificados de experiencia o actas entrega recepción definitivas que acrediten fehacientemente la experiencia en Comercialización de bienes, o comercialización de garantía técnica, o comercialización de licenciamiento, o comercialización de servicios, tales como, implementación, o configuración, o migración, o mantenimiento, o soporte técnico especializado de soluciones de Firewall de Nueva Generación (NGFW). Solicitamos de la manera más comedida se acepte presentar Certificados de experiencia o actas entrega recepción definitivas que acrediten fehacientemente la experiencia en Comercialización de bienes, o comercialización de garantía técnica, ocomercialización de licenciamiento, o comercialización de servicios, tales como, implementación, o configuración, o migración, o mantenimiento, o soporte técnico especializado de soluciones de Firewall de Nueva Generación (NGFW) o solucionestecnológicas de datacenter, permitiendo la libre participación a más canales conexperiencia en el mercado.

RESPUESTA 171.

No se acoge su solicitud, por favor remitirse a la experiencia requerida en la sección III. Criterios de Evaluación y Calificación, página 56.

PREGUNTA 172.-

Estimada entidad en la página 61, mencionan: (b) Si el Oferente no es fabricante: Si el Oferente no es fabricante, pero está ofertando los Bienes en nombre del fabricante de acuerdo con el Formulario de Autorización del Fabricante (Sección V, “Formularios de la Oferta”), el oferente deberá demostrar las calificaciones (i), (ii) y (iii) referidas en el literal a, por favor detallar lo que se debe presentar de acuerdo a las calificaciones (i), (ii) y (iii) referidas en el literal a

RESPUESTA 172.

Referirse a la sección III. Criterios de Evaluación y Calificación, página 55, numeral V, literal a.

PREGUNTA 173.-

Estimada entidad, Para la transferencia de conocimiento, entendemos que el instructor debe ser certificado por el fabricante como instructor certificado en los productos a ofertarse; y será esta persona la que realice la transferencia mediante cursos y material oficial. Por favor confirmar

RESPUESTA 173.

No es correcto su entendimiento, referirse a la sección Sección III. Criterios de Evaluación y Calificación, página 59, Rol "Instructor de transferencia de conocimiento", Estudios o certificado requerido, donde se establece que:

"Certificación Técnica vigente nivel profesional, avanzado o equivalente ***emitida por el fabricante del sistema de Firewalls y del servicio SaaS de protección de correo electrónico ofertados****."*

Adicional, en la misma sección, Rol "Instructor de transferencia de conocimiento", Asignaciones Específicas Mínimas, se establece que:

- *"**Impartir la transferencia de conocimiento.***
- *Diligenciar todos los insumos necesarios para la transferencia de conocimiento.*
- *Elaborar la documentación de respaldo de la ejecución de la transferencia de conocimiento." (énfasis añadido)*

PREGUNTA 174.-

Estimada entidad, al presentar experiencia de haber participado en un consorcio con la experiencia solicitada, entendemos que el monto de la experiencia vale en su totalidad? Por favor confirmar.

RESPUESTA 174.

Solo será válido el porcentaje del monto de la participación que haya tenido en el consorcio.

PREGUNTA 175.-

Estimada Entidad, en **18.2 (a)**, Prueba documental solicitan: Se requiere la

autorización del fabricante. Entendemos que se refiere a la certificación del fabricante donde menciona que el canal es distribuidor autorizado para el Ecuador de la solución ofertada. Por favor confirmar

RESPUESTA 175.

No es correcto su entendimiento, el fabricante deberá suscribir el formulario "Autorización del fabricante" establecido en la sección V. Formularios de la Oferta, página 85. (Dicho formulario no podrá ser modificado en su contenido).

Adicionalmente, el fabricante deberá emitir un certificado en el cual establezca que el oferente es distribuidor autorizado del fabricante en los siguientes componentes:

- Sistema de Firewall de Nueva Generación,
- Servicio SaaS de protección de correo electrónico,
- Componente de análisis de configuración y eventos,
- Servidores de gestión principal y alterno.

Dichos certificados deberán ser emitidos durante el año en curso de la presentación de la oferta.

PREGUNTA 176.-

Estimada entidad, en la formación del personal técnico solicitan en titulación académica Ingeniero. Solicitamos que también se acepte tecnólogo ya que también es registrado como título de tercer nivel en Ecuador. Favor confirmar

RESPUESTA 176.

Es correcta su interpretación.

PREGUNTA 177.-

Estimada entidad con respecto al formulario autorización del fabricante, es posible colocar el contenido de la carta en el formato del fabricante ya que ellos cuentan con una estructura aprobada por su equipo legal y por políticas internas globales, no emiten certificados en formatos que no sean los que ellos manejan. Favor confirmar

RESPUESTA 177.

Conforme lo determinado en la Solicitud de Ofertas (SDO), Sección V. Formularios de la Oferta, pág. 85, el Formulario "Autorización del Fabricante", deberá estar escrito en papel membretado del fabricante, suscrito por una persona debidamente autorizada para firmar documentos que comprometan jurídicamente al fabricante; y, el fabricante deberá declarar que sus compromisos de prácticas de responsabilidad ambiental y social – ASSS, están alineadas al cumplimiento de las políticas ambientales y sociales, determinadas por el Banco Interamericano de Desarrollo.

PREGUNTA 178.-

Estimada entidad, por favor mencionar cuales son los documentos financieros que debe entregar el oferente y los parámetros que deba cumplir financieramente el oferente

RESPUESTA 178.

Referirse a la sección III. Criterios de Evaluación y Calificación, página 55, numeral V, literal a, que establece lo siguiente:

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

i. En relación a los últimos 5 años con cierre fiscal, se deberá entregar copia simple de los estados financieros, declaraciones de impuestos anuales, facturas por la provisión de bienes y/o servicios de seguridad informática. 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."

PREGUNTA 179.-

En la sección Instalación del Hardware, el ítem 9 menciona sobre transceivers, por favor mencionar la cantidad requerida de tranceivers según el tipo de conexión.?

RESPUESTA 179.

