Bogotá D.C., 9 de noviembre de 2021

Señores
PROVEEDORES
Ciudad

Referencia: CONVOCATORIA PÚBLICA PARA CONTRATAR LOS SERVICIOS DE SOC (SECURITY OPERATION CENTER – CENTRO DE OPERACIÓN DE SEGURIDAD) PARA LA CORRELACIÓN, DETECCIÓN Y MONITORIO DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACION EN LA CCB. No. 3000000777.

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
Cuanto tiempo se tener disponibilidad de logs en línea y por cuanto tiempo se deben mantener por fuera de línea.

Respuesta
Logs en línea: 6 meses
Logs por fuera de línea: 6 meses

Pregunta 2
Se solicita a la entidad confirmar si es viable que los reportes solicitados en el numeral 3.5 Reportes, puedan ser generados por CCB por medio de un portal web, que se entregaría al cliente en el momento de iniciar el servicio. Este portal puede generar los reportes que se requieran en tiempo real, dado que no es practico generar reportes por el contratista.

Respuesta
El proveedor y la CCB definirán en conjunto el mecanismo para la generación y entrega de estos reportes

Pregunta 3
Según el requerimiento de la entidad en el numeral 3.8 Recursos tecnológicos para monitorear, se deben monitorear entre otros Bases de datos, Firewalls, Antimalware, soluciones de seguridad,etc. CCB indica que el listado de dispositivos a monitorear aparece en el anexo 13, pero en dicho anexo solo se mencionan servidores on premise e infraestructura en AWS, se solicita a la entidad entregar el listado completo de los dispositivos a monitorear incluyendo Modelo y sistemas operativos de las soluciones de Bases de datos, Firewalls, Antimalware, soluciones de seguridad, etc.

Respuesta
De acuerdo con lo estalecido en el numeral 3.8. el proponente para la generación de la propuesta económica deberá considerar hasta 2500 EPS (eventos por segundo), y un crecimiento de hasta un 15% en los 36 meses. El inventario de activos a monitorear ofrecido en el anexo 13 de la invitación y numeral 3.8 Recursos tecnológicos para monitorear, es referencial. La información asociada a las bases de datos se encuentra en el Anexo N°1 de este documento.

Pregunta 4
Según el requerimiento: 3.1 Alcance del servicio:

El servicio debe contemplar el monitoreo de la actividad en las bases de datos, mediante una solución tipo DAM u otra(s) que permita gestionar como mínimo los siguientes casos de uso:
Monitoreo de Usuarios:
Usuarios no autorizados
Usuarios Desarrolladores
Usuarios de Altos privilegios
Monitoreo de comandos DML, DCL, DDL sobre bases de datos: ▪ Ejecución de comandos especiales sobre bases de datos
Ejecución de comandos sobre objetos sensibles
Ejecución de comandos desde direcciones IP no autorizadas

Se solicita a la entidad entregar la siguiente información para realizar el dimensionamiento adecuado de la solución DAM:
Ubicación de cada uno de los servidores en donde están alojadas las bases de datos a proteger.
Cantidad de servidores dedicados a bases de datos.
Cantidad de Cores por servidor dedicado a cada motor de base de datos.
Versión exacta de cada uno de los motores de bases de datos.
Interfaz de conexión a los servidores de bases de datos (cobre o fibra), velocidad de las interfaces(10,100, 1000 Mbps).
Si es posible por favor entregar un diagrama de la interconexión actual de los servidores de bases de datos que se deben auditar.
Es posible presentar una solución en appliance virtual en donde la CCB brindaría máquinas virtuales para su implementación? O es obligatoria una solución onpremise con appliances físicos dedicados?

Respuesta
Ver pregunta 3. El diagrama de la interconexión de los servidores de bases de datos será entregado al proveedor seleccionado. La solución tecnológica propuesta debe estar en nube bajo un modelo tipo SaaS.

Pregunta 5
El anexo 2, numeral 3 de especificaciones técnicas: Solicitamos al proponente proporcionar un espacio para el almacenamiento de los registros de auditoría-Logs y asegurar su almacenamiento, disponibilidady recuperación, así como de la información generada en la ejecución del servicio contratado. Estos registros deben ser almacenados de manera cifrada por un tiempo mínimo de (6) seis meses y se debe garantizar la disponibilidad para cuando la CCB los requiera. Es importante que el proponente defina un plan de respaldo en caso de borrados accidentales o provocados. Permítase aclarar si se realizará la eliminación de la información después de los 6 meses de retención solicitada o si la entidad requiere la retención o almacenamiento en frio por el periodo de ejecución del contrato.

Respuesta
Logs en línea: 6 meses
Logs por fuera de línea: 6 meses

Pregunta 6
En el numeral 3.3.3 Equipo de trabajo, se indican cual es el personal requerido para la ejecución del proyecto. Se solicita respetuosamente a la entidad aclarar la Disponibilidad de los perfiles solicitados.

Respuesta
De conformidad con la Nota 3 del numeral 3.3.3 de la invitación el proponente deberá definir la cantidad de Analistas de Operación requeridos para el cumplimiento de los acuerdos de niveles de servicio.

El proponente dentro de su propuesta podrá presentar personal adicional al mínimo requerido.

Es responsabilidad del proveedor asegurarse de que exista la cantidad suficiente de especialistas para cumplir con el cronograma de implementación y los ANS definidos en este documento.

La CCB cuando lo estime conveniente, podrá solicitar las hojas de vida del equipo de trabajo del Rol Analistas de Operaciones que hace parte de la operación, para efectos de verificación, control y auditorias entre otros, del cumplimiento de los requisitos exigidos.

Pregunta 7
Un socio y representante legal de NewNet, ,es miembro de la junta directiva de la CCB. Luego de leer el código de ética e inhabilidades, no encontramos con claridad si NewNet se pudiese presentar o no a este proceso. EL RL no se involucra en la operación de la empresa y por lo tanto no participaría en la oferta, y se declararía impedido para participar en la decisión que tome la Cámara. Peor no sabemos si es esto es suficiente declararlo o definitivamente estaríamos inhabilitados para poder ofertar y contratar con la CCB por este hecho. Apreciamos su claridad para poder apoyarlos en este proceso, el cual es nuestra fortaleza y desearíamos servirles

Respuesta
Una sociedad en la cual un miembro de la Junta Directiva de la CCB ejerce funciones de dirección o tiene participación alguna, está inmersa en una causal de inhabilidad para participar en procesos contractuales o contratar con la CCB, de acuerdo con el Código de Ética y Buen Gobierno Corporativo.

