Bogotá D.C., 10 de noviembre de 2021

Señores
PROVEEDORES
Ciudad

Referencia: CONVOCATORIA PÚBLICA PARA PARA CONTRATAR LOS SERVICIOS PARA LA IMPLEMENTACIÓN, OPERACIÓN Y MONITOREO DE LAS SOLUCIONES QUE CONFORMAN LA ARQUITECTURA DE CIBERSEGURIDAD PARA LA PLATAFORMA TECNOLÓGICA DE LA CÁMARA DE COMERCIO DE BOGOTÁ (CCB), BAJO LA MODALIDAD HÍBRIDA (ON PREMISES Y EN LA NUBE) CON EL OBJETIVO DE PROTEGER LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN EN LA CCB. No. 3000000778.

Asunto: Respuesta a observaciones

Con el presente documento la Cámara de Comercio de Bogotá (CCB) responde a las preguntas allegadas en tiempo dentro del proceso de invitación de la referencia.

Pregunta 1
Con relación a lo dispuesto en el numeral 3.3.2 de la Convocatoria, se solicita a la Cámara de Comercio de Bogotá la ampliacion del rango de fechas de los contratos para acreditar la experiencia, permitiendo acreditar contratos con fecha de ejecucion desde el 1 de enero de 2016. Adicional, se solicita que se permita acreditar la experiencia mínimo en 2 contratos y no en 4 como está el actual requerimiento.

Respuesta
No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 2
Con relación a lo dispuesto en el numeral 4.1 de la Convocatoria, se solicita a la Cámara de Comercio de Bogotá indicar si el plazo de ejecución corresponde al del licenciamiento o corresponde al soporte local sobre las soluciones.

Respuesta
La solución tecnológica debe ser entregada como servicio. La CCB no está adquiriendo licenciamiento. El plazo indicado en el numerl 4.1 hace referencia al plazo de ejecución del contrato que se va a suscribir.

Pregunta 3
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita a la Cámara de Comercio de Bogotá aclarar si el WAF debe estar instalado en AWS en el tenant de la entidad en HA, o si se permiten soluciones en la nube del fabricante.

Respuesta
La solución tecnológica debe ser entregada como servicio. La nube será seleccionada por el proveedor, quien debe garantizar el cumplimiento de los ANS solicitados.

Pregunta 4
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita a la Cámara de Comercio de Bogotá entidad aclarar el throughput requerido en Mbps (Mega bits por segundo), con el fin de estimar el throughput requerido y no solo el consumo total (15 TB).

Respuesta
La entidad cuenta con dos enlaces que ofrecen un total de 600 Mbps. De esta capacidad se utiliza aproximadamente un 70% en temporada alta y un 40% el resto del período.

Pregunta 5
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita a la Cámara de Comercio de Bogotá permitir que se puedan ofrecer soluciones que no se integren nativamente con el Firewall de Nueva generación, ya que los ataques Web en su mayoría son en capa de aplicación y no capa 3 (dirección IP), por lo que se pueden generar falsos positivos, así como tener una solución del mismo fabricante que no garantiza tener lo mejor de los dos mundos ya que muchos de los fabricantes de FW no aparecen en gartner como fabricantes de WAF y viceversa.

Respuesta
Se mantienen las especificaciones técnicas solicitadas. No se está solicitando que las soluciones ofrecidas sean del mismo fabricante.

Pregunta 6
Con relación al tema de autenticación de usuarios se solicita resolver las siguientes inquietudes:

- ¿Se espera contar con una solución de tipo NAC para este servicio? **Rpta.:** No es el requerimiento solicitado
- ¿Cuál es el número de IPs? **Rpta.:** Considerar 2200 usuarios finales
- ¿Existe actualmente una política de seguridad configurada general o varía en función de diferentes entornos? **Rpta.:** Esta información será compartida con el proveedor seleccionado.
- ¿Cuál es la volumetría estimada de excepciones mensuales? **Rpta.:** Esta información será compartida con el proveedor seleccionado.
- ¿Cuál es la volumetría estimada de incidencias mensuales? **Rpta.:** Esta información será compartida con el proveedor seleccionado.

Pregunta 7
Con relación al WAF se solicita resolver las siguientes inquietudes:

- ¿Cuántas aplicaciones web se quieren proteger y cuántas aplicaciones web se tienen pensado integrar en los próximos años? **Rpta.:** Aplicaciones WEB a proteger: hasta 50
- ¿Dónde se encuentran los servidores web a ser protegidos? **Rpta.:** En Nube.
- ¿Qué tipo de web servers se necesitan proteger? ¿Se necesitan proteger algún servicio web HTTP API (REST, SOAP, etc.)? **Rpta.:** Servidores IIS, Apache y API (REST, SOAP)
- ¿Se está buscando complementar la funcionalidad WAF con una solución de tipo bot management, protección frente a DDoS o CDN? **Rpta.:** No está dentro del alcance de este contrato.
- ¿La organización necesita dar cumplimiento a alguna normativa o regulación concreta? Ej. PCI-DSS. **Rpta.:** Esta información será compartida con el proveedor seleccionado.

Pregunta 8
Con relación al WF se solicita resolver las siguientes inquietudes:

- Brindar información sobre la topología (se dispone de una doble barrera perimetral, se encuentra en un entorno de firewalls en cloud, cuántas sedes existen en la organización, etc.). **Rpta.:** Esta información será compartida con el proveedor seleccionado.
- Listado o número aproximado de redes incluidas en los firewalls. **Rpta.:** Aproximadamente 15
- Número estimado de VPNs a ser configuradas. **Rpta.:** Esta información será compartida con el proveedor seleccionado.

- ¿Cuál es el número estimado de peticiones de cambio por semana/mes? ¿Existe algún tipo de ventana de cambio acordada? **Rpta.:** Esta información será compartida con el proveedor seleccionado.
- ¿Cuál es la política actual de backup? **Rpta.:** Se cuenta con un esquema, diario, semanal y mensual.
- ¿Cuál es el número de reglas o políticas a definir en el firewall? **Rpta.:** Esta información será compartida con el proveedor seleccionado.
- ¿Se realizan de forma periódica auditorías de reglas en los firewalls? **Rpta.:** Esta información será compartida con el proveedor seleccionado.

Pregunta 9

Con relación al EDR se solicita resolver las siguientes inquietudes:

- ¿Cuáles son las volumetrías de cambio estimadas al mes? **Rpta.:** Bajas
- ¿Cuáles son las volumetrías de incidencias estimadas al mes? **Rpta.:** Esta información se entregará al proveedor seleccionado.
- ¿Se cuenta con una política de protección general o existen varias en función de departamentos, áreas, sedes, etc.? **Rpta.:** Esta información será compartida con el proveedor seleccionado.
- ¿Se requiere realizar análisis de malware? En caso afirmativo, ¿Cuál es la volumetría anual estimada? **Rpta.:** Se debe cumplir con las especificaciones técnicas solicitadas en la invitación.
- ¿Se requieren servicios de gestión/tratamiento de alertas? **Rpta.:** Se debe cumplir con las especificaciones técnicas solicitadas en la invitación.
- ¿Se requieren servicios de Threat Hunting? **Rpta.:** Se debe cumplir con las especificaciones técnicas solicitadas en la invitación.

Pregunta 10

Con relación al DLP+CASB se solicita resolver las siguientes inquietudes:

- Indicar el número de usuarios de correo. **Rpta.:** 2200.
- Indicar el número de puestos clientes. **Rpta.:** 2200.
- ¿Existe una política de clasificación de la información? **Rpta.:** Sí, el detalle de esta información será compartida con el proveedor seleccionado.
- ¿Existe algún proyecto de levantamiento y clasificación de la información? **Rpta.:** Sí, el detalle de esta información será compartida con el proveedor seleccionado.
- ¿Cuál es el fabricante de Antivirus que tiene la Cámara de Comercio de Bogotá? **Rpta.:** Esta información será compartida con el proveedor seleccionado.
- ¿Existe una consola de gestión centralizada de agentes (SCCM)? **Rpta.:** No
- ¿Cuál fabricante de Proxy usa la Cámara de Comercio de Bogotá? **Rpta.:** Esta información será compartida con el proveedor seleccionado.
- ¿Cuál fabricante de Firewall usa la Cámara de Comercio de Bogotá? **Rpta.:** Actualmente Palo Alto (On premises).
- ¿Cuál es el nivel de licenciamiento de Microsoft de Cámara de la Comercio de Bogotá (E3, E3P1, E3P2, E5,…)? **Rpta.:** E3
- Adicionalmente a la suite de O365, ¿existen otras aplicaciones cloud corporativas? (Salesforce, Workday, etc.) **Rpta.:** Sí, considerar hasta 10. El listado será compartido con el proveedor seleccionado.
- ¿Existen entornos de virtualización de aplicaciones de trabajo para usuario final dentro del scope (Citrix, etc.)? **Rpta.:** No
- ¿Cuál es el cliente de correo? ¿es el corporativo? **Rpta.:** Outlook.
- ¿Cuál es el navegador web? ¿es el corporativo? **Rpta.:** Se utilizan los principales del mercado.
- ¿Se permiten navegadores alternativos además del corporativo? **Rpta.:** N/A

Pregunta 11
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita comedidamente a la Cámara de Comercio de Bogotá aclarar si los costos tenant en AWS deben ir incluidos en esta solicitud o serán entregados por la entidad. ¿Quién entregará y administrará el tenant, VPC para la instalación de los componenentes de seguridad solicitados?

Respuesta
La solución tecnológica propuesta debe ser bajo modelo SaaS.

Pregunta 12
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita a la Cámara de Comercio de Bogotá aclarar si se debe incluir la adminitración del Tenant y todos los componentes requeridas de AWS.

Respuesta
Ver pregunta 3.