En la sección VI. Requisitos de los Bienes y Servicios Conexos, página 105, en los numerales del 9 al 12 se establece que:

"El contratista debe proveer, como parte de la instalación de cada equipo entregado, los transceptores ("transceivers") **que sean necesarios** para su conexión con la infraestructura de red del SRI, en los centros de datos principal y alterno, utilizando los modelos que se indican en la tabla a continuación.

MEDIO	***TIPO DE CONEXIÓN***	***FABRICANTE***	***MODELO***
Óptico	*40Gbps BASE-SR QSFP+ LC*	*Cisco*	*QSFP-40/100-SRBD*
Óptico	*25Gbps BASE-SR SFP+ LC*	*Cisco*	*SFP-25G-SR-S*
Óptico	*10Gbps BASE-SR SFP+ LC*	*Cisco*	*SFP-10G-SR*
Óptico	*1Gbps BASE-SX SFP LC*	*Cisco*	*GLC-SX-MMD*

Tabla 7. *Modelos de transceptores ("transceivers") soportados por el switch de core institucional." (énfasis añadido)*

En virtud de lo expuesto, el contratista debe proveer e instalar la cantidad que sea necesaria de los transceivers de los componentes de hardware que conforman el objeto de esta contratación (solución ofertada) y los transceivers del switch de core institucional (tabla 7), para la correcta operación del sistema.

PREGUNTA 180.-

En la sección Servicios Conexos Requeridos, 5.4.1. Migración, el ítem 8.e se menciona que se debe realizar todas las configuraciones de integración con los sistemas centralizados, por favor, mencionar todos los sistemas que se requiere integrar.?

RESPUESTA 180.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 108, numeral 8.e, donde se establece que:

"Realizar todas las configuraciones de integración con los sistemas centralizados ***(ej. Active Directory, vCenter, etc.)*** *necesarias para la operación de cada componente;" (énfasis añadido)*

Referirse además a la misma sección, página 110, numeral 4 donde se establece que*:*
"Se deben utilizar las integraciones establecidas en la etapa de preparación, ***por ejemplo, con Active Directory, con vCenter, con ACI****, para reemplazar objetos de red de las reglas existentes con los obtenidos en estas integraciones" (énfasis añadido)*

Adicional, se deberán incluir todas las integraciones que el fabricante de la solución ofertada requiera para el correcto funcionamiento de esta.

PREGUNTA 181.-

En la sección de Componente de Software, 6.2.1 Productos Esperados, se menciona que el componente de análisis de configuración y eventos debe contar con funcionalidad de análisis automática de configuración, respaldo automático, recolección, análisis y correlación de eventos, supervisión, es de interés para el cliente se pueda manejar con distintas soluciones tecnológicas que se dediquen a las funcionalidades requeridas, ya que se indica que puede pertenecer a diferentes fabricantes.?

RESPUESTA 181.

Referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, 6.2 COMPONENTE DE SOFTWARE, 6.2.1 PRODUCTOS ESPERADOS, página 136, A COMPONENTES DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS, numeral 1, donde se establece:

"Las funciones y módulos que comprenden el COMPONENTE DE ANÁLISIS DE CONFIGURACIÓN Y EVENTOS pueden pertenecer a diferentes fabricantes."

En función de lo expuesto, las funciones detalladas en el numeral 3 pueden pertenecer a diferentes fabricantes.

PREGUNTA 182-

Se menciona del sistema de Proxy Web del SRI, por favor nos puedan compartir la función que tiene este sistema y la versión.

RESPUESTA 182.

La función del Proxy Web del SRI es gestionar la navegación de aproximadamente 3500 usuarios, identificando el tráfico por usuario, cuenta con un componente Web Proxy Caché para mejorar el desempeño de la navegación, permite la generación de políticas de navegación alineadas con las normas de seguridad del SRI y restricción de acceso a sitios web que representen riesgos de seguridad.

La versión del sistema de Proxy Web del SRI (Fabricante: Broadcom/Symantec/BlueCoat; Modelo: ProxySG) es: SGOS 7.4.5.1 SWG Edition.

PREGUNTA 183.-

Se menciona del sistema de Proxy Web del SRI, por favor nos confirme que la herramienta puede exportar sus eventos en formato syslog/CEF.?

RESPUESTA 183.

Se confirma que los eventos del sistema de Proxy Web del SRI se pueden exportar en formato syslog.

PREGUNTA 184.-

Se menciona que se requiere el respaldo automático de las configuraciones y eventos del sistema de Proxy Web del SRI, por favor comentar el tamaño de configuraciones y volumen de logs y eventos aproximado se estima se realizará el respaldo.?

RESPUESTA 184.

El sistema Proxy Web del SRI genera un volumen de logs y eventos de aproximadamente 600MB (comprimidos) al día.

PREGUNTA 185.-

En la sección de C. Servicio SaaS de Protección de Correo Electrónico, para el ítem 22 La solución debe tener soporte multilingüe para el análisis del contenido de los mensajes de correo electrónico, incluyendo al menos el Inglés, el Español y el Francés, confirmar que es de interés para SRI que la herramienta de seguridad haga un análisis de contenido basado en distintos criterios de escaneo independientemente del idioma Inglés, Español y Francés, ya que se pueden crear Keywords y Regular Expressions.?

RESPUESTA 185.

Regirse a la necesidad institucional plasmada en el numeral 22, de la sección VI. Requisitos de los Bienes y Servicios Conexos, página 142, donde se establece que:

"La solución debe tener soporte multilingüe para el análisis del contenido de los mensajes de correo electrónico, incluyendo al menos el Inglés, el Español y el Francés."

PREGUNTA 186.-

En la sección de C. Servicio SaaS de Protección de Correo Electrónico, para el ítem 24 La solución debe permitir la adición de etiquetas en el correo electrónico entrante que permitan, al menos, informar al destinatario, confirmar que es de interés para SRI el cumplimiento de al menos dos de los criterios mencionados.?