La norma presenta una excepción que indica que, en el evento en que se trate de una sociedad anónima abierta, lo que quiere decir que sus títulos puedan ser adquiridos en la bolsa de valores, la causal antes mencionada no se configura.

OBSERVACIONES DE CARÁCTER TÉCNICO
Pregunta 8
Item Alcance del Servicio
Solicitamos amablemente a la entidad indicar si dentro el alcance para la prestacióndel servicio y la instalación On-premise de la tecnología SIEM y el uso de los Collectores, la entidad suministrara la infraestructura requerida para la implementación de estos, o de lo contrario debe ser suministrada por el proponente.

Respuesta
La infraestructura tecnológica que soportará el servicio debe ser suministrada por el proponente y estar en la nube.

Pregunta 9
Item Alcance del Servicio
Solicitamos amablemente a la entidad indicar si la infraestructura que se posee en nube AWS el modelo es IaaS o SaaS, con el fin de determinar el alcance del tráficoy la ingesta de logs.

Respuesta

El modelo es IaaS. Existen bases de datos como servicios PaaS. Existen servicios de AWS utilizados como serverless.

Pregunta 10

Para el item " El proponente deberá presentar un modelo que minimice la transferencia de los logs teniendo en cuenta que la infraestructura y aplicaciones de la CCB estarán en la nube de AWS".

Solicitamos amablemente a la entodad listar las fuentes con el detalle que se encuentran en la infraestructura de AWS.

Respuesta

Los activos enumerados en el anexo 13 serán migrados en su totalidad a AWS, excepto el Firewall y F5.

Pregunta 11

Item Alcance del Servicio.

Solicitamos amablemente a la entidad indicar cuanto tiempo en línea se deben mantener los logs capturados.

Respuesta

Logs en línea: 6 meses
Logs por fuera de línea: 6 meses

Pregunta 12

Item Alcance del Servicio.

Solicitamos amablemente a la entidad indicar si dentro del alcance del servicio se tiene contemplado que la tecnología SIEM se encuentre en un modelo SaaS (En lanube del fabricante) o un modelo On-premise (implementado localmente en la entidad)

Respuesta

Modelo SaaS en la nube.

Pregunta 13

En el Item, "El servicio debe contemplar el monitoreo de la actividad en las bases de datos, mediante una solución tipo DAM u otra(s) que permita gestionar como mínimo los siguientes casos de uso."

Solicitamos amablemente a la entidad ampliar la información con referencia a esteitem, indicando si la entidad actualmente posee una solución DAM o si dentro del servicio el proponente debe suministrar una solución DAM si es así debe suministrarla siguiente información de cada uno de los servidores de BD:
Tipo: ej. OnPrem/virtual
Estado de Cluster: ej. Satndalone Sistema Operativo: ej. Windows ServerVersión del Sistema Operativo: ej. 2012Total de Cores Del Nodo: ej. 6
Motores DBs: ej. MS SQLVersion: ej. 2019
Cant, Bases de daos: ej. 3

Respuesta

El proponente debe suminstrar una solución tecnológica que cumpla con los casos de uso mínimos solicitados en las especificaciones técnicas. La CCB no suministrará el DAM. Ver pregunta 3 para la información sobre las bases de datos.

Pregunta 14

En el Item " La solución tecnológica con la prestará el servicio deberá estar aprovisionada en la nube de AWS"

Es de nuestro entender que los componentes de recolección de eventos/logs debenestar aprovisionada en AWS, Solicitamos a la entidad indicar si es correcto, de lo contrario ampliar la información de este item.

Solicitamos amablemente a la entidad indicar si dentro del alcance se requiere quelos componentes del servicio se manejen bajo un modelo IaaS (CCB provee la infraestructura para la instalación de los componentes del servicio) o SaaS (los componentes de la infraestructura son incluidos en la propuesta del proponente)

Respuesta

Modelo SaaS en la nube.

Pregunta 15

En el Item "La infraestructura actual de recursos tecnológicos a monitorear está compuesta por los activos listados en el anexo 13"

No se encuentra el Anexo 13 dentro de los documentos suministrados por la entidad, Solicitamos amablemente a la entidad él envió de esta información

Respuesta

Todos los documentos de la invitación están disponibles en la siguiente dirección: https://www.ccb.org.co/Vinculese-a-nuestro-grupo-de-proveedores-y-contratistas/Convocatorias/Invitaciones-vigentes/Prestar-los-servicios-de-SOC-Security-Operaction-Center-Centro-de-Operacion-de-Seguridad

Pregunta 16

Solicitud de reunión

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

Respuesta

Se mantienen los requisitos establecidos en la invitación.

REQUERIMIENTOS ADICIONALES SOC

Pregunta 17

Solicitamos a CCB que se tenga en cuenta que el servicio del SOC cuente con mínimos dos (2) SOC geográficamente ubicados en diferentes países diferentes y actuando como alta disponibilidad Activo/Activo entre sí para sufuncionamiento.

Respuesta

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

Pregunta 18

Solicitamos tener en cuenta servicios que cuente con una alianza directa y activa para combatir el cibercrimen a nivel mundial como ICSPA

Respuesta
Se mantienen los requisitos establecidos en la invitación. El proveedor podrá ofrecer los valores agregados que considere para la prestación del servicio, pero la selección se realizará teniendo en cuenta los requisitos establecidos en la invitación.

Pregunta 19
Solicitamos a CCB que el SOC sea de la misma compañía que este presentado la propuesta y no involucre terceros en el proceso

Respuesta
El SOC es un servicio provisto por un proveedor que puede tener soluciones propias o adquiridas. En estricto sentido no hay un "fabricante" de SOC. La CCB está buscando un servicio con unos ANS específicos y unas condiciones sobre las soluciones que están descritos en los requerimientos técnicos. Teniendo esto en cuenta la pregunta se refiere a la eventualidad de que una compañía pueda presentar propuesta con un SOC de otra empresa, lo cual está limitado por lo descrito en el numeral 3.1.1 y la cláusula 30 del proyecto de contrato.

Pregunta 20
Solicitamos requerir acreditación en datacenter como mínimo en tier 3 en diseño y operación, con la finalidad que todo el proceso de servicio este alineado con las mejores capacidades operativas a nivel internacional.