Pregunta 13
Con relación a lo dispuesto en el numeral 3.3 de la Convocatoria, se agradece a la Cámara de Comercio de Bogotá aclarar el termino "*como de la información generada en la ejecución del servicio contratado*". En este punto, ¿qué tipo de información requiere la entidad? luego no se entiende si es a nivel operacional, a nivel de incidentes, ANS de servicio, monitoreo de canales, solicitudes, tickets, etc.

Respuesta
Se hace referencia a lo definido dentro del numeral 3.5 Reportes.

Pregunta 14
Con relación a lo dispuesto en el numeral 3.3 de la Convocatoria, se agradece a la Cámara de Comercio de Bogotá aclarar el termino "*un plan de respaldo en caso de borrados accidentales o provocados*". Se agradece a la entidad aclarar si se quiere hacer cumplimiento de alguna normativa en recuperación ante desastres. ¿Se requiere que esta información se guarde en algún tipo de medio para respaldar la información Cinta, discos, NAS? ¿Se requriere que el respaldo se entregue a la entidad?. Se requiere aclarar si la entidad requiere el servicio de cintoteca resguardar los registros. ¿La entidad se hará cargo de los costos adicionales que implique el resguardo de registros fuera de la entidad? ¿Requiere la entidad que este tipo de respaldo aplique una normativa en específica?

Respuesta
El servicio es Modelo SaaS para todos sus entregables y la solución tecnológica debe estar aprovisionada en nube.

Pregunta 15
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se agradece a la Cámara de Comercio de Bogotá incluir el "*termino más estable*", luego no siempre la última versión es la más estable para la operación.

Respuesta
No se acepta su observación, se mantienen los requerimientos técnicos.

Pregunta 16
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se agradece a la Cámara de Comercio de Bogotá aclarar el termino "*y es responsable de la remediación que le sean identificadas de acuerdo con la criticidad y tiempos establecidos con la CCB*", luego en caso de encontrarse vulnerabilidades en activos como servidores, equipos de computo, IOT, Networking, etc. ¿Deberá el oferente realizar la remediación correspondiente de estos activos?

Respuesta
Se hace referencia a la solución tecnológica propuesta por el proponente.

Pregunta 17
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita amablemente a la Cámara de Comercio de Bogotá aclarar y especificar si cuentan con una herramienta para la gestión y administración de usuarios (inyternos, externos, privilegiados).

Respuesta
Directorio Activo.

Pregunta 18
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita amablemente a la Cámara de Comercio de Bogotá especificar y detallar la cantidad de dispositivos corporativos y externos (de usuarios finales), sobre los cuales se habilitará el acceso a la redes de la entidad. Adicionalmente, aclarar si es posible instalar agentes o realizar configuraciones sobre estos dispositivos.

Respuesta
De acuerdo con lo indicado en la invitación, son 2200 usuarios.

Pregunta 19
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita amablemente a la Cámara de Comercio de Bogotá aclarar y especificar si la CCB cuenta con herramientas de doble factor de autenticación, gestión y generación de certificados. Adicionalmente, ¿cual será la cantidad de certificados necesarios?

Respuesta
El proveedor deberá ofertar la solución que cumpla con los requerimientos solicitados en la invitación.

Pregunta 20
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita amablemente a la Cámara de Comercio de Bogotá aclarar y especificar cual es la plataforma y sobre que recursos se encuentra el servicio de directorio activo de la CCB. Adicionalmente, por favor especificar en que lugar se encuentra alojado este servicio (en premisas o en nube).

Respuesta
Microsoft Windows server 2016 y 2019, en Nube

Pregunta 21
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita amablemente a la Cámara de Comercio de Bogotá aclarar y especificar cual es la herramienta de antimalware que tiene la CCB, versión y tipo de despliegue actual. Adicionalmente, aclarar si es posible realizar integraciones con las soluciones de otros fabricantes a proponer.

Respuesta
La CCB cuenta con una solución antimalware. Los detalles serán entregados al proveedor seleccionado.

Pregunta 22
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita amablemente a la Cámara de Comercio de Bogotá aclarar si los 350 servidores estan ya en publición o se deberá establecer junto a la entidad un cronograma de migración de soluciones.

Respuesta
No es necesario un cronograma de migración de soluciones.

Pregunta 23
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita amablemente a la Cámara de Comercio de Bogotá aclarar y especificar si cuentan con un listado o matriz de aplicaciones y servicios autorizados en la nube y usuarios con perfiles y permisos para el uso de estas aplicaciones.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 24
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita amablemente a la Cámara de Comercio de Bogotá indicar que tipo de servicios de Shadow IT requieren ser bloqueados y las nubes que se van a integrar.

Respuesta
AWS.

Pregunta 25
Con relación a lo dispuesto en el numeral 3.8 de la Convocatoria, se solicita amablemente a la Cámara de Comercio de Bogotá aclarar y especificar si cuentan con un proceso de clasificación y etiquetado de la información.

Respuesta
Ver pregunta 10.

Pregunta 26
Respecto a la funcionalidad del parche virtual solicitada en los requerimientos técnicos del Endpoint Detection and Response, solicitamos aceptar funcionalidades que permitan evitar que alguna vulnerabilidad en el sistema operativo o aplicaciones sea utilizada para crear una brecha en los sistemas, independientemente que no se considere o se llame parche virtual.

Respuesta
La solución debe implementar protección de vulnerabilidades para vulnerabilidades conocidas en el sistema operativo y para aplicaciones que no son del sistema operativo.

Pregunta 27
Respecto a la condición solicitada en el EDR "*Los informes deben incluir análisis guiados y soluciones basadas en la inteligencia recopilada por el proveedor, por ejemplo, "los siguientes pasos necesarios para contener esta amenaza son xyz*" nos permitimos indicar que existen soluciones en el mercado que toman acciones proactivas y no reactivas como las solicitadas, por lo tanto, el informe contendrá la información de lo que se hizo para contener la amenaza. Agradecemos sea tenido en cuenta esta condición para dar por cumplido este requerimiento.

Respuesta
De acuerdo.

Pregunta 28
Solicitamos indicar cual es la solución antimalware que actualmente posee la Cámara de Comercio de Bogotá, para validar la integración con nuestras soluciones.

Respuesta
La CCB cuenta con una solución antimalware. Los detalles serán entregados al proveedor seleccioando.

Pregunta 29
En caso de que no sea posible "*hacer uso de la información que genere el Antimalware con el que actualmente cuenta la CCB*", solicitamos permitir que la solución EDR pueda remplazar la funcionalidad antimalware, sin que esto represente un mayor valor para la entidad.

Respuesta
De acuerdo.

Pregunta 30
Respecto a las características solicitadas para el componente FWasS, solicitamos a la entidad indicar cual es la tecnología SDWAN utilizada en la actualidad.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 31
Respecto a las condiciones técnicas del CASB, agradecemos NO solicitar la información de dispositivo y ubicación del empleado, ya que bajo ciertas tecnologías esta información no siempre puede ser obtenida de forma confiable.

Respuesta
No se acepta su observación, se mantienen los requerimientos solicitados.

Pregunta 32
Solicitamos que sea modificado el requisito para CASB "*Permitir la aplicación de políticas para proteger los datos de la organización en la nube. Esto debe implicar, al menos, un control de acceso granular y mecanismos para impedir la carga de datos en la nube que no cuenten con autorización para ello, de*

acuerdo políticas de seguridad establecidas por la CCB" por "*Permitir la aplicación de políticas para proteger los datos de la organización en la nube. Esto debe implicar, al menos, un control de acceso granular, de acuerdo políticas de seguridad establecidas por la CCB*".

Respuesta
No se acepta si observación, se mantienen los requerimientos solicitados.

Pregunta 33
Agradecemos indicar si el siguiente requerimiento de CASB "*detectar aquellos usuarios que llevan mucho tiempo inactivos, así como los usuarios externos a la organización (consultores externos, proveedores, etc.)*" puede ser logrado a través de funcionalidades propias de Microsoft 365.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 34
Solicitamos a la CCB indicar el tipo de suscripciones que poseen para los usuarios.

Respuesta
No se indica a qué suscripciones se refiere.

Pregunta 35
Agradecemos indicar si es posible presentar dos alternativas de arquitecturas para el servicio.

Respuesta
El proponente debe definir la solución tecnológica que cubra lo solicitado en el apartado "Requerimientos Técnicos".

Pregunta 36
Respecto a las penalidades, entendemos que estas se aplican únicamente sobre el valor mensual de la funcionalidad afectada (CASB, EDR, FWasS, etc.) agradecemos confirmar si el entendimiento es correcto.

Respuesta
Los ANS están definidos considerando el servicio total contratado.

Pregunta 37
Respecto a la funcionalidad de CASB "*Permitir habilitar políticas únicas para dispositivos administrados y no administrados, en navegadores o en aplicaciones móviles enriquecidas*.", solicitamos sea modificada de la siguiente manera: "*Permitir habilitar políticas únicas para dispositivos administrados y no administrados*".

Respuesta
No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 38
Respecto a la funcionalidad de DLP, solicitamos que sea eliminado el requerimiento de gestión de políticas de red, ya que esto implicaría el despliegue de appliances en la red de la entidad.

Respuesta
No se acepta su observación, se mantienen los requerimientos solicitados.