RESPUESTA 186.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 187.-

En la sección de C. Servicio SaaS de Protección de Correo Electrónico, para el ítem 49 La cuarentena debe almacenar los mensajes en carpetas diferenciadas de acuerdo con el tipo motor de detección, confirmar que es de interés para SRI que la herramienta realice la cuarentena de acuerdo con los motivos generados por el motor de detección independientemente que para ello se genere varias carpetas considerando que la función principal es el análisis generado por la herramienta.?

RESPUESTA 187.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 188.-

En la sección de C. Servicio SaaS de Protección de Correo Electrónico, para el ítem 51 La solución debe proporcionar una función de "vista previa segura" para que los administradores puedan ver información detallada de los mensajes en cuarentena y decidir las acciones necesarias, confirmar que es de interés para SRI que la solución permita descargar el correo en ZIP con contraseña como "Vista Segura".?

RESPUESTA 188.

Favor remitirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 145, numeral 51, donde se establece que:

"La solución debe proporcionar una función de "vista previa segura" para que los administradores puedan ver información detallada de los mensajes en cuarentena y decidir las acciones necesarias."

PREGUNTA 189.-

En la sección de C. Servicio SaaS de Protección de Correo Electrónico, para el ítem 55 La solución debe contar con inteligencia que permita intentar acceder a un archivo protegido con contraseña utilizando información contextual del mensaje utilizado para su envío, confirmar que es interés para SRI que la solución cuente con un diccionario de palabras para así abrir archivos protegidos con contraseña.?

RESPUESTA 189.

Referirse al Boletín de Enmiendas Nro. 2

PREGUNTA 190.-

En la sección de C. Servicio SaaS de Protección de Correo Electrónico, para el ítem 95 La solución debe emitir alertas en base a condiciones asociadas a las políticas, las carpetas de cuarentena y los umbrales de cola, por favor mencionar a que se refiere con umbrales de cola.?

RESPUESTA 190.

Esto se refiere a la capacidad de la solución para monitorear la cola de mensajes (los correos que están en espera de ser procesados). Si la cola alcanza un cierto umbral (por ejemplo, un número elevado de mensajes pendientes), la solución debe generar una alerta para que los administradores puedan investigar y resolver el problema.

PREGUNTA 191.-

La Garantía de Fiel cumplimiento por qué porcentaje del valor contrato se deberá entregar en caso de ser adjudicado?

RESPUESTA 191.

Remitirse a la sección VIII. Condiciones Especiales de Contrato (CEC), página 175, CGC 19.1

PREGUNTA 192.-

La Garantía de Anticipo por que tiempo deberá estar vigente y por qué porcentaje se debe entregar en caso de ser adjud

RESPUESTA 192.

Conforme el llamado a licitación página 199, la garantía por anticipo no aplica.

PREGUNTA 193.-

En la página 118, literal B numeral 6 se indica acerca de la capacidad de procesamiento de tráfico SSL/TLS:

- Cada gateway físico (nodo) debe tener la capacidad de realizar la inspección SSL/TLS de un volumen de tráfico (“throughput”) no menor a **1532 Mbps**, para las funciones de seguridad que se detallan.

La capacidad en el caso de nuestros gateways ha sido medida con ECDHE-RSA-AES256-GCM-SHA384, ECDSA-AES256-GCM-SHA384, asumimos que esto será aceptable para el SRI; favor confirmar

RESPUESTA 193.

No es correcto su entendimiento, la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 119, numeral 6, establece que:

"Capacidad de procesamiento de tráfico SSL/TLS:

- *Cada gateway físico (nodo) debe tener la capacidad de realizar la inspección SSL/TLS de un volumen de tráfico ("throughput") no menor a **1532 Mbps**, para las funciones de seguridad que se detallan:*
  - *Protección IPS de los servidores del SRI publicados en internet y alojados en la DMZ del sistema de Firewall.*

- *Cada gateway físico (nodo) debe tener la capacidad de realizar la inspección SSL/TLS de un volumen de tráfico ("throughput") no menor a **492 Mbps**, para las funciones de seguridad que se detallan:*
  - *Control de navegación,*
  - *Protección IPS de los clientes internos del SRI,*
  - *Protección antimalware,*
  - *Protección contra amenazas no basada en firmas.*

***NOTA:** Las condiciones en las que se debe cumplir con este requerimiento se establecen en el apartado **INSPECCIÓN SSL/TLS** del componente **A. CLÚSTER DE FIREWALL PRINCIPAL Y ALTERNO** en la sección **4.1.2. FUNCIONALIDAD DEL HARDWARE**."*

PREGUNTA 194.-

En la página 126, sección PROTECCIÓN CONTRA AMENAZAS NO BASADA EN FIRMAS, consta en el numeral 80: La función de protección contra amenazas no basadas en firmas debe emplear mecanismo basados en aprendizaje automático ("machine learning") para analizar imágenes en páginas web y determinar si están imitando marcas conocidas como parte de una campaña phishing.

Considerando que si aplicamos controles avanzados para prevención de phishing a nivel de los diferentes motores de inspección de código y servicios web apalancados en algoritmos de Machine Learning, se garantiza mayor efectividad en control de amenazas avanzadas, favor confirmar si se consideraría cubierto el requerimiento?

RESPUESTA 194.

Se solicita referirse a la necesidad institucional plasmada en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 127, numeral 80, en la que se establece que:

"La función de protección contra amenazas no basada en firmas debe emplear mecanismo basados en aprendizaje automático ("machine learning") para analizar imágenes en páginas web y determinar si están imitando marcas conocidas como parte de una campaña phishing."

En función de lo expuesto, se solicita regirse a la necesidad institucional plasmada en la Solicitud de ofertas (SDO).

PREGUNTA 195.-

En la página 134, numeral 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE consta que: Si se evidencia que los nodos físicos del sistema de Firewalls experimenten un consumo de capacidad de cómputo (CPU o RAM) superior al 90% mientras procesan un volumen de tráfico ("throughput") inferior al 90% de lo establecido en la CAPACIDAD DE PROCESAMIENTO DE TRÁFICO o en la CAPACIDAD DE PROCESAMIENTO DE TRÁFICO SSL/TLS solicitada se determinará que los equipos en cuestión no cumplen con este requerimiento y deberán ser fortalecidos o reemplazados por el Contratista.