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

Pregunta 21
Solicitamos incluir que EL PROVEEDOR deba permitir al CLIENTE poder contactarse al CyberSOC para la apertura de tickets con al menos tres formas distintas de comunicación, por llamada telefónica a un teléfono fijo, por correo o por el portal web de generación de tickets.

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

Pregunta 22
Solicitamos a CCB que la gestión de los servicios realicen mediante un único Dashboard de Gestión, que proporcione un resumen ejecutivo y un cuadro de mandos, con el estado de los servicios en tiempo real (incluyendo los cumplimientos de los SLA’s comprometidos), así como, una visión más operativa con información detallada de lo que está pasando y quien tiene que resolverlo.

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

Pregunta 23
Las experiencias relacionadas pueden ser de otros paises en donde Sencinet tiene presencia?

Respuesta
Sí, la experiencia puede ser de otros países siempre y cuando las certificaciones cumplan con los requisitos y características solicitadas, tener en cuenta las notas 4 y 5 del numeral 3.3.2 de la invitación si las certificaciones se presentan en moneda diferente al peso colombiano.

Pregunta 24
3.3.3 Equipo de trabajo
En relación al equipo de trabajo que proponen para el servicio, solicitamos su colaboración en indicar si es factible presentar una estructura diferente para el equipo de trabajo el cual cumpla con los requerimientos solicitados y permita diversificar y segmentar los roles.

Respuesta
El equipo de trabajo debe estar conformado por mínimo los perfiles solicitados en la invitación. El proponente podrá presentar personal adicional al mínimo requerido, de acuerdo con lo definido en la Nota 3 del numeral 3.3.3.

Pregunta 25
3.2 Modelo de Operación
Solicitamos su amable colaboracion en aclarar si el Cliente, posee un plan para la respuesta ante incidentes de seguridad de la informacion y si puede ser enviado a Netready

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 26
3.2 Modelo de Operación
¿La responsabilidad de una contencion, erradicacion y solución de un incidente de seguridad, dependerá o sera responsabilidad del cliente y sus correspondientes administradores de las plataformas tecnológicas?, Especificar.

Respuesta
Sí, será responsabilidad de la CCB la implementación de las acciones. No obstante el proveedor deberá generar recomendaciones para la respuesta a los incidentes presentados.

Pregunta 27
3.2 Modelo de Operación
Por favor indicar para el dimensionamiento del servicio, la cantidad promedio mensual de incidentes de seguridad (SOC) que poseen registrados en el cliente.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 28
3.2 Modelo de Operación
Por favor indicar para el dimensionamiento del servicio, la cantidad promedio mensual de los requerimientos (cambios y parametrizaciones) que poseen registrados en el cliente.

Respuesta

Esta información será compartida con el proveedor seleccionado.

Pregunta 29
3.6. Acuerdos de Niveles de Servicios
Por favor aclarar si los tiempos de atencion de incidentes (ANS) presentes en el documento, estan asociados a los incidentes sobre la plataforma tecnologica de monitoreo de eventos en Cyberseguridad o estan asociados a los incidentes que se reporten como resultado del monitoreo.

Respuesta
Estos ANS están asociados a la plataforma tecnologica de monitoreo de eventos

Pregunta 30
3.8. Recursos Tecnológicos para monitorear
¿Por favor indique cantidad de controladores de dominios a monitorear?

Respuesta
Actualmente: 4 controladores de dominio
Al finalizar la migración a la nube: 2 controladores de dominio.

Pregunta 31
3.8. Recursos Tecnológicos para monitorear
¿Por favor indique cantidad de usuarios en el dominio o forrest a monitorear?

Respuesta
Aproximadamente 2200

Pregunta 32
3.8. Recursos Tecnológicos para monitorear
¿Por favor indique Listado y cantidad de aplicaciones para monitoreo de eventos a monitorear?

Respuesta
Esta información será entregada al proveedor seleccionado.

Pregunta 33
3.8. Recursos Tecnológicos para monitorear
¿Cuales son las soluciones de Firewall y antimalware actuales?

Respuesta
Firewall: Palo Alto y Antimalware: Kaspersky

Pregunta 34
3.8. Recursos Tecnológicos para monitorear
¿Por favor indique cantidad de firewalls a monitorear a monitorear?

Respuesta
Actualmente se cuenta con un Firewall físico Palo Alto. Se contará adicionalmente con NGFWaaS y otros elementos. La información detallada se entregará al proveedor seleccionado.

Pregunta 35
3.8. Recursos Tecnológicos para monitorear
¿Cuales son las soluciones de DLP, EDR, NGFWaaS, SD WAN, CASB y MFA?

Respuesta
Esta información será entregada al proveedor seleccionado.

Pregunta 36
3.8. Recursos Tecnológicos para monitorear
¿Existe actualmente una solución de monitoreo de bases de datos?

Respuesta
Ver pregunta 13.

Pregunta 37
3.8. Recursos Tecnológicos para monitorear
¿Cuales son las Versiones de las bases de datos a monitorear SQLServer, DB2, RDS (Aurora MySQL, PostgreSQL, SAP HANA) y cantidad de instancias por cada base de datos?

Respuesta
Ver pregunta 3.

Pregunta 38
El porcentaje de disponibilidad solicitado es de 99,96% sin embargo la tabla de penalidades es

Rango % Disponibilidad Promedio		% Penalidad
Inferior	Superior	
-	99.93%	0 %
99,93%	99,77%	0,80%
99,77%	99,62%	1,60%
99,62%	99,46%	2,40%
99,46%	99,30%	3,20%
Menor a 99,30%		4,00%

¿Es decir que que minimo debemos cumplir con el 99,93%?

Respuesta
El porcentaje de disponibilidad que debe considerarse es de 99.93%.

Pregunta 39
¿La complejidad en cambios y parametrizaciones solicitadas por la CCB se acuerda entre las partes o es una decision unilateral?

Respuesta
Al inicio del contrato entre el proveedor y la CCB se definirá los casos específicos a considerar en cada tipo de complejidad.

Pregunta 40
Cronograma del proceso
Se solicita a la CCB ampliar el cronorgrama del proceso e incluir la fecha prevista para evaluación de las propuestas, plazo para subsanaciones y fecha estimada de adjudicación e inicio de ejecución.

Respuesta
Se acepta su observación, mediante adenda se amplió el plazo de cierre, para el 16 de noviembre de 2021 a las 2:00:00 p.m.