Pregunta 39
Respecto del numeral 3.8 Requerimientos técnicos, en el capítulo asociado a la solución de EndPoint Detection and Response (EDR):
a) En el requerimiento que indica: "...*la solución debe implementar protección de vulnerabilidades con nombre (parche virtual) para vulnerabilidades conocidas en el sistema operativo y para aplicaciones que no son del sistema operativo*...", solicitamos amablemente a la CCB dejar este punto como opcional, con el objeto de garantizar la pluralidad de oferentes, toda vez que, de mantenerse, limitaría la oferta a un par de fabricantes específicos (Kaspersky o Trendmicro). **Rpta**.: Ver pregunta 26.
b) En el requerimiento que indica: "...*Capacidad de aislar aplicaciones para separar las aplicaciones que no son de confianza del resto del sistema*...", amablemente solicitamos a la CCB modificar por: "...*Capacidad de bloquear aplicaciones, parar procesos o aislar la maquina comprometida*...", lo anterior teniendo en cuenta que las soluciones de EDR están en capacidad de bloquear y no aislar las aplicaciones, funcionalmente el concepto puede ser similar, pero si se entra al detalle textual puede prestarse para interpretaciones erróneas. **Rpta**.: No se acepta su observación, se mantienen los requerimientos.
c) Respecto del requerimiento que indica: "... *El agente de endpoint debe incluir capacidades de engaño (señuelos) basadas en endpoint diseñadas para exponer a un atacante*...", agradecemos a la CCB ampliar el detalle de lo requerido, qué es lo esperado por la CCB, o generar un ejemplo de caso de uso respecto del requerimiento. **Rpta.:** La solución deberá proporcionar postura de seguridad proactiva al tratar de "engañar" a los atacantes mientras la solución en sus análisis observa y aprende del comportamiento de la amenaza.
d) Respecto del requerimiento que indica: "...*Capacidad de cifrado de disco duro*...", agradecemos a la CCB aclarar el detalle de este requerimiento, lo anterior teniendo en cuenta que típicamente las funcionalidades de cifrado de disco duro no hacen parte de soluciones EDR, este tipo de soluciones por lo general se refieren a herramientas para prevención de fuga de información, que sin duda estaríamos en capacidad de ofertar, pero queremos estar seguro que esto realmente es lo que requiere la CCB en este ítem. **Rpta**.: Se mantienen los requerimientos solicitados.
e) Respecto del requerimiento que incida: "... *El EDR deberá estar en capacidad de hacer uso de la información que genere el Antimalware con el que actualmente cuenta la CCB*...", agradecemos a la CCB indicar cual es la solución actual de Antimalware con la que cuenta, toda vez que es necesario validar las capacidades de integración de la misma con la solución ofertada. **Rpta.:** La solución EDR ofrecida por el proveedor y que se implementará a partir del 2023 deberá ofrecer la solución antimalware.
f) Respecto del requerimiento que incida: "... *El EDR deberá estar en capacidad de hacer uso de la información que genere el Antimalware con el que actualmente cuenta la CCB*...", agradecemos a la CCB dejar este ítem como opcional, toda vez que puede limitar la oferta a la herramienta que actualmente tiene la CCB para protección Antimalware. **Rpta.:** La solución EDR ofrecida por el proveedor y que se implementará a partir del 2023 deberá ofrecer la solución antimalware.
g) Con el objeto de que la CCB adquiera una solución robusta y líder en el segmento de protección EDR y garantizando la pluralidad de oferentes, amablemente proponemos a la entidad incluir funcionalidades como:

- La solución deberá contar con un módulo de investigación guiada que provea mayor contexto al analista más allá del solo alertamiento.
- El fabricante de la solución deberá poder ofrecer además capacidades de antimalware avanzado contemplando todas las posibles capas de analisis (firmas, listas blancas y negras, antiexploit, análisis bajo demanda, reglas de control de acceso y protección contra día cero como mínimo).

- La solución deberá tener la posibilidad de ser administrada por una consola Cloud, así como con una consola on-prem
- La solución deberá aparecer como líder del cuadrante de Gartner en el último cuadrante publicado.
- La solución puede expandirse a una solución del estilo XDR agregando servicios de integración a otros ámbitos como Web y Cloud, esto con el fin de hacer expandir el nivel de capacidades granularmente.
- La solución deberá poder ofrecer una visión de la postura de seguridad, identificando los GAP de mejora, y asimismo, lo pasos para mitigar dichos GAP
- La solución deberá contener un servicio que enumere las campañas que se encuentran atacando actualmente en la región y en el mercado con el fin de poder identificar IOC presentes.

Respuesta
Se mantienen los requerimientos solicitados.

Pregunta 40
Respecto del numeral 3.8 Requerimientos técnicos, en el capítulo asociado a la solución de Cloud Access Security Broker (CASB):
a) Respecto del requerimiento que indica: "... *Permitir habilitar políticas únicas para dispositivos administrados y no administrados, en navegadores o en aplicaciones móviles enriquecidas*...", agradecemos amablemente a la CCB indicar a que se refieren con aplicaciones móviles enriquecidas, lo anterior para mitigar riesgos asociadas a diversas interpretaciones que pueden ir en contravía con lo requerido por la Entidad. **Rpta.:** Es una aplicación web que tiene características del software de aplicación de escritorio.
b) Con el objeto de que la CCB adquiera una solución robusta y líder en el segmento de protección CASB y garantizando la pluralidad de oferentes, amablemente proponemos a la entidad incluir funcionalidades como:

- La solución ofertada deberá ser parte del último cuadrante de líderes de Gartner
- La solución ofertada deberá ser parte del último cuadrante de líderes de IDC
- La solución ofertada deberá ser parte del último cuadrante de líderes de Forrester
- La solución ofertada deberá poder integrarse a una solución de EDR con el fin de otorgar capacidades de XDR
- Para los servicios Cloud corporativos como O365, g-suite, Salesforce, servicenow, como mínimo deberán poder ofrecerse coberturas de integración mediante API
- Deberán poder ofrecerse reglas de control de acceso para dispositivos administrados y no administrados
- Deberá contar con capacidades de UEBA
- Deberá contener un módulo que administre las métricas sobre la actual postura de seguridad vs la industria, y asimismo, poder identificar los puntos de mejora para aumentar dicha postura.
- La solución deberá poder controlar la navegación de los usuarios, las reglas de DLP, la postura de seguridad, la seguridad de los workloads, reglas de whitelisting de aplicaciones y reglas de FIM en una única consola.
- Deberá poder ofrecerse no solo capacidades de SASE sino capacidades de CNAPP

Respuesta
Se mantienen los requerimientos solicitados.

Pregunta 41
Respecto del numeral 3.8 Requerimientos técnicos, en el capítulo asociado a la solución de Data Loss Prevention (DLP):
Con el objeto de que la CCB adquiera una solución robusta y líder en el segmento de protección de fuga de información - DLP y garantizando la pluralidad de oferentes, amablemente proponemos a la entidad incluir funcionalidades como:

- Al no existir actualmente el cuadrante de lideres de Gartner para este tipo de soluciones, se deberá presentar al menos el galardón de Gartner como Peer Insights Choise en 2020
- Deberá otorgar cualidades de clasificación manual, ya sea propias del producto o adquiridas de terceros.
- Las políticas y clasificación de DLP deberán ser administradas desde una única consola central. En el caso de no tenerse esta cualidad deberá incluirse un servicio de personal dedicado a hacer esta sincronización.
- La solución deberá poder recibir IOC de otras fuentes para determinar, no solo si el archivo contiene información sensible, sino si es considerado riesgoso.
- La consola de administración deberá poder ofrecerse como física, virtual y Saas.

Respuesta
Se mantienen los requerimientos solicitados.

Pregunta 42
Solicitamos amablemente a la entidad indicar actualmente cual es la solución IAM que tiene la CCB.

Respuesta
Ver pregunta 17.

Pregunta 43
Para el Firewall de la sede salitre, solicitamos amablemente a la entidad definir si se debe contemplar los servicios de este firewall. Si es así por favor indicar la marca modelo y módulos habilitados.

Respuesta
El detalle de esta información será entregada al proveedor seleccionado. El proveedor seleccionado no operarará o getsionará este componente.

Pregunta 44
Solicitamos amablemente a la entidad indicar para este ítem si las soluciones deben estar implementadas en AWS (definir para cada una de las soluciones solicitadas) o de lo contrario si las soluciones pueden estar implementadas en On-premise o SaaS. Adicionalmente para las soluciones que deben ser implementadas en AWS u Onpremise solicitamos a la entidad indicar si la infraestructura necesaria para la implementación será suministra por CCB o de lo contrario debe ser incluida en la propuesta por el proponente. Así mismo solicitamos a la entidad aclarar si el licenciamiento requerido (licenciamiento de sistemas operativos y bases de datos) también será aprovisionado.

Respuesta
Ver pregunta 14. En la nube que el proveedor seleccionado defina.

Pregunta 45
Solicitamos amablemente a la entidad si en el modelo de autenticación se contempla single site o multisite (definir la cantidad de sitios, si es Nube privada, Nube publica o aplicaciones SaaS).

Respuesta
Nube pública y aplicaciones SaaS.

Pregunta 46
Solicitamos amablemente a la entidad indicar si la infraestructura de los Gateway o conectores será suministrada por la entidad o de lo contrario debe ser contemplada por el proveedor.

Respuesta
El modelo propuesto debe ser SaaS

Pregunta 47
Solicitamos amablemente a la entidad ampliar la información con respecto a este Item confirmando la fecha de inicio y terminación de la prestación del servicio, también el modelo de pago de este servicio ya que por las fechas se tendría que cotizar independiente a las otras tecnologías y el precio del licenciamiento podría variar ya que la implementación seria llevada a cabo en un

Respuesta
La solución debe prestarse a partir del 1 de enero de 2023 por 23 meses. La facturación se iniciará con la activación de la solución.

Pregunta 48
Solicitamos amablemente a la entidad quitar este punto o dejarlo como opcional, ya que este tipo de capacidades es netamente de tecnologías de decepción y solo es integrado en la solución de Symantec lo que limita la pluralidad de tecnologías. Existen diferentes soluciones lideres del mercado con capacidades similares que permitirían obtener una mejor oferta para la CCB manteniendo los estándares de calidad de ciberseguridad.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 49
Solicitamos amablemente a la entidad indicar la versión de los sistemas operativos de servidores a soportar por la herramienta.