Confirmar si este incremento en cómputo se refiere a valores máximos, considerando que los equipos están diseñados para enfrentar situaciones de ataque y sobrecarga o se refiere a un promedio del consumo de CPU (data plane y control plan) o Memoria RAM; y de ser este el caso, cuánto tiempo se consideraría para obtener el promedio para la medición con todos los módulos de seguridad activados.

RESPUESTA 195.

Los equipos objetos del presente proceso de contratación deberán cumplir con lo establecido en la CAPACIDAD DE PROCESAMIENTO DE TRÁFICO o en la CAPACIDAD DE PROCESAMIENTO DE TRÁFICO SSL/TLS solicitada dentro de los umbrales establecidos en la Solicitud de la Oferta (SDO). Independientemente de la situación, ya sea un pico de tráfico que llegue al umbral establecido en el pliego o que el volumen de tráfico se mantenga permanentemente en ese umbral, el equipo debe tener la capacidad suficiente para soportarlo y funcionar óptimamente.

Quedará a criterio del SRI el periodo de observación de esta medida, en función de los efectos del comportamiento del equipo en la operación tecnológica institucional.

PREGUNTA 196.-

En la página 109, numeral 5.4.1.1. SISTEMAS DE FIREWALLS, numeral 12. En el nuevo sistema de Firewalls se deben crear los usuarios VPN de acceso remoto existentes en la configuración actual, previa depuración, con sus respectivas reglas de acceso, utilizando doble factor de autenticación.

-

Confirmar que el sistema de doble factor de autenticación que utilizará el SRI permite conexión vía SAML o Radius. Podemos entender que este componente será provisto por SRI?

RESPUESTA 196.-

Se aclara que todos los componentes necesarios para la operación del mecanismo de autenticación de doble factor del sistema de firewalls deberán ser instalados, configurados y provistos con todo el software base y licenciamiento necesario para su funcionamiento.

De acuerdo a lo establecido en la Solicitud de la Oferta (SDO) en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 106, 5.3 INSTALACIÓN DEL SOFTWARE, numeral 5, donde se establece que:

"Si para la instalación y operación de los componentes de software se requiere software base como, por ejemplo, sistemas operativos, bases de datos, etcétera, el contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la instalación, activación y funcionamiento de dichos prerrequisitos siguiendo las mejores prácticas de fábrica, aplicando los estándares tecnológicos institucionales y cumpliendo con los requerimientos técnicos del SRI."

PREGUNTA 197.-

5. En la página 174 se indica que uno de los pagos se efectuará a "la suscripción del acta de entrega recepción de la instalación del hardware".

Con respecto a este punto, pedimos se nos aclare qué deberíamos entender por "instalación del Hardware".

RESPUESTA 197.

Referirse a la sección VIII. Condiciones Especiales de Contrato (CEC), página 174, BIENES REQUERIDOS, numeral 1, en el que se establece que:

"El plazo de la entrega de los bienes instalados será de hasta 90 días calendario contados a partir de la notificación del administrador del contrato. ***Para el efecto, el***

contratista deberá entregar el oficio de culminación de la instalación del hardware." *(énfasis añadido)*

Además, se solicita referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, 5.2 INSTALACIÓN DEL HARDWARE, páginas 105 y 106, numerales del 15 al 17.

PREGUNTA 198.-

En el documento de Licitación Pública Internacional, en la sección 5.2 INSTALACIÓN DEL HARDWARE, se indican que disponen de las siguientes SFPS y conexiones"

MEDIO	TIPO DE CONEXIÓN	FABRICANTE	MODELO
Óptico	40Gbps BASE-SR QSFP+ LC	Cisco	QSFP-40/100-SRBD
Óptico	25Gbps BASE-SR SFP+ LC	Cisco	SFP-25G-SR-S
Óptico	10Gbps BASE-SR SFP+ LC	Cisco	SFP-10G-SR
Óptico	1Gbps BASE-SX SFP LC	Cisco	GLC-SX-MMD

Por favor confirmar que, en este proceso se debe incluir SFP y estas serán provistas por el SRI. Caso contrario, especificar la cantidad de SFPs requeridas y sus características.

RESPUESTA 198.

En la sección VI. Requisitos de los Bienes y Servicios Conexos, página 105, en los numerales del 9 al 12 se establece que:

"El contratista debe proveer, como parte de la instalación de cada equipo entregado, los transceptores ("transceivers") **que sean necesarios** para su conexión con la infraestructura de red del SRI, en los centros de datos principal y alterno, utilizando los modelos que se indican en la tabla a continuación.

MEDIO	TIPO DE CONEXIÓN	FABRICANTE	MODELO
Óptico	*40Gbps BASE-SR QSFP+ LC*	*Cisco*	*QSFP-40/100-SRBD*
Óptico	*25Gbps BASE-SR SFP+ LC*	*Cisco*	*SFP-25G-SR-S*
Óptico	*10Gbps BASE-SR SFP+ LC*	*Cisco*	*SFP-10G-SR*
Óptico	*1Gbps BASE-SX SFP LC*	*Cisco*	*GLC-SX-MMD*

Tabla 7. *Modelos de transceptores ("transceivers") soportados por el switch de core institucional." (énfasis añadido)*

En virtud de lo expuesto, el contratista debe proveer e instalar la cantidad que sea necesaria de los transceivers de los componentes de hardware que conforman el objeto de esta contratación (solución ofertada) y los transceivers del switch de core institucional (tabla 7), para la correcta operación del sistema.

PREGUNTA 199.-

Por Favor en el caso que para realizar integraciones con el Directorio Activo y se requiera un servidor intermedio para esta integración, se entiende que el SRI suministrará la máquina virtual y/o servidor y el oferente deberá solo incluir la configuración y/o software de operación: "Si para la instalación y operación de los componentes de software se requiere software base como, por ejemplo, sistemas operativos, bases de datos, etcétera, el contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la instalación, activación y funcionamiento de dichos prerrequisitos siguiendo las mejores prácticas de fábrica, aplicando los estándares tecnológicos institucionales y cumpliendo con los requerimientos técnicos del SRI." Por favor confirmar.