Pregunta 41
Numeral 3.3.3
Un (1) Coordinador de SOC: Profesional en ingeniería de sistemas o afines según el SNIES que tenga como mínimo 2 años de experiencia en la coordinación de operaciones de contratos cuyo objeto se relacione con la correlación, detección y monitoreo de los eventos de Seguridad, debe contar con certificación en el uso de las herramientas propuestas por el proponente, en la versión más reciente con la que se prestará el servicio.
Rol: Será el responsable de coordinar la ejecución de las actividades del contrato.

Se solicita a la entidad que para el coordinador del SOC no se solicite la certificación en el uso de las herramientas propuestas, dado que estas certificaciones están asociadas al perfil del ingeniero que administrará la plataforma de monitoreo y será asignado como personal al proyecto. Se solicita que incluyan certificaciones de acuerdo con la naturaleza del Cargo, CISSP, EH, ISO 27001, ISO 27032.

Respuesta
Se mantienen los requisitos solicitados

Pregunta 42
Numeral 3.3.3
Analistas de operación: Deben contar con certificación en el uso de las herramientas propuestas por el proponente, en la versión más reciente con la que se prestará el servicio.

Se solicita a la entidad que para los Analistas de operación no se solicite la certificación en el uso de las herramientas propuestas, dado que estas certificaciones están asociadas al perfil del ingeniero que administrará la plataforma de monitoreo y será asignado como personal al proyecto. Se solicita que incluyan certificaciones de acuerdo con la naturaleza del Cargo, certificaciones de incidentes de seguridad.

Respuesta
Se mantienen los requisitos solicitados

Pregunta 43
Corresponde a la tenencia de un certificado de calidad ISO 27001:2013 Vigente, el cual debe ser presentado junto con la propuesta.

En virtud de la naturaleza del proceso y de acuerdo a los requerimientos solicitados, es importante que el proponente que preste los servicios garantice la alineación con las normas vigentes la protección de los activos de información, esto se logra si se cuenta con una madurez en los procesos, mediante una acreditación o certificación vigente alineada a seguridad de la información, lo que garantizará a la Cámara de Comercio de Bogotá, la protección adecuada de su infraestructura y activos de información,

por lo cual es de suma importancia que la entidad solicite para este proceso que los procesos o procedimientos del SOC se encuentren dentro del alcance de la certificación de ISO 27001

Respuesta
Tanto en el anexo 2 Especificaciones técnicas numeral 1.5 y numeral 6.3 la certificación de ISO 27001:2013 se solicita y a su vez esta es criterio de calificación.

Pregunta 44
Numeral 3.3.3
Carta de compromiso y soporte de perfiles.

Por favor confirmar si es correcto nuestro entendimiento en cuanto a que con la oferta solo se deberán presentar carta de compromiso y documentos de soporte para los perfiles de Lider de cuenta y Coordinador de SOC.

Respuesta
Los documentos de soporte a presentar deben corresponder a los perfiles de Líder de cuenta y Coordinador SOC (ver Nota 4 del numeral 3.3.3). Para las Cartas de Compromiso ver Nota 1 y 2 del numeral 3.3.3.

Pregunta 45
Numeral 2.1
La CCB actualmente está en el proceso de migración de toda su infraestructura tecnológica a la nube.

Se solicita a la entidad indicar para cuando se tiene proyectado la finalización de la migración de la infraestructura a la nube.

Respuesta
La fecha estimada de finalización es 30 de abril 2022.

Pregunta 46
Numeral 2.1
El servicio y el modelo de operación del SOC ofrecido deberá adaptarse a los componentes que se aprovisione en la migración total de la infraestructura tecnológica en nube.

Se solicita a la entidad indicar para un mejor dimensionamiento de la solución los componentes que se aprovisionarán en la migración total de la infraestructura tecnológica en nube.

Respuesta
Los Componentes son los equivalentes a los que se entregaron en el anexo 13 de esta invitación.

Pregunta 47
Numeral 2.1
El Servicio debe comprender la correlación, detección y el monitoreo de los eventos de seguridad de la infraestructura tecnológica, aplicaciones incluyendo la captura, integración, correlación, análisis, alertamiento, escalamiento y reportes de los eventos, alarmas e incidentes de seguridad de la información y generación de recomendaciones para la respuesta al evento. Para prestar este servicio el proponente debe considerar:

Se solicita a la entidad indicar cuantos incidentes de seguridad se presentan al mes.

Respuesta
Se mantienen los requisitos solicitados

Pregunta 48
Numeral 3.1
El servicio debe contemplar el monitoreo de la actividad en las bases de datos, mediante una solución tipo DAM u otra(s) que permita gestionar como mínimo los siguientes casos de uso:

Se solicita a la entidad indicar la cantidad de servidores de bases de datos, los Cores de esos servidores de bases de datos, si están en esquema de clúster, activo activo o pasivo pasivo, los servidores de bases de datos se encuentran en un mismo datacenter o en diferentes datacenter, tienen en la nube, motores de bases de datos, cantidad aproximado de bases de datos e instancias.

Respuesta
Ver pregunta 3.

Pregunta 49
Numeral 3.1
El proponente deberá presentar un modelo que minimice la transferencia de los logs teniendo en cuenta que la infraestructura y aplicaciones de la CCB estarán en la nube de AWS.

Se solicita a la entidad indicar la infraestructura y aplicaciones que estarán en la nube de AWS.

Respuesta
Ver pregunta 46. El resto de la información será entregada al proveedor seleccionado.

Pregunta 50
Numeral 3.1
El proponente realizará la reconfiguración de las fuentes de premisas a fuentes de nube en la solución que se presente para el servicio a medida que la CCB realice la migración de la infraestructura.

Se solicita a la entidad indicar cuantas fuentes faltan migrar de onpremise a la nube.

Respuesta
Se migraran los activos indicados en el Anexo 13 de esta invitación. Este proceso se estima que finalizará el 30 de abril de 2022.

Pregunta 51
Numeral 3.1
Ataques de denegación de servicio (externos o internos), tráfico desde / hacia sitio con reputación sospechosa, actividades asociadas a conexión de escritorio remoto

Se solicita a la entidad indicar si actualmente cuentan con una solución para mitigación de ataques de denegación de servicios.

Respuesta
Esta información será compartida con el proponente seleccionado.