Respuesta
Windows 2016 en adelante. Linux Redhat 7 en adelante.

Pregunta 50
Solicitamos amablemente a la entidad indicar la marca y versión de antimalware que actualmente tiene la entidad.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 51
Solicitamos amablemente a la entidad indicar la cantidad de sesiones concurrentes, cantidad de usuarios VPN client, Cantidad de VPN Slte.

Respuesta
VPN Client: 2200. El resto de la información será compartida con el proveedor seleccionado.

Pregunta 52
Solicitamos amablemente a la entidad indicar la tecnología SD-WAN que actualmente utiliza la entidad.

Respuesta
La información será entregada al proveedor seleccionado.

Pregunta 53
Solicitamos amablemente a la entidad indicar la plataforma de logs y reportes que actualmente posee la entidad.

Respuesta
La información será entregada al proveedor seleccionado.

Pregunta 54
Solicitamos a la entidad indicar la cantidad y el listado de aplicaciones en la nube con las que se debe integrar la solución.

Respuesta
La información será entregada al proveedor seleccionado.

Pregunta 55
Solicitamos amablemente a la entidad indicar la cantidad de agentes que se deben considerar para la solución, ya que el ítem de usuarios se encuentra vacío.
Respuesta
2200 usuarios.

Pregunta 56
Solicitamos amablemente a la entidad indicar si la infraestructura requerida para la instalación de la solución será suministrada por la entidad o debe ser suministrada por el proponente y alojada en la CCB.

Respuesta
Ver pregunta 14.

Pregunta 57
Solicitamos amablemente a la entidad indicar el tráfico que debe soportar la solución en Mbps.

Respuesta
Ver pregunta 4.

Pregunta 58
Solicitamos amablemente a la entidad indicar si la solución debe ser implementada en AWS, Apliance On-premise o cloud SaaS.

Respuesta
Ver pregunta 14.

Pregunta 59
Solicitamos amablemente a la entidad que este ítem sea quitado o dejado como opcional ya que las soluciones WAF de uso especifico tienen la capacidad de bloquear o denegar el tráfico por direccionamiento IP o ubicación geográfica.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 60
Solicitamos a la entidad que únicamente se reciban los contratos puesto que en la experiencia pueden entrar contratos en ejecución, y para dichos contratos nos existiría un acta de liquidación.

Respuesta
No se acepta su onservación. Se están solicitando certificaciones de los contratos para demostrar la expericiencia, ahora bien, de conformidad con lo establecido en el numeral 3.3.2 NOTA 2 el aportar los contratos junto con la respectiva acta de recibo y acta de liquidación es opcional, pues estos documentos puede reemplazar una certificación.

Pregunta 61
Solicitamos amablemente a la entidad poder realizar una reunión de entendimiento y observaciones con todos los proponentes, con el fin de aclarar algunos puntos del alcance del proyecto.

Respuesta
Se mantienen los términos de la invitación.

Recomendaciones

- Solicitamos atentamente a la entidad contemplar que las soluciones propuestas no sean de la misma marca ya que por recomendaciones de seguridad si se presenta una brecha de seguridad en dicha marca esto podría afectar todo el ecosistema de tecnologías de seguridad que posee la entidad.
- La solución de DLP debe permitir descubrir y clasificar la información de forma automática, con el fin de que apoye en las políticas y en la creación de políticas de Fuga de información.
- En caso que la CCB quiera mantener las soluciones actuales enviar una carta de la apertura de precios a los fabricantes para que los proponentes puedan competir en igualdad de condiciones.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 62
Con relación al numeral 3.3.3 de la Convocatoria, es de nuestro entendimiento, que el equipo de trabajo será remoto y se ejecutará los servicios desde la sede del propoponente. Agradecemos confirmar.

Respuesta
El equipo de trabajo podrá laborar de forma remota y deberá atender las sesiones de trabajo presnecial que el supervisor de contrato solicite.

Pregunta 63
Con relación al numeral 5.1 de la Convocatoria, en aras de preservar el equilibrio económico del contrato y teniendo en cuenta que esto servicios son suscripciones anuales con una alta posibilidad de variaciones en la TRM, solicitamos atentamente a la Cámara de Comercio de Bogotá que sea posible presentar la

oferta en dólares americanos que se propone sea cancelado a la TRM del día de radicación de la factura mensual correspondiente.

Respuesta
No se acepta su observación.

Pregunta 64
Con relación al numeral 1.6 de la Convocatoria, con el fin de realizar un adeacuado dimensionamiento de esfuerzos de implementación y libreación de nuevas configuraciones producto de las migraciones que la CCB realizará, solicitamos atentamente sea llegado el roadmap de dicha migración, sin detalle pero teniendo en cuenta por lo menos anualmente qué procentaje se espera sean migrados.

Respuesta
La fecha estimada de fin de migración es 30 de abril de 2022.

Pregunta 65
Con relación al numeral 2.1 de la Convocatoria, es de nuestro entendimiento que la CCB está solicitando de parte de proponente no solo los servicios de configruación, implementación, puesta en marcha, administración y operación, si no que tambien se incluyen los productos enumerados en el numeral 3. ESPECIFICACIONES TÉCNICAS, sub numeral 3.8 Requerimientos Técnicos.

Respuesta
La CCB está solicitando un servicio que debe contemplar las soluciones tecnológicas que soporte las funcionalidades descritas en el numeral 3.8. No se contempla la adquisición de licenciamiento por parte de la CCB.

Pregunta 66
Con relación al numeral 3.8 de la Convocatoria, atentamente solicitamos aclarar cual es el antimalware de la CCB.

Respuesta
Ver preguntas 29 y 39.

Pregunta 68
Con relación al numeral 3.8 de la Convocatoria, atentamente solicitamos que debido a que no se pueden predecir por parte del proveedor los precios futuros de una solución, este item pueda ser presentado como "*sujeto a cambios en los precios de lista del fabricante*" y sean detallados en otro aparte o item separado del formulario económico.

Respuesta
No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 69
Con relación al numeral 3.10 de la Convocatoria, atentamente solcitamos a la CCB que las hojas de vida de los perfiles solicitados en este numeral, sean presentados después del acta de inicio del contrato, entendiendo que el proponente se está comprometiendo con el cumplimiento en la ejeución de los servicios mediante carta de aceptación de la propuesta.

Respuesta
El numeral 3.10 del Anexo 2 -Aceptación especificaciones técnicas- hace referencia a los analistas de operación y conforme a la NOTA 2 la CCB cuando lo estime conveniente, podrá solicitar las hojas de vida del equipo de trabajo Rol Analista de Operaciones, por consiguiente, no es necesario que presenten las hojas de vida de quienes desarrollarán el mencionado rol con la propuesta.

Pregunta 70
Con relación al numeral 3.11 de la Convocatoria, entendemos que se trata de un proceso de entregas paulatinas que debe ser propuesto para aprobación mediante comité de cambios de la CCB, por lo tanto sugerimos a la entidad, sea considerada más la metdología para el ingreso de cada uno de estos servicios a la operación.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 71
Se solicita a la entidad tener en cuenta que los fabricantes de este tipo de soluciones no entregan precios a futuro y segundo estos precios son ofrecidos en moneda extranjera, como lo es dolares americanos, no siendo posible establecer un valor del costo de las licencias requeridas. Tener en cuenta los posibles incrementos que pueden sufrir estos costos o eliminar este requerimiento del proyecto y solicitarlo de nuevo en una fecha cercana a enero 1 de 2023.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 72
Se solicita tener en cuenta que las organizaciones llevan muy poco tiempo o están en proceso de migración de su plataforma a la nube, razón por la cual no se contemplaban dentro de sus contratos, adqusición de plataformas en la nube y de igual manera las soluciones una vez implementadas, la operación y administración es la misma como la de soluciones on-premise. Con base en lo anterior, se solicita a la entidad permitir a los proponentes acreditar experiencia en la implementación o prestación de servicios de Ciberseguridad "El proponente deberá acreditar experiencia mediante la presentación de mínimo cuatro (4) certificaciones de contratos ejecutados y/o en ejecución a partir del 1 de enero de 2018 cuya sumatoria debe ser igual o superior a $ 4.800.000.000 antes de IVA, en las cuales debe constar como mínimo la prestación de servicios de ciberseguridad, con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información. Respecto de los contratos en ejecución, estos deben tener mínimo un año de ejecución e indiciar en la certificación el monto facturado antes de IVA a octubre 2021.

Respuesta
No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 73
Se solicita que esta persona tenga experiencia en gerencia de proyectos de Ciberseguridad de la siguiente manera "*a) Un (1) Líder de Cuenta: o Profesional universitario en ingeniería de sistemas o afines que tenga como mínimo dos (2) años de experiencia en gerencia de proyectos de Ciberseguridad*".

Respuesta
No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 74
Se solicita a la entidad tener en cuenta que una vez la solución es desplegada en nube, su administración y operación es similar a la de las soluciones tradicionales y muchos fabricantes no generan certificaciones específicas como implementador de firewall como servicio (FWasS), aceptar las certificaciones como implementador o administrador de la plataforma de firewall, permitiendo una mayor pluralidad de oferentes.

Respuesta
No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 75
Se solicita que esta persona tenga experiencia en coordinador de operaciones de Ciberseguridad , de la siguiente manera "c*)Coordinador de Operaciones Profesional universitario en ingeniería de sistemas o afines que tenga como mínimo dos (2) años de experiencia en gerencia de proyectos de Ciberseguridad*".

Respuesta
No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 76
Se solicita a la entidad entregar un mayor detalle de el firewall instalado en la sede salitre, modelo, marca, contrato de soporte vigente etc., esto con el fin de poder dimensionar los servicios y recursos para asumir esta operación y administración.