RESPUESTA 199.

En la sección VI. Requisitos de los Bienes y Servicios Conexos, página 106, numeral 5.3 INSTALACION DE SOFTWARE, en los numerales del 2 al 5 se establece que:

2. *"Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como instancias virtuales (máquina o appliance) en los servidores de gestión de acuerdo con el detalle de la **tabla 6**.*
3. *El contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la instalación, activación y funcionamiento del software de virtualización necesario para el despliegue de las instancias virtuales (máquina o appliance) de los componentes de software, de acuerdo con el estándar del SRI (véase **INFRAESTRUCTURA ACTUAL**).*
4. *El contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la integración del software de virtualización instalado con la infraestructura virtual del SRI.*
5. *Si para la instalación y operación de los componentes de software se requiere software base como, por ejemplo, sistemas operativos, bases de datos, etcétera, el contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la instalación, activación y funcionamiento de dichos prerrequisitos siguiendo las mejores prácticas de fábrica, aplicando los estándares tecnológicos institucionales y cumpliendo con los requerimientos técnicos del SRI."*

En función de lo expuesto, en caso de ser necesario utilizar un servidor adicional para la integración con el Active Directory, deberá incluirse como una máquina virtual adicional dentro de la virtualización solicitada en el numeral 2 y cumpliendo el numeral 5 del texto citado.

PREGUNTA 200.-

Estimada Entidad, para asegurar la continuidad de los productos y considerando la vigencia y vida útil de los equipos, solicitamos que se acepten únicamente modelos lanzados al mercado a partir del año 2023 o en adelante. De esta manera el SRI, asegura una vigencia superior de los equipos. Por favor confirmar.

RESPUESTA 200.

Por favor referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 118, A. CONDICIONES GENERALES, literal 3 en el que se establece que:

"Para garantizar la vigencia tecnológica, solamente se aceptan equipos cuyo modelo se hayan liberado desde el año 2022 en adelante."

Adicional a esto, en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 134, numeral 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE, numeral 3 se establece que:

"Todos los equipos que conforman el componente de hardware del objeto de contrato deberán ser nuevos y se deberá garantizar que éstos no entren en EOST ("End-of-Support") ni en EOL ("End-of-Life") durante los 5 años posteriores a la fecha de suscripción del contrato."

PREGUNTA 201.-

Estimada Entidad, considerando que los equipos que dispondrán requieren capacidades de almacenamiento para una mejor operación de los equipos, solicitamos que, para beneficio del SRI, se acepte de manera mandatoria discos SSD de 900 GB o superior NVMe configurados en RAID-1. Por favor confirmar.

RESPUESTA 201.

Por favor referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, B. CLUSTER DE FIREWALL PRINCIPAL Y ALTERNO, página 119, numeral 7 en el que se establece que:

"Almacenamiento:

- *Cada equipo debe tener un volumen de almacenamiento con una capacidad de **no menos de 480GB de espacio**;*
- *El volumen de almacenamiento debe estar constituido por un arreglo RAID1, RAID10, RAID5 o RAID6;*
- *El volumen de almacenamiento debe estar conformado por al menos dos (2) unidades de estado sólido (SSD)." (énfasis añadido)*

En función de lo expuesto, es responsabilidad del oferente incluir la capacidad de almacenamiento necesaria para la óptima operación del sistema, tanto para el procesamiento del tráfico como para las operaciones de mantenimiento (ejemplo: respaldos, generación de información de diagnóstico, actualizaciones de versión, etc), de acuerdo con la arquitectura del fabricante, siendo la cantidad mínima 480 GB de espacio para almacenamiento.

PREGUNTA 202.-

En el documento de Licitación Pública Internacional, solicitan:

Conexión de red para tráfico de datos:

- Cada equipo debe tener no menos de dos (2) interfaces físicas independientes (no compartidas) Ethernet 40 Gbps Base-SR QSFP+ LC;
- Cada equipo debe tener no menos de una (1) interfaz Ethernet 10 Gbps Base-SR SFP+ LC;

Cada equipo debe contar con los transceptores ("transceiver") propios de fábrica necesarios para la operación de las interfaces de tráfico de datos.

Por favor confirmar que la cantidad de transceivers requerido sea correcto:

- Cada equipo deberá tener 2 interfaces Ethernet 40 Gbps Base-SR QSFP+ LC y se debe incluir el transceiver correspondiente, total 2.
- Cada equipo deberá tener 1 interfaz Ethernet 10 Gbps Base-SR SFP+ LC y se debe incluir el transceiver correspondiente, total 1**.**

RESPUESTA 202.

En la sección VI. Requisitos de los Bienes y Servicios Conexos, página 105, en los numerales del 9 al 12 se establece que:

"El contratista debe proveer, como parte de la instalación de cada equipo entregado, los transceptores ("transceivers") **que sean necesarios** para su conexión con la infraestructura de red del SRI, en los centros de datos principal y alterno, utilizando los modelos que se indican en la tabla a continuación.

MEDIO	***TIPO DE CONEXIÓN***	***FABRICANTE***	***MODELO***
Óptico	*40Gbps BASE-SR QSFP+ LC*	*Cisco*	*QSFP-40/100-SRBD*
Óptico	*25Gbps BASE-SR SFP+ LC*	*Cisco*	*SFP-25G-SR-S*
Óptico	*10Gbps BASE-SR SFP+ LC*	*Cisco*	*SFP-10G-SR*
Óptico	*1Gbps BASE-SX SFP LC*	*Cisco*	*GLC-SX-MMD*

Tabla 7. *Modelos de transceptores ("transceivers") soportados por el switch de core institucional." (énfasis añadido)*

En virtud de lo expuesto, el contratista debe proveer e instalar la cantidad que sea necesaria de los transceivers de los componentes de hardware que conforman el objeto de esta contratación (solución ofertada) y los transceivers del switch de core institucional (tabla 7), para la correcta operación del sistema.