Pregunta 52
Numeral 3.1.
El proponente debe realizar un monitoreo a los análisis de tendencia de amenazas y riesgos disponibles en internet o en centros de respuesta a incidentes que permita informar a la CCB alertas, tendencias, ataques y amenazas provenientes desde el ciberespacio y puedan afectar la infraestructura o los servicios que la CCB presta. Asimismo, el proponente debe disponer de servicios de inteligencia ante Ciber Amenazas.

Se solicita a la entidad aclarar si requieren un servicio de monitoreo y/o protección de Marca, si es así por favor indicar los siguiente:
Cuáles marcas se deben monitorear?
Cuáles dominios web, portales y apps móviles se deben monitorear?
Cuáles dominios de correo se deben monitorear?
Cuáles redes sociales se deben monitorear y en cuales tienen cuenta?
Cantidad de palabras claves
Cantidad de desactivaciones requeridas (cantidad por año)

Respuesta
No se está solicitando dentro del alcance de este servicio un monitoreo y/o protección de Marca.

Pregunta 53
Numeral 3.2
La solución tecnológica con la prestará el servicio deberá estar aprovisionada en la nube de AWS.
Se solicita a la entidad indicar si la solución tecnológica que prestar el servicio debe estar aprovisionada en la nube de AWS o se únicamente tener los collectores en la nube de AWS, en este tipo se escenario, los collectores están en AWS y los demás componentes de la solución estará en la premisas del datacenter del proponente.

Respuesta
Los Colectores en infraestructura AWS, los demás componentes pueden ser aprovisionados en el data center del proponente (siempre y cuando sea en nube).

Pregunta 54
Numeral 3.2
Las soluciones tecnológicas de monitoreo para la infraestructura, aplicaciones y bases de datos deberán estar incluidas por Gartner en el cuadrante mágico o peer insight en la versión más reciente.

De acuerdo a la naturaleza del proceso, el servicio solicitado, la confidencialidad y la protección de la infraestructura de la Cámara de Comercio de Bogotá, solicitamos a la entidad que incluya dentro de los requerimientos que la solución SIEM a utilizar dentro del servicio, se encuentre como líder en el cuadrante Gartner, esto garantiza que se cuente con una solución robusta, con grandes capacidades, de alto nivel, capaz de cubrir todos los requerimientos solicitados, con cubrimiento y soporte a nivel mundial, integración con cualquier fabricante, inversión en desarrollo y nuevas funcionabilidades.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 55

Numeral 3.2

El proponente hará monitoreo constante del estado de disponibilidad, desempeño y salubridad de solución tecnológica propuesta para la prestación del servicio solicitado y generará los reportes correspondientes de caídas que se presenten y que puedan afectar los acuerdos de niveles de servicio y porcentajes de disponibilidad contratados por la CCB.

Se solicita a la entidad aclarar si el monitoreo de disponibilidad, desempeño y salubridad se debe realizar sobre las soluciones ofrecidas para el servicio o sobre los dispositivos de CCB, de ser correcto lo último se solicita a la entidad indicar la cantidad, modelo y tipo de dispositivo que estará monitoreado, la ubicación (on premise, nube)

Respuesta

El monitoreo de disponibilidad, desempeño y salubridad se debe realizar sobre las soluciones ofrecidas para el servicio.

Pregunta 56

Numeral 3.8

La correlación, detección, monitoreo y alertamiento de la infraestructura y aplicaciones, incluye las siguientes capas:

Categoría por incluir en monitoreo	Tipo de dispositivo
Aplicaciones	Sistemas con formato SYSLOG
Bases de datos	SQLServer, DB2, RDS (Aurora MySQL, PostgreSQL, SAP – HANA)
Servicios infraestructura	Directorio activo, correo electrónico, Balanceadores de carga, IIS, WAS
Dispositivos de seguridad	Firewall, antimalware, Monitoreo de bases de datos
Recursos nube	Cloud trail, soluciones nativas de AWS: balanceadores, IAM
Soluciones Ciberseguridad	DLP, EDR, NGFWaaS, SD WAN, Múltiple factor de autenticación, CASB

Se solicita a la entidad indicar el fabricante, modelo, sistema operativo, rol, de los dispositivos mencionados.

Respuesta

Esta información será entregada al proveedor seleccionado.

Pregunta 57

Numeral 3.10

El proveedor potencial debe incluir el cronograma de ejecución del servicio para cada uno de los temas requeridos, detallando las principales fases y/o actividades, así como los recursos requeridos del proveedor y de la CCB.

Se solicita a la entidad indicar si el cronograma se debe entregar con la propuesta o se debe entregar durante la ejecución del contrato.

Respuesta
Con la propuesta el proveedor debe presentar el cronograma de implementación.

Pregunta 58
Sugerimos que el proveedor que quede seleccionado para prestar el servicio de correlación de eventos tenga alguno de los niveles más altos de certificación del fabricante propuesto. Esto deberá ser demostrado en una certificación emitida directamente por el fabricante con fecha de expedición no mayor a 30 días y dirigida directamente a la entidad.

Respuesta
Se mantienen los requisitos solicitados. No obstante el proveedor puede incluir los valores agregados que considere oportunos, sin que estos generen costos adicionales para la CCB.

Pregunta 59
Se sugiere que CCB sea propietario de la solución ofertada de correlación de eventos para que al final del contrato con el proveedor la entidad tenga los logs, analítica y casos de uso permitiendo así continuar con el servicio de forma óptima manteniendo la confidencialidad de la información.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 60
Se solicita amablemente a la entidad aclarar la cantidad de dispositivos tecnológicos a monitorear, considerando que en el Anexo 13. solo se relaciona la información de los servidores, bases de datos y los recursos en nube, sin embargo, no se relaciona la cantidad de activos de seguridad, red y ciberseguridad que deben ser contemplados, se requiere conocer la cantidad exacta de equipos relacionados en el item 3.8 Recursos tecnológicos para monitorear.

Respuesta
De acuerdo con lo estalecido en el numeral 3.8. el proponente para la generación de la propuesta económica deberá considerar hasta 2500 EPS (eventos por segundo), y un crecimiento de hasta un 15% en los 36 meses.

Pregunta 61
Para realizar el dimensionamiento correcto de la solución de DAM, solicitamos amablemente complementar la información relacionada en el Anexo.13 con la cantidad de cuentas de usuarios privilegiados quese esperan auditar.

Respuesta
Ver pregunta 3.

Pregunta 62
Solicitamos amablemente a la entidad aclarar si para la solución de DAM se requiere un diseño de alta disponibilidad.

Respuesta
El proveedor deberá cumplir con los ANS del servicio.