Respuesta.
El Firewall actualmente instalado en la sede salitre no se reemplazará, esto debe considerarse para la solución propuesta. Esto no implica que el proveedor seleccionado vaya a asumir la administración y operación de este firewall.

Pregunta 77
Se solicita a la entidad entregar un mayor detalle en lo referente a la transferencia de conocimiento, en cuanto a los contenidos, cantidad de personas, horas etc.

Respuesta
Esta información será acordada entre el proveedor seleccionado y la CCB.

Pregunta 78
Se solicita a la entidad teniendo en cuenta que lo requerido es el suministro, operación y administración de soluciones de seguridad desplegadas en nube, dentro de las cuales no se está solicitando servicios ni de SIEM o SOC, eliminar estos requerimientos, los cuales son propios de este tipo de servicio. Adicionalmente al solicitar estas capacidades y ya tenerlas dentro de un servicio de SOC, lo que ocasionaria es sobrecostos en los dos proyectos.

Respuesta
No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 79
Se solicita a la entidad tener en cuenta que la mayoría de los fabricantes de soluciones de EDR no entregan esta funcionalidad y solo es ofrecida por dos fabricantes, no permitiendo la participación de

marcas líderes en el mercado y que cumplen con las otras solicitadas, se solicita eliminar esta funcionalidad.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 80
Se solicita a la entidad entregar un detalle de los diferentes protocolos , servicios, Apis con que cuentan las soluciones de logs y reportes de la Camara de Comercio, para poder validar su integración.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 81
Se solicita a la entidad entregar un mayor detalle de los vectores de correo y red, que permita dimensionar la solución:

- Aplicación de correo usada actualmente (nube on premise) fabricante. **Rpta.:** Outlook
- Número de buzones de correo. **Rpta.:** 2200
- Número de estaciones de trabajo. **Rpta.:** 2200
- Repositorios en Nube o On premise (cantidad, fabricante, etc). **Rpta.:** Nube

Pregunta 82
Solicitamos respetuosamente nos compartan el alcance de este requerimiento: "*La solución debe implementar protección de vulnerabilidades con nombre (parche virtual) para vulnerabilidades conocidas en el sistema opera*" y la mención de (parche virtual) dentro del mismo. (Funcionalidad provista por integrador).

Respuesta
Ver pregunta 26.

Pregunta 83
Solicitamos respetuosamente se indique el alcance y necesidad de este requerimiento: "*El agente de endoints debe incluir capacidades de engaño (señuelos) basadas en endoints diseñadas para exponer a un atacante*" dentro de la solucione de EDR. Si es un elemento deseable y/o mandatorio.

Respuesta
Los requerimientos técnicos son requerimientos mínimos habilitantes. Ver numeral 3.3. de la invitación a proponer.

Pregunta 84
Solicitamos respetuosamente, su apoyo compartiendo si esta funcionalidad: "*Capacidad de cifrado de disco duro*" es un elemento deseable y/o mandatorio dentro de la evaluación. (Funcionalidad provista por integrador).

Respuesta
Los requerimientos técnicos son requerimientos mínimos habilitantes. Ver numeral 3.3. de la invitación a proponer.

Pregunta 85
Solicitamos respetuosamente, se aclaren los siguientes puntos sobre este requerimiento "*El EDR deberá estar en capacidad de hacer uso de la información que genere el Antimalware con el que actualmente cuenta la CCB*":

- Por favor compartir la información del Antimalware utilizado actualmente por la CCB.
- Por favor compartir detalles sobre el nivel de integración y alcance del uso de la información.
- Por favor aclarar si este es un requerimiento de integración directo con la solucion de EDR y/o la solucion de SIEM. (Integrador).

Respuesta
Ver preguntas 29 y 39.

Pregunta 86
Solicitamos respetuosamente a la CCB, se comparta el nivel calificación de acuerdo al el cumplimiento de los requerimientos inscritos en el numeral 3.8, para la sección EDR. Crowdstrike cuenta con un nivel de cumplimiento del 97% y un 3% en donde el cumplimiento se realiza de formas alternas, con integraciones y/o otras aplicaciones. Agradecemos la claridad en la evaluación.

Respuesta
Los requerimientos técnicos son requerimientos mínimos habilitantes. Ver numeral 3.3. de la invitación a proponer.

Pregunta 87
Por favor aclarar si la CCB requiere una solución que permita validar los requerimientos mínimos de seguridad de los dispositivos que no son corporativos antes de permitir que se conectan a la red. A esta solución se le conoce como Network Access Control.

Respuesta
El proveedor debe presentar la solución tecnológica que cumpla con los requerimientos técnicos solicitados.

Pregunta 88
¿La solución debe realizar autenticación de dos factores en servidores, estaciones de trabajo, Firewalls, VPNS y aplicaciones públicas de la CCB?.

Respuesta
La solución debe integrarse con el Directorio Activo de la CCB.

Pregunta 89
Sugerimos a la entidad tener en cuenta en la calificación de los oferentes el análisis de Gartner Peer Insights en donde se evalúan las diferentes soluciones de TI de forma confiable y se puede visualizar. Esto con el fin de que la CCB contrate los servicios con las mejores soluciones posicionadas.

Respuesta
No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 90
¿La solución debe proteger de ataques y dar respuesta en tiempo real para evitar ataques de ramsonware o de día cero y cifrado de datos sin requerir herramientas complementarias de antimalware basado en firmas y así evitar incidentes en las estaciones finales?.

Respuesta
La solución debe cumplir con los requerimientos técnicos solicitados.

Pregunta 91
Las soluciones de EDR del mercado no incluyen las capacidades de engaño (señuelos). Por favor aclarar si la CCB requiere incluir una tecnología de engaño adicional para cumplir con este requerimiento.

Respuesta
El proveedor debe presentar la solución tecnológica que cumpla con los requerimientos técnicos solicitados.

Pregunta 92
Las soluciones de EDR del mercado no incluyen la capacidad de cifrado de disco. Por favor indicar si la CCB requiere incluir una solución adicional para cumplir con este requerimiento.

Respuesta
El proveedor debe presentar la solución tecnológica que cumpla con los requerimientos técnicos solicitados.

Pregunta 93
Las soluciones de EDR del mercado incluyen funcionalidades de antimalware por lo cual no requiere hacer uso de la información que genere el Antimalware actual de la CCB. ¿Es correcta nuestra apreciación?.

Respuesta
Ver pregunta 29 y 39.

Pregunta 94
Las soluciones de CASB del mercado no incluyen las funcionalidades de SandBox. ¿Por favor indicar si la CCB desea incluir como parte del servicio una solución adicional de sandbox para detectar actividad anómala y archivos sospechosos en las estaciones de trabajo?

Respuesta
El proveedor debe presentar la solución tecnológica que cumpla con los requerimientos técnicos solicitados.

Pregunta 95
Las soluciones de CASB no realizan remediación post infección. Esta característica es propia de las soluciones de EDR. Agradecemos a la entidad eliminar este requerimiento de este capitulo de CASB.

Respuesta
El proveedor debe presentar la solución tecnológica que cumpla con los requerimientos técnicos solicitados.

Pregunta 96
¿La funcionalidad de DLP puede ser provista por diferentes soluciones en cada vector que se contemplaría dentro del servicio?

Respuesta
El proveedor debe presentar la solución tecnológica que cumpla con los requerimientos técnicos solicitados.

Pregunta 97
Las soluciones de WAF del mercado incluyen características de mitigación de falsos positivos, protección de ataques conocidos y desconocidos, así como el escaneo de vulnerabilidades sobre las aplicaciones y la contención de ataques que modifiquen la apariencia de las aplicaciones (ataques de reputación). Por favor aclarar si el servicio propuesto deberá incluir estas funcionalidades.

Respuesta
El proveedor debe presentar la solución tecnológica que cumpla con los requerimientos técnicos solicitados.

Pregunta 98
Solicitamos amablemente a la entidad, confirmar si nuestro entendimiento es correcto, en el modelo de la oferta económica en el item de servicio de implementación, ¿es un único valor por la implementación de todas las soluciones y se pagara en un único pago.? Toda vez que en el formato dice que NO aplica valor mensual.

Respuesta
De acuerdo.

Pregunta 99
En el ítem de servicios de EDR, se entiende que el servicio empieza a prestarse a partir de enero de 2023, pero el pago mensual lo realizara la CCB una vez se legalice contractualmente la oferta. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
Lo correspondiente al EDR se comenzará a facturar una vez se active el servicio.

Pregunta 100
En el tercer item donde aparecen todas las tecnologías, la cantidad de meses es de 35, pero en el plazo de ejecución es de 3 años. Por favor aclarar la vigencia de los servicios.

Respuesta
Tres (3) años: 1 mes de implementación y 35 de operación y gestión.

Pregunta 101
Se solicita a la entidad confirmar si se realiza facturación mes a mes o es una única factura con pagos mensuales.

Respuesta
La CCB pagará al CONTRATISTA de manera mensual el valor del contrato por los servicio efectivamente prestados previo recibo a satisfacción por parte del Supervisor del contrato y de los entregables.

Pregunta 102
Se solicita a la entidad aclarar si en "Valor Total IVA" se refiere al valor del IVA mensual, o al valor total del IVA o al Valor total de la oferta con IVA incluido.

Respuesta
En el anexo 4 oferta económica el valor total IVA se refiere al valor total del servicio antes de IVA

OBJETO	Cantidad	Valor mensual antes de IVA	Valor Total antes de IVA

se adjunta anexo 4 oferta económica.

Pregunta 103
Sugerimos a la CCB solicitar acompañamiento de las fábricas propuestas para el servicio en la fase del diseño e implementación con el fin de garantizar los requerimientos del modelo Zero Trust.