PREGUNTA 203.-

Estimada Entidad, solicitan:

La función de inspección SSL/TLS de tráfico saliente debe permitir el descifrado selectivo en base a categorías de navegación, ya sea por tipo de contenido o por nivel de riesgo o por representar contenido sensible, y en base a nombres de host ("hostnames") y dominios.

¿Esto se refiere al bypass de inspección SSL para sitios definidos por categorías? Es correcto nuestro entendimiento

RESPUESTA 203.

No es correcto su entendimiento. No se limita únicamente al bypass de inspección SSL para sitios definidos por categorías.

Se aclara que la función de inspección SSL/TLS debe ser capaz de descifrar y analizar selectivamente el tráfico saliente, tomando decisiones basadas en categorías de navegación, ya sea por el tipo de contenido o por nivel de riesgo o por representar contenido sensible y en base a nombres de host y dominios.

PREGUNTA 204.-

En el documento de Licitación Pública Internacional solicitan:

"24. La gestión de políticas debe tener la capacidad de integrarse con el sistema vCenter del SRI (véase INFRAESTRUCTURA ACTUAL) para importar objetos de manera que se puedan utilizar como origen o destino para crear reglas de seguridad."

¿Por favor confirmar si actualmente disponen del VCenter y como parte de este proyecto es realizar la integración, o la solución propuesta deberá tener la capacidad de

integración a futuro? ¿Y si es a futuro se debe contemplar como parte de esta implementación?

RESPUESTA 204.

En la sección VI. Requisitos de los Bienes y Servicios Conexos, página 102, numeral 12, tabla 3 se detalla las versiones de software de los componentes de la plataforma de virtualización que dispone el SRI, en el que se incluye el vcenter.

La necesidad institucional plasmada en la Solicitud de ofertas (SDO). requiere que la gestión de políticas tenga la capacidad de integrarse con el sistema vCenter del SRI en la actualidad; no se trata de una propuesta de integración futura.

PREGUNTA 205.-

En el documento de Licitación Pública Internacional solicitan: “La gestión de políticas debe tener la capacidad de integrarse con el sistema Active Directory del SRI (véase INFRAESTRUCTURA ACTUAL) para importar objetos de manera que se puedan utilizar como origen o destino para crear reglas de seguridad.” Por favor hay que aclarar que objetos corresponden a los usuarios y grupos de usuarios del directorio activo.

RESPUESTA 205.

Se confirma que los objetos a importarse desde el sistema Active Directory son: usuarios y grupos de usuarios, sin limitarse a otros objetos del Active Directory.

PREGUNTA 206.-

En el documento de Licitación Pública Internacional solicitan la rescritura de nuevo de las reglas. Referencia en el punto 5.4.1.1. ¿Se debe realizar la migración de reglas usando Migrate Export o se debe considerar una reescritura de las reglas?

RESPUESTA 206.

Referirse a la necesidad institucional plasmada en la sección Sección VI. Requisitos de los Bienes y Servicios Conexos, página 107, 5.4.1. MIGRACIÓN.

Además, referirse a lo solicitado en la misma sección, página 5.4.11 SISTEMAS DE FIREWALLS , numeral 1, donde se establece que:

*“Las políticas del sistema de firewalls deberán **ser transcritas** desde el sistema actual*

al nuevo sistema." (énfasis añadido)

PREGUNTA 207.-

En el documento de Licitación Pública Internacional numeral 3. Especificaciones Técnicas, sub numeral 4. INFRAESTRUCTURA ACTUAL se detalla la infraestructura (hardware, software) que a la fecha dispone el SRI, mencionando que: *"Toda la información de este apartado ha sido levantada a la fecha del presente documento. Esta puede variar en función de la operación y las necesidades institucionales y de las nuevas liberaciones de los fabricantes. Es responsabilidad del contratista hacer las validaciones correspondientes oportunamente"* en este contexto se pregunta si está previsto la realización de visita técnica para efectuar validación, en el caso de ser la respuesta positiva por favor indicar el cronograma y condiciones para su ejecución.

RESPUESTA 207.

Se aclara que la nota incluida en la sección VI. Requisitos de los Bienes y Servicios Conexos, página 103:

*"**NOTA**: Toda la información de este apartado ha sido levantada a la fecha del presente documento. Esta puede variar en función de la operación y las necesidades institucionales y de las nuevas liberaciones de los fabricantes. Es responsabilidad del contratista hacer las validaciones correspondientes oportunamente."*

La visita técnica para realizar las validaciones correspondientes aplicará únicamente para el oferente adjudicado.

PREGUNTA 208.-

En el documento de Licitación Pública Internacional numeral 3. Especificaciones Técnicas, numeral 5.3 INSTALACIÓN DEL SOFTWARE, sub numeral 4 establece: *"El contratista deberá entregar el licenciamiento y realizar los trabajos necesarios para la integración del software de virtualización instalado con la infraestructura virtual del SRI."*

Por favor indicar los fabricantes y versiones de infraestructura virtual del SRI con la que hay que integrar la solución a adquirir por medio del presente proceso.

RESPUESTA 208.-

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, INFRAESTRUCTURA ACTUAL, página 102, tabla 3.

PREGUNTA 209.-

En el documento de Licitación Pública Internacional numeral 3. Especificaciones Técnicas, sub numeral *5.4.1. MIGRACIÓN, numeral 5 se establece que: "Todas las actividades de las etapas de Transición, Puesta en producción y Estabilización asociadas con la intervención de equipos tecnológicos deberán realizarse presencialmente por el personal especializado del Fabricante en conjunto con el personal técnico del Contratista.",* por otro lado referente *a* PERSONAL TÉCNICO MÍNIMO se requiere *"Técnico especialista de instalación y migración"* con un perfil que acredite *"Certificación Técnica vigente nivel profesional, avanzado o equivalente emitida por el fabricante del sistema de Firewalls y del servicio SaaS de protección de correo electrónico ofertados"* entendemos que el personal técnico certificado por el fabricante está capacitado para realizar la migración de forma presencial apoyado de forma remota por el fabricante, ratificar o rectificar nuestro entendimiento.

RESPUESTA 209.