Pregunta 63
Se solicita amablemente a la entidad indicar si es posible contar con un diagrama topológico en el cual se evidencia la distribución física de los motores de bases de datos con el fin de determinar de Gateway de bases de datos que se deben implementar.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 64
Se solicita a la entidad aclarar si dentro de su centro de datos existe capacidad de espacio en rack y suministro energético para implementar recursos tecnológicos con el fin de garantizar el monitoreo, la correlación de eventos y auditoria de los equipos y bases de datos que se encuentran en premisa.

Respuesta
La solución tecnológica propuesta debe ser bajo Modelo SaaS y estar aprovisionada en nube .

Pregunta 65
¿Se solicita a la entidad aclarar qué tipo de red LAN tiene la entidad? (Fibra-Cobre/1Gb-10Gb) y si existen disponibles puertos para conexiónde los equipos.

Respuesta
La solución tecnológica propuesta debe ser bajo Modelo SaaS y estar aprovisionada en nube .

Pregunta 66
Según nuestro entendimiento el servicio de monitoreo se realizará basado en la configuración y monitoreo de los casos de uso descritos en el punto 3.1 Alcance del servicio, teniendo en cuenta nuestra experiencia se recomienda muy respetuosamente a la entidad limitar la cantidad de casos de uso adicionales que se puedan llegar a solicitar sobre los activos descritos en el Anexo.13

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 67
Se solicita amablemente a la entidad conocer si se cuenta con un cronograma de migración de la infraestructura on premise hacia la nube (Servidores, bases de datos, aplicaciones y seguridad) que tiene proyectado realizar la entidad durante el periodo de prestación del servicio, esto con el fin de diseñar de manera apropiada la arquitecturade la solución y del servicio.

Respuesta
Se estima que para el 30 de abril de 2022 haya finalizado la migración.

Pregunta 68
Es de nuestro entendimiento que los cambios que se deban realizar solo hacen referencia a modificaciones en la plataforma de monitoreo y correlación de eventos, los cambios en las plataformas tecnológicas objeto del monitoreo son responsabilidad por parte de la entidad.

Respuesta
Su entendimiento es correcto.

Pregunta 69
Solicitamos amablemente aclarar si en caso de adicionarse como valor agregado la funcionalidad de FIM para monitoreo de integridad en archivos y directorios críticos, cuantos servidores Linux y Windows mínimo deberían tener esta característica.

Respuesta
Se definirán en conjunto con el proveedor al inicio del contrato.

Pregunta 70
Se solicita amablemente a la entidad conocer si CCB cuenta con una herramienta de gestión de ticket con el fin de realizar el seguimiento delos incidentes o si debe ser considerado dentro de la propuesta de servicio.

Respuesta
No se debe considerar dentro de la solución propuesta el uso de herramientas internas de la CCB para la gestión de tickets.

Pregunta 71
Se solicita amablemente aclarar si la ENTIDAD cuenta con recursos en AWS para realizar la implementación de la solución tecnológica o si estos recursos deben estar contemplados dentro de la propuesta económica establecida por el proponente.

Respuesta
Debe incluirse dentro de la propuesta, considerando que lo solicitado es bajo un modelo tipo servicio (SaaS).

Pregunta 72
Se solicita amablemente a la entidad indicar si la CCB cuenta con un servicio de SOC, de ser así solicitamos amablemente conocer laherramienta de SIEM y arquitectura del servicio.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 73
Al numeral 3. Especificaciones técnicas" El Servicio debe comprender la correlación, detección y el monitoreo de los eventos de seguridad de la infraestructura tecnológica, aplicaciones incluyendo la captura, integración, correlación, análisis, alertamiento, escalamiento y reportes de los eventos, alarmas e incidentes de seguridad de la información y generación de recomendaciones para la respuesta al evento. "

P:// Es de nuestro entendimiento que el servicio debe incluir el monitoreo de disponibilidad y rendimiento de la infraestructura tecnológica y aplicaciones para que el servicio de SOC pueda identificar si el incidente o falla se genera por temas de seguridad, disponibilidad, problemas de recursos o rendimiento. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
No está considerado dentro del alcance solicitado.

Pregunta 74

Al numeral 3.1 Alcance del servicio

" El proponente debe realizar un monitoreo a los análisis de tendencia de amenazas y riesgos disponibles en internet o en centros de respuesta a incidentes que permita informar a la CCB alertas, tendencias, ataques y amenazas provenientes desde el ciberespacio y puedan afectar la infraestructura o los servicios que la CCB presta. Asimismo, el proponente debe disponer de servicios de inteligencia ante Ciber Amenazas."

P:// Solicitamos amablemente a la entidad aclarar si el servicio de SOC requiere un servicio de indicadores de compromiso para identificar riesgos de seguridad en dispositivos y usuarios. En caso afirmativo por favor confirmar la cantidad de dispositivos y puntos finales que deben considerarse.

Respuesta

No se requiere.

Pregunta 75

Al numeral 3.1. Alcance del servicio

" El proponente deberá presentar un modelo que minimice la transferencia de los logs teniendo en cuenta que la infraestructura y aplicaciones de la CCB estarán en la nube de AWS."

P:// Es de nuestro entendimiento que la solución SIEM para el servicio de SOC debe estar alojada en AWS para minimizar la transferencia de logs. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta

La nube en la cual estará aprovisonada la solución tecnológica ofrecida es selección del proveedor.

Pregunta 76

Al numeral 3.2 Solución Tecnológica

" Las soluciones serán licenciadas y deben cumplir las condiciones técnicas necesarias para realizar el monitoreo sobre la plataforma tecnológica, aplicaciones y bases de datos incluidas en el alcance de monitoreo. Por lo tanto, el proponente instalará, configurará y mantendrá las soluciones a utilizar en la prestación del servicio, recursos y complementos necesarios para la captura, correlación, análisis, monitoreo, alertas y gestión de eventos e incidentes de seguridad sobre la plataforma tecnológica de la CCB."

P:// Es de nuestro entendimiento que la infraestructura en AWS para el despliegue de las soluciones SIEM, monitoreo de base de datos y todas las que sean necesarias para el servicio de SOC será responsabilidad de la Cámara de Comercio de Bogotá, ya que esta infraestructura pertenece a la suscripción con la que cuenta la entidad y cuya facturación mensual está a su cargo. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta.

Ver pregunta 71.