Respuesta
Se mantienen los requisitos establecidos en la invitación. El proveedor podrá ofrecer los valores agregados que considere para la prestación del servicio.

Pregunta 104
Sugerimos a la CCB incluir capacitaciones dictadas directamente por las fábricas propuestas para el servicio con el fin de garantizar un mejor conocimiento sobre las soluciones y correcta evaluación del servicio post-implementación

Respuesta
Se mantienen los requisitos establecidos en la invitación. El proveedor podrá ofrecer los valores agregados que considere para la prestación del servicio.

Pregunta 105
Los modelos Zero Trust garantizan la verificación de autenticidad para cada dispositivo y usuarios independientemente desde donde se quiera conectar. Para obtener esto se sugiere a la CCB que las soluciones propuestas en el servicio sean en su mayoría del mismo fabricante para tener mayor integración, visibilidad, facilidad en administración, y respuesta automatizada en el servicio.

Respuesta
Se mantienen los requisitos establecidos en la invitación.

Pregunta 106
Solicitamos amablemente a la entidad, que, dentro de los documentos solicitados, el oferente presente la certificación directa del fabricante en su nivel más alto, en al menos en una de las tecnologías requeridas dentro de la presente invitación.

Respuesta
Se mantienen los requisitos establecidos en la invitación. El proveedor podrá ofrecer los valores agregados que considere para la prestación del servicio.

Pregunta 107

"El proponente deberá acreditar experiencia mediante la presentación de mínimo cuatro (4) certificaciones de contratos ejecutados y/o en ejecución a partir del 1 de enero de 2018 cuya sumatoria debe ser igual o superior a $ 4.800.000.000 antes de IVA, en las cuales debe constar como mínimo la prestación de servicios de ciberseguridad para plataformas tecnológicas en la nube con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información." Solicitamos amablemente a la entidad, considerar la presentación de certificaciones de experiencia de plataformas en nube y/o en On premise. Toda vez que el contenido de la presente invitación (como se detalla en el Objeto) tiene componentes híbridos (on premises y en la nube).

Respuesta

Se mantienen los requerimientos solicitados.

Pregunta 108

"El proponente deberá acreditar experiencia mediante la presentación de mínimo cuatro (4) certificaciones de contratos ejecutados y/o en ejecución a partir del 1 de enero de 2018 cuya sumatoria debe ser igual o superior a $ 4.800.000.000 antes de IVA, en las cuales debe constar como mínimo la prestación de servicios de ciberseguridad para plataformas tecnológicas en la nube con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información." Es de nuestro entendimiento, que al mencionar que como mínimo se deben presentar certificaciones en servicios de ciberseguridad en plataformas tecnológicas, incluye también soluciones en seguridad informática y de la información, que protegen la confidencialidad, integridad y disponibilidad de la información. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta

En las certificaciones presentadas debe constar como mínimo la prestación de servicios de ciberseguridad para plataformas tecnológicas en la nube con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información, por consiguiente, si los servicios que se presentan en la certificación cumplen con la acreditación de la experiencia solicitada se tendrán en cuenta, sin embargo, será responsabilidad del equipo evaluador valorar cada una de las certificaciones aportadas por el proponente.

Pregunta 109

Se solicita por favor ampliar el plazo de la fecha de presentación de propuesta.

Respuesta

Se acepta su observación, el plazo se amplo mediante adenda No. 1

Pregunta 110

Determinar por favor si el requerimiento de experiencia es Mínimo cuatro (4) ó Máximo cuatro (4) Certificaciones.

Respuesta

Ver numeral 3.3.2. de la invitación., es mínimo cuatro (4).

Pregunta 111

Se solicita por favor incluir dentro del requerimiento de la experiencia del proponente la modalidad híbrida (On Premise o en la Nube), esto acorde al objeto de la Convocatoria.

Respuesta
No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 112
Se solicita revisar viabilidad para conformación de uniones temporales ó consorcios.

Respuesta
La CCB le informa que no se permite la participación de consorcios, uniones temporales o cualquiera de las formas de proponente plural para esta convocatoria de conformidad con lo establecido en su numeral 3.1.1 CAPACIDAD PARA PRESENTAR OFERTAS.

Pregunta 113
Por favor adicionar al siguiente enunciado del numeral 6.3 de la Convocatoria la palabra "del oferente", quedando así: "*Corresponde a la tenencia de un certificado de gestión de seguridad de la información ISO 27001:2013 del oferente, Vigente, el cual debe ser presentado junto con la propuesta*...".

Respuesta
No se acepta su observación, se mantienen los requisitos solicitados.

Pregunta 114
Agradecemos poder aclarar la cantidad de usuarios que serán objeto de la solución de DATA LOSS PREVENTION (DLP).

Respuesta
2200 usuarios.

Pregunta 115
Agradecemos aclarar para la solución CASB, qué tecnologías en la nube tiene la entidad para verificar y dimensionar el cumplimiento con estos servicios en nube.

Respuesta
Ver pregunta 10.

Pregunta 116
Por favor relacionar el discriminado de servidores Windows y Linux, así como estaciones de trabajo con su respectivo sistema operativo, lo anterior para determinar la compatibilidad de las soluciones que se incluirán en la oferta.

Respuesta
Esta información será entregada al proveedor seleccionado.

Pregunta 117
Se solicita amablemente a la entidad exigir que la solución de Endpoint Detection and Response (EDR) se encuentre dentro del cuadrante mágico de Gartner como LÍDER, esto con el fin de que la entidad pueda seleccionar soluciones robustas y debidamente validadas en el mercado teniendo en cuenta el objeto de la CCB.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 118
Se solicita amablemente a la entidad exigir que la solución de Cloud Access Security Broker (CASB) se encuentre dentro del cuadrante mágico de Gartner como LÍDER, esto con el fin de que la entidad pueda seleccionar soluciones robustas y debidamente validadas en el mercado teniendo en cuenta el objeto de la CCB.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 119
Sobre la solución de Autenticación de Usuarios descrita en la página 33, se solicita amablemente a la entidad indicar cuántas y cuáles aplicaciones debe tener esta solución, y confirmar si estas aplicaciones soportan SAML o OAUTH y si el directorio activo esta On Premise o es Nube.

Respuesta
El Directorio activo es en nube. El resto de la información será compartida con el proveedor seleccionado.

Pregunta 120
Se solicita amablemente a la entidad aclarar desde dónde se loguean los usuarios, desde la consola de su máquina y allí solicitar un segundo factor o cuando dice que llevan su dispositivo entonces sería al dominio / la intranet. Adicional aclarar en qué punto se requiere pedir el doble factor, en el PC o en la VPN, intranet, dominio o con un portal de acceso que puede proveer la solución y a través de este se vayan todos?

Respuesta
La solución debe soportar distintos escenarios.

Pregunta 121
Se solicita amablemente a la entidad aclarar si para DLP la entidad requiere que desde el vector de protección de red se incluyan funcionalidades de Descubrimiento, Monitoreo y Prevención
Se solicita amablemente a la entidad aclarar si el tráfico de las aplicaciones es de 15TB para el servicio de Web Application Firewalls (WAF), así mismo confirmar si son requeridas las funcionalidades de Protección contra Denegación del Servicio.

Respuesta
Ver pregunta 4. La solución deberá cumplir con los requisitos solicitados.

Pregunta 122
Se solicita amablemente a la entidad aclarar cuántos usuarios VPN se espera que soporte la solución Firewall como servicio (FWasS)

Respuesta
2200

Pregunta 123
Se solicita amablemente a la entidad, indicar el nombre de la solución de Eventos de Seguridad (SIEM) y Administración de Identidad (IAM), que actualmente utiliza CCB.

Respuesta
Directorio Activo. La información del SIEM será entregada al proveedor seleccionado.

Pregunta 124
Se solicita muy amablemente a la entidad modificar la experiencia requerida, "*en las cuales debe constar como mínimo la prestación de servicios de ciberseguridad para plataformas tecnológicas en la nube con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información*." Para que sea acorde con el objeto del contrato, modificar la experiencia solicitada de la siguiente manera:

El proponente deberá acreditar experiencia mediante la presentación de mínimo cuatro (4) certificaciones de contratos ejecutados y/o en ejecución a partir del 1 de enero de 2018 cuya sumatoria debe ser igual o superior a $ 4.800.000.000 antes de IVA, en las cuales debe constar como mínimo la prestación de servicios de ciberseguridad para plataformas tecnológicas en modalidad híbrida (On premises y en la nube) con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información.

Respuesta
No se acepta su onservación, se mantienen los requisitos solicitados.

Pregunta 125
De acuerdo al numeral 3.3 Solución Tecnológica: "*La solución tecnológica con la que se prestará el servicio deberá estar aprovisionada en la nube de AWS bajo el modelo de servicio*.", se solicita muy amablemente a la entidad aclarar si el aprovisionamiento de los recursos de CPU, RAM y Storage necesarios para el despliegue de las soluciones ubicadas en AWS lo entregaría la entidad.

Respuesta
Ver pregunta 3.

Pregunta 126
De acuerdo al numeral 3.8 Requerimientos técnico, Endpoint Detection and Response (EDR) "*El fabricante debe pertenecer al cuadrante mágico de Gartner para para plataformas de protección de endpoints*.", se solicita muy amablemente a la entidad que para la solución de EDR se tenga en cuenta Gartner peer insight, ya que Gartner desde el año 2020 no está realizando los cuadrantes mencionados, el proceso actual se trata de evaluar las diferentes soluciones mediante peer insight y se asignan puntajes a cada tipo de solución.

Respuesta
No se acepta su observación, se mantienen los requerimientos solicitados.

Pregunta 127
De acuerdo al numeral 2.1 Premisas: "*El Firewall actualmente instalado en la sede salitre no se reemplazará, esto debe considerarse para la solución propuesta*.", solicitamos amablemente a la entidad aclarar cuál es el modelo de Firewall actual en la sede Salitre.