No es correcto su entendimiento, referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, página 107, 5.4 SERVICIOS CONEXOS REQUERIDOS, 5.4.1 MIGRACIÓN, numeral 5 y 6 donde se establece que:

5. *"Todas las actividades de las etapas de **Transición**, **Puesta en producción** y **Estabilización** asociadas con la intervención de equipos tecnológicos deberán realizarse **presencialmente por el personal especializado del Fabricante en conjunto con el personal técnico del Contratista.** (énfasis añadido)*
6. *Si el SRI considera necesaria la intervención del personal especializado del Fabricante en cualquiera de las etapas de migración, este podrá solicitarla formalmente, aplicándose el **ACUERDO DE NIVEL DE SERVICIO** para Asistencia Técnica con prioridad 3."*

PREGUNTA 210.-

En el documento de Licitación Pública Internacional numeral 3. Especificaciones Técnicas, sub numeral 5.4.2.1 MANTENIMIENTO PREVENTIVO numeral 4 se establece:

"En cada periodo, el contratista deberá realizar una (1) visita de mantenimiento preventivo por cada centro de datos (…)" por lo que entendemos que se debe realizar tres mantenimientos preventivos durante la vigencia del contrato: Primer periodo: 295 días, Segundo periodo: 295 días, Tercer periodo: 294 días, por favor ratificar o rectificar nuestro entendimiento.

RESPUESTA 210.

Es correcto su entendimiento

PREGUNTA 211.-

En el documento de Licitación Pública Internacional numeral 3. Especificaciones Técnicas, sub numeral 5.4.2.2 MANTENIMIENTO CORRECTIVO se requiere el mencionado servicio, entendemos que para brindar el mismo el SRI debe cumplir con los términos y condiciones de la garantía técnica proporcionada por el fabricante y/o proveedor que cubre defectos de fabricación y excluye daños causados por uso inadecuado, negligencia, accidentes, o modificaciones no autorizadas, por lo que en el caso de que el SRI no cumpla con las condiciones establecidas en la garantía el mencionado servicio sería facturado, por xfavor ratificar o rectificar nuestro entendimiento

RESPUESTA 211.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, páginas 134 y 135, 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, páginas 115, 116 y 117, 5.5 ACUERDO DE NIVEL DE SERVICIO.

Además, referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, 5.2 INSTALACIÓN DEL HARDWARE, página 105, numeral 7, donde se establece que:

"El contratista deberá instalar el hardware siguiendo las mejores prácticas de ensamblaje, montaje, configuración de parámetros y de conexión recomendadas por el fabricante de este."

No se podrá facturar ningún servicio adicional al establecido en el presente proceso.

PREGUNTA 212.-

En el documento de Licitación Pública Internacional numeral 3. Especificaciones Técnicas, sub numeral 5.4.2.2 MANTENIMIENTO CORRECTIVO numeral 6 establece: "Si la atención de un incidente requiere el levantamiento de información, la ejecución de algún comando, la captura u obtención de datos o la obtención de registros de eventos ("logs"), es responsabilidad del contratista hacer todas las solicitudes y gestiones necesarias de forma oportuna y previsiva para obtener estos(as), sin perjuicio del cumplimiento del ACUERDO DE NIVEL DE SERVICIO." un incidente es un evento no planificado que se presenta de forma imprevista por lo que nuestro entender no es posible aplicar el "hacer todas las solicitudes y gestiones necesarias de forma oportuna y previsiva", por favor ratificar o rectificar nuestro entendimiento.

RESPUESTA 212.

Se aclara que la frase "hacer todas las solicitudes y gestiones necesarias de forma oportuna y previsiva", significa que el contratista debe actuar rápidamente ante las necesidades que puedan surgir durante la gestión del incidente.

PREGUNTA 213.-

En el documento de Licitación Pública Internacional numeral 3. Especificaciones Técnicas, sub numeral 5.4.2.3 ASISTENCIA TÉCNICA, se detalla requerimientos relacionados al mencionado servicio, por favor podrían establecer el alcance de este servicio en términos de número de horas, el valor de cada hora de servicio, periodicidad de facturación

RESPUESTA 213.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, 5.4.2.3 ASISTENCIA TÉCNICA, página 114, numeral 2, donde se establece que:

"El servicio de asistencia técnica debe estar disponible las 24 horas del día, los 7 días de la semana, durante la vigencia del contrato."

Adicional referirse a la misma sección numeral 3, donde se establece que:
*"El servicio de asistencia técnica se manejará en base a requerimientos, los cuales serán registrados mediante los canales de comunicación provistos por el contratista en la fase de **INSTALACIÓN**."*

En función de lo expuesto, la Asistencia Técnica, forma parte del SOPORTE LOCAL y se pagará de acuerdo con lo establecido en la sección VIII. Condiciones Especiales de Contrato (CEC), página 174, CGC 17.1 numeral 3. Soporte Local.

PREGUNTA 214.-

En el documento de Licitación Pública Internacional numeral 3. Especificaciones Técnicas su numeral 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE se requiere la referida garantía, entendemos que la misma cubre defectos de fabricación y excluye daños causados por uso inadecuado, negligencia, accidentes, o modificaciones no autorizadas, por favor ratificar o rectificar nuestro entendimiento.

RESPUESTA 214.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, páginas 134 y 135, 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, páginas 115, 116 y 117, 5.5 ACUERDO DE NIVEL DE SERVICIO.

Además, referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, 5.2 INSTALACIÓN DEL HARDWARE, página 105, numeral 7, donde se establece que:

"El contratista deberá instalar el hardware siguiendo las mejores prácticas de ensamblaje, montaje, configuración de parámetros y de conexión recomendadas por el fabricante de este."

No se podrá facturar ningún servicio adicional al establecido en el presente proceso.

PREGUNTA 215.-

En el documento de Licitación Pública Internacional numeral 3. Especificaciones Técnicas, sub numeral 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE, numeral 5 se establece: "Si se evidencia que la capacidad de cómputo (CPU o RAM) de alguno de los Servidores de gestión, principal o alterno, no es suficiente para la óptima operación de las máquinas virtuales y appliance virtuales alojados, se deberá agregar la cantidad de recursos tecnológicos necesarios para este efecto, manteniendo la simetría entre principal y alterno, y cumpliendo con las condiciones de desempeño establecidas en ambos casos."