Pregunta 77

Al numeral 3. Especificaciones Técnicas

P:// Solicitamos amablemente a la entidad aclarar si se requiere monitoreo de integridad de archivos o FIM para los servidores de la infraestructura on premise y en nube. En caso afirmativo por favor aclarar la cantidad de servidores que requieren esta funcionalidad.

Respuesta

No está dentro del alcance solicitado. No obstante el proveedor puede incluir los valores agregados que considere oportunos, sin que estos generen costos adicionales para la CCB.

Pregunta 78

Al numeral 3. Especificaciones Técnicas

P:// Es de nuestro entendimiento que el servicio de SOC debe contemplar el monitoreo de transacciones sintéticas para identificar problemas propios de aplicaciones y servicios en los protocolos Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC y todos los puertos genéricos TCP/UDP. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta

No forma parte del alcance solicitado.

Pregunta 79

Al numeral 3.2 Solución Tecnológica

" El proponente debe definir la solución tecnológica que permita la correlación, detección y monitoreo de eventos de la infraestructura tecnológica, aplicaciones y bases de datos (nube y On premises). "

P:// Solicitamos amablemente a la entidad el listado de todas las aplicaciones y servicios que se tienen en on premise y en nube incluyendo las cantidades.

Respuesta

Esta información será compartida con el proveedor seleccionado.

Pregunta 80

Al numeral 3.2 Solución Tecnológica

" El proponente debe definir la solución tecnológica que permita la correlación, detección y monitoreo de eventos de la infraestructura tecnológica, aplicaciones y bases de datos (nube y On premises). "

P:// Solicitamos amablemente a la entidad el listado de motores de bases de datos que deben monitorearse, la cantidad y la ubicación actual (on premise o nube).

Respuesta

Ver pregunta 3.

Pregunta 81

Al numeral 3.3. Canales de Comunicación

"El proponente debe definir el modelo de conexión de los dispositivos que serán monitoreados, especificar los requerimientos técnicos para cumplir con el servicio a contratar; apoyar y soportar a la CCB en la conexión, configuración y activación de las conexiones técnicas de los dispositivos a monitorear."

P:// Solicitamos amablemente a la entidad aclarar si es posible configurar dos VPNs sitio a sitio para el servicio de SOC, la primera entre la ubicación del SOC y la infraestructura on premise de la CCB y la segunda entre la ubicación del SOC y la infraestructura en nube.

Respuesta
La conectividad se definirá con el proveedor seleccionado. El servicio debe ser ofrecido bajo modelo SaaS.

Pregunta 82
Al numeral 3.4 Seguridad, mantenimiento y soporte de la solución tecnológica propuesta.
P:// Es de nuestro entendimiento que la entidad requiere apoyo del fabricante para revisar como mínimo anualmente la solución SIEM del servicio SOC para realizar sugerencias de mejora y afinamientos, los cuales deben ser aplicados por el proponente. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
Se mantienen los requisitos solicitados. No obstante el proveedor podrá presentar los valores agregados que considere sin que estos generen costos adicionales a la CCB.

Pregunta 83
Al numeral 3.4 seguridad, mantenimiento y soporte de la solución tecnológica propuesta.
P:// Es de nuestro entendimiento que la entidad requiere apoyo del fabricante para el diseño de la arquitectura del servicio de SOC y las herramientas necesarias para el mismo. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
Se mantienen los requisitos solicitados. No obstante el proveedor podrá presentar los valores agregados que considere sin que estos generen costos adicionales a la CCB.

Pregunta 84
Al numeral 3.8 Recursos tecnológicos a monitorear
P:// Solicitamos amablemente a la entidad aclarar la marca y cantidades de los balanceadores de carga y los dispositivos de seguridad (Firewall, antimalware, monitoreo de bases de datos, DLP, EDR, NGFWaaS, SD-WAN, múltiple factor de autenticación y CASB).

Respuesta
Esta información será entregada al proveedor seleccionado.

Pregunta 85
Al numeral 3.8 Recursos tecnológicos a monitorear
" El modelo propuesto para el monitoreo de los eventos de seguridad deberá considerar el listado de activos del anexo 13 y su migración a la nube."

P:// Solicitamos amablemente a la entidad aclarar el crecimiento contemplado en cantidad de dispositivos a monitorear durante los 36 meses de vigencia del contrato.

Respuesta
De acuerdo con lo estalecido en el numeral 3.8. el proponente para la generación de la propuesta económica deberá considerar hasta 2500 EPS (eventos por segundo), y un crecimiento de hasta un 15% en los 36 meses.

Pregunta 86
Al numeral 3.4 Seguridad, mantenimiento y soporte de la solución tecnológica propuesta.
P:// Es de nuestro entendimiento que la entidad requiere capacitación dictada directamente por el fabricante para la solución SIEM del servicio de SOC con posibilidad de acceso a laboratorios para la cantidad de empleados que considere la entidad. Agradecemos aclarar si nuestro entendimiento es acertado

Respuesta
Se mantienen los requisitos solicitados. No obstante el proveedor podrá presentar los valores agregados que considere sin que estos generen costos adicionales a la CCB.

Pregunta 87
Al anexo 10 CARTA DE COMPROMISO SOLUCIÓN TECNOLÓGICA PROPUESTA
P:// Solicitamos amablemente a la entidad, corregir el contenido de los componentes del presente anexo, ya que no guarda relación con el objeto de la presente invitación.

Componente	Aplicación tecnológica Propuesta:
Autenticación de Usuarios	
Endpoint Detection and Response (EDR)	
Firewall como servicio (FWasS)	
Cloud Access Security Broker (CASB)	
Data Loss Prevention (DLP)	
Web Application Firewalls (WAF)	

Respuesta
Se ajusta la información del anexo 10 Carta de Compromiso solución Tecnológica propuesta, mediante adenda.

Pregunta 88
Al numeral 3.1 Alcance del servicio
Monitoreo de comandos DML, DCL, DDL sobre bases de datos:
Ejecución de comandos especiales sobre bases de datos
Ejecución de comandos sobre objetos sensibles
Ejecución de comandos desde direcciones IP no autorizadas"

P:// Solicitamos amablemente a la entidad eliminar el monitoreo de comandos DML y DCL, ya que este tipo de monitoreo normalmente requiere despliegue de agentes en los servidores de bases de datos, los cuales pueden afectar considerablemente el rendimiento de los mismos.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 89

Al numeral 3.1 Alcance del servicio

" Los tipos de reglas, alertas y notificaciones deben enfocarse en eventos relevantes de seguridad. El proveedor presentará de acuerdo con su experiencia los casos de uso los cuales deberán ser aprobados por la CCB."