Respuesta
Palo Alto.

Pregunta 128
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios: "*Habilitar el acceso para los usuarios ya sean invitados, inalámbricos y conectados localmente o con cable, considerando los principios de ZeroTrust y registrando la información del usuario, dispositivo y la ubicación*.", es de nuestro entendimiento que la solución de autenticación de usuarios se debe integrar con la solución inalámbrica actual para autenticación a través del protocolo estándar RADIUS. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
RADIUS y Directorio activo.

Pregunta 129
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios: "*Habilitar el acceso para los usuarios ya sean invitados, inalámbricos y conectados localmente o con cable, considerando los principios de ZeroTrust y registrando la información del usuario, dispositivo y la ubicación*.", solicitamos amablemente a la entidad aclarar cuáles son las marcas de la solución inalámbrica y switches que se tienen actualmente.

Respuesta
Switches: Aruba. Solución inalámbrica: Aruba y Ruckus.

Pregunta 130
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios: "*Habilitar el acceso para los usuarios ya sean invitados, inalámbricos y conectados localmente o con cable, considerando los principios de ZeroTrust y registrando la información del usuario, dispositivo y la ubicación*.", es de nuestro entendimiento que el tipo de autenticación que se requiere para conexiones por cable es 802.1x, con el fin de validar y autorizar los clientes o dispositivos que se conectan a través de los switches. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
De acuerdo.

Pregunta 131
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios: "*Asegurar el acceso con el uso de autenticación de dos factores y administración de certificados*.", es de nuestro entendimiento que la entidad requiere autenticación de doble factor mediante tokens basados en software con licenciamiento vitalicio. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
Se deben considerar múltiples posibilidades. Debe considerarse que la contratación es bajo Modelo SaaS y la CCB no adquirirá liceciamiento.

Pregunta 132
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios: "*Asegurar el acceso con el uso de autenticación de dos factores y administración de certificados*." Solicitamos amablemente a la entidad aclarar si la solución de autenticación de usuarios debe ser autoridad de certificación para emisión y revocación de certificados de tipo interno.

Respuesta
No está dentro del alcance.

Pregunta 133
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios: "*Autenticar tanto a los usuarios como a las máquinas, incluyendo el escenario en donde los colaboradores traen sus propios dispositivos personales a la red empresarial.*", solicitamos amablemente a la entidad aclarar si se está requiriendo una solución de control de acceso a la red para revisar la postura de seguridad de las máquinas que se conectan y garantizar que los dispositivos no sean vulnerables.

Respuesta
Sí se requiere

Pregunta 134
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios: "*Integrarse con el Directorio Activo de la CCB*.", solicitamos amablemente a la entidad aclarar la versión de sistema operativo del servidor de Directorio Activo.

Respuesta
Windows 2016 y 2019

Pregunta 135
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios "*Asegurar el acceso con el uso de autenticación de dos factores y administración de certificados*." Es de nuestro entendimiento que la solución de autenticación de usuarios debe permitir autenticación de doble factor para equipos de usuario, con el fin de robustecer el acceso de los usuarios a sus máquinas y evitar suplantación de identidad. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
La solución debe cumplir con lo solicitado en el numeral 3.8.

Pregunta 136
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios: "*Asegurar el acceso con el uso de autenticación de dos factores y administración de certificados*." Es de nuestro entendimiento que la solución de autenticación de usuarios debe integrarse con plataformas de seguridad y red para permitir autenticación de doble factor a usuarios administradores y de esta forma evitar accesos no autorizados a las herramientas de la CCB. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
El alcance es a todos los usuarios.

Pregunta 137
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios: "*Asegurar el acceso con el uso de autenticación de dos factores y administración de certificados*." Es de nuestro entendimiento que la solución de autenticación de usuarios debe permitir autenticación de doble factor para conexiones VPN cliente-sitio y acceso a aplicaciones web. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
La solución debe estar integrada al Directorio Activo.

Pregunta 138
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios: "*Asegurar el acceso con el uso de autenticación de dos factores y administración de certificados*." Es de nuestro entendimiento que la solución de autenticación de usuarios debe administrar certificados utilizados para VPNs sitio a sitio, con el fin de robustecer la autenticación simple por pre – shared key. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
No es requerido

Pregunta 139
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios Solicitamos amablemente a la entidad incluir el siguiente requerimiento: "*La solución de autenticación de usuarios debe encontrarse en los Peer Insights de Gartner*." Lo anterior con el fin de considerar una buena experiencia con la solución en otras empresas y contar con un buen posicionamiento en el mercado.

Respuesta
No se acepta su observación, se mantienen los requerimientos solicitados.

Pregunta 140
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios, es de nuestro entendimiento que los recursos de cómputo necesarios para el despliegue de la solución de autenticación de usuarios en AWS serán responsabilidad de la CCB, ya que se deben implementar en la suscripción de la entidad, por lo cual esta facturación no hace parte del proponente. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
Ver pregunta 3.

Pregunta 141
De acuerdo al numeral 3.8 Requerimientos Técnicos, autenticación de usuarios, solicitamos a la entidad amablemente aclarar cuál es la retención de logs necesaria para la solución de autenticación de usuarios.

Respuesta
Ver numeral 3.3. de la invitación.

Pregunta 142
De acuerdo al numeral 3.8 Requerimientos Técnicos, Endpoint Detection and Response (EDR): "*La solución debe proteger contra malware conocido y desconocido sin depender de actualizaciones diarias de agentes / definiciones*.", es de nuestro entendimiento que la solución EDR debe actuar a nivel de kernel para mitigar en tiempo real ataques tipo ransomware y evitar cifrado de datos. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 143

De acuerdo al numeral 3.8 Requerimientos Técnicos, Endpoint Detection and Response (EDR): "*La solución debe almacenar los datos del indicador de compromiso (IOC) / indicador de ataque (IOA) en una ubicación central para un análisis retrospectivo*." Es de nuestro entendimiento que los eventos considerados como sospechosos o maliciosos deben ser listados en el marco de ataques MITRE para investigación forense. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta

La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 144

De acuerdo al numeral 3.8 Requerimientos Técnicos, Endpoint Detection and Response (EDR): "*La solución debe permitir que los falsos positivos sean suprimidos / ignorados desde la consola de administración sin excluir todas las técnicas de protección, por ejemplo, suprimir la detección de archivos, pero aún monitorear el comportamiento*." Es de nuestro entendimiento que la solución EDR debe soportar machine learning para mitigar falsos positivos y frenar la pre-ejecución de malware. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta

La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 145

De acuerdo al numeral 3.8 Requerimientos Técnicos, Endpoint Detection and Response (EDR): "*Debe incluir el acceso a sandbox en la nube.*", solicitamos amablemente a la entidad eliminar este requerimiento, ya que el objetivo de tener una solución EDR es realizar analítica dinámica de amenazas, no estática como la hace una solución de Sandbox. Lo anterior hace que una solución EDR sea mucho más preventiva y eficiente que una solución de Sandbox.

Respuesta

La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 146

De acuerdo al numeral 3.8 Requerimientos Técnicos, Endpoint Detection and Response (EDR): "*El agente de endpoint debe incluir capacidades de engaño (señuelos) basadas en endpoint diseñadas para exponer a un atacante*.", solicitamos amablemente a la entidad aclarar si se requiere una solución de Deception o tecnología de engaño, ya que este requerimiento no hace parte de las funcionalidades de un EDR.

Respuesta

La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 147

De acuerdo al numeral 3.8 Requerimientos Técnicos, Endpoint Detection and Response (EDR): "*Capacidad de cifrado de disco duro.*", solicitamos amablemente a la entidad eliminar este requerimiento, ya que esta funcionalidad no hace parte de una solución EDR y se encuentra presente como característica nativa del sistema operativo Windows, así como en Linux hay varias herramientas gratuitas que ofrecen esta funcionalidad, por lo cual se puede utilizar sin licenciamiento que implique costos adicionales.

Respuesta
No se acepta su observación, se mantienen los requerimientos solicitados.

Pregunta 148
De acuerdo al numeral 3.8 Requerimientos Técnicos, Endpoint Detection and Response (EDR): "*El EDR deberá estar en capacidad de hacer uso de la información que genere el Antimalware con el que actualmente cuenta la CCB.*", solicitamos amablemente a la entidad eliminar este requerimiento, ya que la solución EDR realiza un análisis en tiempo real basado en kernel utilizando machine learning, por lo cual es más óptimo y no requiere utilizar la información del antimalware actual que realiza un análisis basado en firmas únicamente.

Respuesta
Ver pregunta 29 y 39.

Pregunta 149
De acuerdo al numeral 3.8 Requerimientos Técnicos, Endpoint Detection and Response (EDR): "*El EDR deberá estar en capacidad de hacer uso de la información que genere el Antimalware con el que actualmente cuenta la CCB*.", solicitamos amablemente a la entidad aclarar si el uso de la información que genere el antimalware actual puede ser utilizada de forma manual por el proveedor que ofrezca el servicio.

Respuesta
Ver pregunta 29 y 39.

Pregunta 150
De acuerdo al numeral 3.8 Requerimientos Técnicos, Endpoint Detection and Response (EDR): "*El EDR deberá estar en capacidad de hacer uso de la información que genere el Antimalware con el que actualmente cuenta la CCB.*" Es de nuestro entendimiento que el EDR puede utilizar la información del antimalware actual a través de la correlación de la solución SIEM que se va a tener en el servicio de SOC. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
Ver pregunta 29 y 39.