Por favor su ayuda contestando las siguientes preguntas ¿Cómo se va a medir de forma objetiva analítica la capacidad de cómputo? ¿Cuáles parámetros se van a evaluar? ¿Cuáles son los umbrales definidos para cada uno de los parámetros?

RESPUESTA 215.

En base a las estadísticas de consumo de la capacidad de cómputo CPU o RAM de los servidores de gestión principal o alterno el Administrador de Contrato notificará al contratista la necesidad de incrementar estos recursos hasta que se logre un nivel óptimo de funcionamiento en función de los efectos del comportamiento del equipo en la operación tecnológica institucional. Adicionalmente cabe indicar que los requerimientos de capacidad de cómputo (CPU o RAM) dependerán de la arquitectura tecnológica y la cantidad de componentes que incluya el sistema ofertado.

PREGUNTA 216.-

En el documento de Licitación Pública Internacional numeral 3. Especificaciones Técnicas, sub numeral 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE, sub numeral 12 se establece: "El servicio de soporte de fábrica del hardware debe incluir, pero no debe estar limitado a, las prestaciones que se indican a continuación (..)" Por favor determinar las prestaciones que debe incluir el soporte de fábrica

RESPUESTA 216.-

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE, página 135, numeral 12, donde se establece que:

12. *"**El servicio de soporte de fábrica del hardware debe incluir, pero no debe estar limitado a**, las prestaciones que se indican a continuación:*
    - ***12.a.*** *Gestión de incidentes causados por el hardware;*
    - ***12.b.*** *Recomendación de versiones de firmware para los servidores del sistema;*
    - ***12.c.*** *Revisión del estado de los servidores del sistema;*
    - ***12.d.*** *Acceso a la Base de Conocimientos del fabricante;*
    - ***12.e.*** *Acceso a la Mesa de Ayuda del fabricante;*
    - ***12.f.*** *Notificaciones proactivas de nuevas versiones y parches liberados." (énfasis añadido)*

Se aclara que la expresión “El servicio de soporte de fábrica del hardware debe incluir, pero no debe estar limitado a” significa que el servicio debe contemplar las prestaciones enumeradas como requisitos mínimos (obligatorios) que el fabricante debe ofrecer como parte del soporte, pero también podría incluir otras características que no están específicamente mencionadas.

PREGUNTA 217.-

En el documento de Licitación Pública Internacional numeral 3. Especificaciones Técnicas, sub numeral 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE, numeral 13 se establece: “El contratista deberá dejar constancia de la entrega y vigencia de la garantía técnica mediante un certificado de garantía técnica del hardware que debe adjuntar la documentación que sustente el cumplimiento de todo lo solicitado en este ámbito incluyendo, pero no limitado a (…)” Por favor determinar la documentación y su contenido para sustentar lo solicitado.

RESPUESTA 217.

Referirse a la sección VI. Requisitos de los Bienes y Servicios Conexos, 6.1.3 GARANTÍA TÉCNICA DEL HARDWARE, página 135, numeral 13, donde se establece que:

13. *“El contratista deberá dejar constancia de la entrega y vigencia de la garantía técnica mediante un* ***certificado de garantía técnica del hardware*** *que debe adjuntar la documentación que sustente el cumplimiento de todo lo solicitado en este ámbito incluyendo, pero no limitado a:*

13.a. *La documentación que sustente la vigencia de la garantía técnica del fabricante del hardware de todos los equipos que conforman el componente de hardware del objeto de contrato, indicando su alcance y su fecha de expiración;*

13.b. *La documentación que indique el tipo o el nivel de soporte de fábrica con el que cuentan todos los equipos que conforman el componente de hardware del objeto de contrato, indicando su alcance, su disponibilidad (ej. 24x7), los canales de comunicación con fábrica y su fecha de expiración.”*

Se aclara que la expresión “debe adjuntar la documentación que sustente el cumplimiento de todo lo solicitado en este ámbito incluyendo, pero no limitado a”

significa que los puntos 13.a y 13.b son de cumplimiento obligatorio, pero también se podría incluir otros documentos que sean de relevancia para sustentar el cumplimiento de la entrega y vigencia de la garantía técnica por parte del fabricante.

PREGUNTA 218.-

SERVIDORES DE GESTIÓN PRINCIPAL Y ALTERNO

La especificación "*3. Cada servidor de gestión debecontar con una protección frontal que impida la manipulación no autorizada de los componentesdel servidor.*", **¿podría ser opcional para el casode soluciones que se presenten con hardwarededicado o de propósito específico?**

RESPUESTA 218.

Referirse a la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 104, 5.2 INSTALACIÓN DEL HARDWARE, numeral 5, donde se establece que:

"Los gestores de firewall y los Componentes de análisis de configuración y eventos deben desplegarse como appliance virtual o como máquina virtual (VM) en su respectivo servidor de gestión tal como se indica en la tabla a continuación.

COMPONENTE DE SOFTWARE	***SERVIDOR FÍSICO***	***SITIO***
Gestor de firewall principal	*Servidor de gestión principal*	*CD Principal*
Componente de análisis de configuración y eventos principal	*Servidor de gestión principal*	*CD Principal*
Gestor de firewall alterno	*Servidor de gestión alterno*	*CD Alterno*
Componente de análisis de configuración y eventos alterno	*Servidor de gestión alterno*	*CD Alterno*

Tabla 6. *Correspondencia entre instancias virtuales y servidores físicos."*

En función de lo expuesto, se aclara que los servidores de gestión principal y alterno no pueden ser appliance de propósito específico.

Por lo tanto, no se acoge su solicitud, la necesidad institucional plasmada en la Sección VI. Requisitos de los Bienes y Servicios Conexos, página 120, C. SERVIDORES DE GESTIÓN PRINCIPAL Y ALTERNO (2 EQUIPOS), numeral 3, donde se establece que:

"Cada servidor de gestión debe contar con una protección frontal que impida la manipulación no autorizada de los componentes del servidor."