Pregunta 151
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Endpoint Detection and Response (EDR). Es de nuestro entendimiento que la solución EDR debe manejar respuesta automatizada y orquestada en tiempo real para evitar que los ataques se materialicen en los puntos finales. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 152
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Endpoint Detection and Response (EDR): "*La solución debe continuar recopilando datos de eventos sospechosos cuando el dispositivo de punto final administrado está fuera de la red corporativa*." Es de nuestro entendimiento que para cumplir este

requerimiento la gestión de la solución EDR debe ser desde la nube del fabricante. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
Ver pregunta 3.

Pregunta 153
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Endpoint Detection and Response (EDR). Solicitamos a la entidad amablemente aclarar cuál es la retención de logs necesaria para la solución de EDR.

Respuesta
Ver numeral 3.3.

Pregunta 154
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Firewall como servicio (FWasS): "*Cantidad de tráfico en AWS: 15 TB*", solicitamos amablemente a la entidad aclarar si la cantidad de trafico de 15 TB es mensual.

Respuesta
Sí

Pregunta 155
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Firewall como servicio (FWasS). Es de nuestro entendimiento que los recursos de cómputo necesarios para el despliegue de los NGFWs virtualizados en AWS serán responsabilidad de la CCB, ya que se deben implementar en la suscripción de la entidad, por lo cual esta facturación no hace parte del proponente. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
Ver pregunta 3.

Pregunta 156
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Firewall como servicio (FWasS). Solicitamos a la entidad amablemente aclarar cuál es la retención de logs necesaria para la solución de FWasS.

Respuesta
Ver numeral 3.3.

Pregunta 157
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Cloud Access Security Broker (CASB): "*Monitorear la actividad realizada sobre las aplicaciones y servicios en la nube. En concreto, debe detectar actividad anómala y archivos sospechosos. Debe proporcionar mecanismos que mitiguen las amenazas e impidan la propagación de malware, como entornos sandbox para análisis dinámico o implementando flujos de cuarentena para los ficheros sospechosos*." Es de nuestro entendimiento que la funcionalidad de Sandbox se puede ofrecer en los puntos finales para que la cuarentena se pueda realizar de forma más eficiente a nivel del dispositivo, no únicamente a nivel de archivos. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 158
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Cloud Access Security Broker (CASB): "*Detección de ransomware con capacidad de remediar el estado post infección*", solicitamos amablemente a la entidad cambiar este requerimiento como parte de la solución EDR, ya que esta funcionalidad es propia de una solución EDR no de CASB.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 159
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Data Loss Prevention (DLP): "*Servicio que permita la gestión de políticas para la prevención de pérdidas de datos en endpoint, correo electrónico, nube y red*. " Es de nuestro entendimiento que el servicio DLP puede ser un conjunto de soluciones que tengan esta funcionalidad para cubrir la protección en los niveles solicitados: endpoint, correo, nube y red. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 160
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Data Loss Prevention (DLP): "*Servicio que permita la gestión de políticas para la prevención de pérdidas de datos en endpoint, correo electrónico, nube y red*.", solicitamos amablemente a la entidad aclarar si se requiere una solución DLP para generación de políticas y mitigaciones de acuerdo al proceso de clasificación de activos e información de la entidad.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 161
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Data Loss Prevention (DLP) "Usuarios", Solicitamos amablemente a la entidad aclarar para cuantos usuarios se requiere el servicio de DLP.

Respuesta
2200

Pregunta 162
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Web Application Firewalls (WAF), solicitamos amablemente a la entidad aclarar si la solución de WAF debe ser desplegada en alta disponibilidad.

Respuesta
El proveedor debe asegurar el cumplimiento de los ANS solicitados.

Pregunta 163
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Web Application Firewalls (WAF). Es de nuestro entendimiento que la solución de WAF debe soportar machine learning para mitigación de falsos

positivos, anomalías y protección contra ataques conocidos y desconocidos. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 164
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Web Application Firewalls (WAF). Es de nuestro entendimiento que la solución de WAF debe soportar anti-defacement para evitar que la reputación de la entidad se vea afectada si se generan intentos de modificación a la apariencia de las aplicaciones web. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 165
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Web Application Firewalls (WAF). Es de nuestro entendimiento que la solución de WAF debe soportar escaneo de vulnerabilidades para que apoye el proceso de aseguramiento de código para aplicaciones web de la entidad sin costo adicional. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
La solución propuesta por el proveedor debe cubrir todos los requerimientos solicitados.

Pregunta 166
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Web Application Firewalls (WAF): "*Ancho de banda: 15 TB*.", solicitamos amablemente a la entidad aclarar si el valor de 15 TB de ancho de banda es el consumo correspondiente a un mes.

Respuesta
Sí.

Pregunta 167
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Web Application Firewalls (WAF), solicitamos a la entidad amablemente aclarar cuál es la retención de logs necesaria para la solución de WAF.

Respuesta
Ver numeral 3.3

Pregunta 168
De acuerdo con el numeral 3.8 Requerimientos Técnicos, Web Application Firewalls (WAF). Es de nuestro entendimiento que los recursos de cómputo necesarios para el despliegue de la solución de WAF en AWS serán responsabilidad de la CCB, ya que se deben implementar en la suscripción de la entidad, por lo cual esta facturación no hace parte del proponente. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
Ver pregunta 3.

Pregunta 169

De acuerdo con el numeral 3, especificaciones técnicas: "*El Servicio debe comprender el acompañamiento en la implementación de los controles de ciberseguridad en la nube considerando los requerimientos del modelo Zero Trust, la implementación y configuración de las soluciones de arquitectura de ciberseguridad, la administración, monitoreo y operación de la arquitectura de ciberseguridad, el soporte 7x24 y mantenimiento para la arquitectura, así como la transferencia de conocimiento.*" Es de nuestro entendimiento que las tecnologías para el servicio de implementación de los controles de ciberseguridad en la nube considerando los requerimientos del modelo Zero Trust deben en su mayoría del mismo fabricante o máximo tres fabricantes, con fin de garantizar mayor integración, visibilidad, control y respuesta automatizada. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta

Se mantienen los requisitos solicitados.

Pregunta 170

Solicitamos amablemente a la entidad aclarar si las hojas de vida de los "analistas de operación" se deben entregar con la presentación de la oferta o si deben ser entregadas posterior a la presentación de la oferta.

Respuesta

Conforme a la NOTA 2 del numeral 3.10 del anexo 2 Aceptación de Especificaciones Técnicas la CCB cuando lo estime conveniente, podrá solicitar las hojas de vida del equipo de trabajo Rol Analista de Operaciones, por consiguiente, no es necesario que presenten las hojas de vida de quienes desarrollarán el mencionado rol con la propuesta.

Atentamente,

Cámara de Comercio de Bogotá

ANEXO 4

PROPUESTA ECONÓMICA

Asunto: Convocatoria Pública para contratar los servicios para la implementación, operación y monitoreo de las soluciones que conforman la arquitectura de ciberseguridad para la plataforma tecnológica de la Cámara de Comercio de Bogotá (CCB), bajo la modalidad híbrida (on premises y en la nube) con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información en la CCB. No. 3000000778.

El proponente deberá presentar la oferta económica de manera separa a la propuesta técnica, indicando lo siguiente:

OBJETO	**Cantidad**	**Valor mensual antes de IVA**	**Valor Total antes de IVA**
Servicio de implementación de la solución para Prestar servicios de ciberseguridad para la plataforma tecnológica de la Cámara de Comercio de Bogotá (CCB) en la nube con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información en la CCB.	**1**	**N/A**	
Prestar servicios de ciberseguridad para la plataforma tecnológica de la Cámara de Comercio de Bogotá (CCB) en la nube con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información en la CCB: Endpoint Detection and Response (EDR) (*)	**23**		
Prestar servicios de ciberseguridad para la plataforma tecnológica de la Cámara de Comercio de Bogotá (CCB) en la nube con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información en la CCB: Autenticación de Usuarios Firewall como servicio (FWasS) Cloud Access Security Broker (CASB) Data Loss Prevention (DLP) Web Application Firewalls (WAF)	**35**		

(*) Solo por 23 meses a partir de enero 2023.

Tiempo de validez de la propuesta: Ciento veinte (120) días.

NOTA 1: Este anexo deberá ser presentado sin tachones o enmendaduras, NO PODRÁ SER MODIFICADO, y deberá contener la totalidad de la información solicitada. No serán evaluadas las propuestas que realicen modificaciones al anexo de oferta económica.

NOTA 2: Los valores anotados en la propuesta económica deberán presentarse en pesos colombianos.

NOTA 3: Los valores anotados en la propuesta económica deberán presentarse sin decimales. Si los valores ofrecidos contienen decimales este debe aproximarse al número entero más cercano.

NOTA 4: En el momento de la evaluación de la propuesta económica la CCB revisará y determinará si existen errores aritméticos. En caso de presentarse alguna inconsistencia el proponente acepta que la CCB proceda a su corrección y que para efectos de la adjudicación se tenga en cuenta el valor corregido.

NOTA 5: El valor presentado por el proponente en su oferta económica deberá incluir todos los costos directos e indirectos y serán valores fijos durante todo el plazo de ejecución del contrato. No habrá lugar a reajustes del valor presentado.

NOTA 6: Si el proponente no establece en su oferta uno o varios valores, su propuesta no será tenida en cuenta.

NOTA 7: El proponente acepta que no habrá lugar a ningún tipo de reajuste del valor del contrato durante el plazo de ejecución de este, ni por concepto de IPC o incremento al salario mínimo mensual legal vigente, riesgo cambiario, entre otros. Esto en el entendido que el proponente con la presentación de LA PROPUESTA realizó todos los cálculos, operaciones, análisis y equivalentes necesarios que determinaron que el valor de los servicios que por este documento se contratan, durante todo el plazo de ejecución, corresponden a las sumas determinadas en LA PROPUESTA y establecidas en el presente documento.

NOMBRE DEL REPRESENTANTE LEGAL

C.C.

Firma del Representante Legal