P:// Es de nuestro entendimiento que los eventos de seguridad deben monitorearse y buscarse en tiempo real para tener respuestas y diagnósticos proactivos ante incidentes o fallas que se puedan presentar. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta

El monitoreo debe ser realizado en tiempo real.

Pregunta 90

Al numeral 3.8 Recursos tecnológicos para monitorear

" El proponente para la generación de la propuesta económica deberá considerar hasta 2500 EPS (eventos por segundo), y un crecimiento hasta un 15% en los 36 meses."

P:// Es de nuestro entendimiento que la solución SIEM desplegada en AWS para el servicio de SOC debe ser escalable y su rendimiento no se debe afectar cuando se genere el crecimiento solicitado. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta

Su entendimiento es correcto.

Pregunta 91

Al numeral 3.1 Alcance del servicio

" El proponente deberá presentar un modelo que minimice la transferencia de los logs teniendo en cuenta que la infraestructura y aplicaciones de la CCB estarán en la nube de AWS."

P:// Es de nuestro entendimiento que la solución SIEM del servicio de SOC no debe estar alojada en la nube del fabricante para dar cumplimiento a este requerimiento y evitar latencia en el procesamiento de los eventos de la infraestructura alojada en AWS. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta

El servicio debe ser Modelo SaaS, el proveedor definirá la nube y es responsable de garantizar el cumplimiento de los ANS solicitados.

Pregunta 92

Al numeral 3.1 Alcance del servicio

" El proponente en conjunto con la CCB definirá serie de reglas, alertas y notificaciones clasificadas y priorizadas para detectar los eventos de las fuentes que se estará monitoreando, las cuales serán reportarlas a la CCB cada vez que se encuentre en riesgo los principios de integridad, disponibilidad o confidencialidad de los activos tecnológicos. "

P:// Es de nuestro entendimiento que la solución SIEM del servicio de SOC debe monitorear cambios de configuración de los dispositivos de seguridad y red para identificar incidentes que afecten la

disponibilidad de los activos tecnológicos de la CCB. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
Sí, está incluido como caso de uso dentro de los requerimientos técnicos.

Pregunta 93
Al numeral 3.8 Recursos Tecnológicos para monitorear
"La correlación, detección, monitoreo y alertamiento de la infraestructura y aplicaciones, incluye las siguientes capas:
Recursos en nube: Cloud trail, soluciones nativas de AWS: balanceadores, IAM"

P:// Es de nuestro entendimiento que la solución SIEM del servicio de SOC debe integrarse con cuentas y servicios de AWS a través del protocolo AWS Security Hub SDK para recolectar información de incidentes de seguridad de alta prioridad. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
Esto será definido en conjunto con el proveedor seleccionado al inicio del contrato.

Pregunta 94
Al anexo 13 infraestructura premisas AWS
" 89 instancias EC2 encendidas"
P:// Solicitamos amablemente a la entidad el listado de sistemas operativos y tipo de servicios y aplicaciones alojadas en las 89 instancias activas en AWS.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 95
Al anexo 13 infraestructura premisas AWS
" 94 Buckets S3"
P:// Solicitamos amablemente a la entidad la cantidad de almacenamiento total de los 94 buckets S3 en AWS.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 96
Al numeral 3.8 Recursos tecnológicos a monitorear
Solicitamos amablemente a la entidad la cantidad total de activos en nube y en premisas que se deben monitorear dentro del servicio de SOC.

Respuesta
Ver pregunta 3.

Pregunta 97
Al numeral 3. Especificaciones técnicas

Solicitamos amablemente a la entidad, que dentro de los documentos 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 solicitados. No obstante el proveedor podrá presentar los valores agregados que considere sin que estos generen costos adicionales a la CCB.

Pregunta 98
Al numeral 3.2 Modelo de Operación
"El proponente deberá registrar todos los eventos e incidentes de seguridad que se detecten, asignarle un número único de identificación con el fin de realizar un seguimiento de las acciones tomadas sobre las respuestas ante los incidentes reportados y llevar estadísticas e indicadores con base en este registro."

P:// Amablemente solicitamos a la entidad aclarar si los eventos e incidentes se deben documentar en una herramienta de la Cámara de Comercio o en una provista por el proponente.

Respuesta
Ver respuesta a pregunta 70.

Pregunta 99
Documento: solicitud de cotización
Anexo 2- Aceptación especificaciones técnicas- Premisas

3. La CCB actualmente está en el proceso de migración de toda su infraestructura tecnológica a la nube.
4. El servicio y el modelo de operación del SOC ofrecido deberá adaptarse a los componentes que se aprovisione en la migración total de la infraestructura tecnológica en nube.

Solicitamos de manera atenta a la entidad informar teniendo en cuenta el proceso de migración que se espera a la nube mencionados en los puntos 3 y 4 si la entidadgarantiza la conectividad entre los dispositivos implementados en las instancias deAWS al collector que se centraliza los logs para enviar al SIEM supervisor

Respuesta
La solución debe ser aprovionada en la nube, bajo Modelo SaaS.

Pregunta 100
Documento: solicitud de cotización
Anexo 2- Aceptación especificaciones técnicas- Alcance del servicio

- El proponente deberá presentar un modelo que minimice la transferencia de los logs teniendo en cuenta que la infraestructura y aplicaciones de la CCB estarán en la nube de AWS.

Solicitamos de manera atenta a la entidad informar si luego del proceso de migración garantiza la conectividad entre los dispositivos implementados en las instancias de AWS al collector que se centraliza los logs para enviar al SIEM supervisor.

Respuesta
La solución debe ser aprovionada en la nube, bajo Modelo SaaS.

Pregunta 101
Documento: solicitud de cotización
Anexo 2- Aceptación especificaciones técnicas- Alcance del servicio

- Los tipos de reglas, alertas y notificaciones deben enfocarse en eventos relevantes de seguridad. El proveedor presentará de acuerdo con su experiencia los casos de uso los cuales deberán ser aprobados por la CCB. Los casos de uso mínimos requeridos a monitorear son:
    - Aplicación o modificación de políticas en horarios no autorizados.
    - ataques de denegación de servicio (externos o internos), tráfico desde / hacia sitio con reputación sospechosa, actividades asociadas a conexión de escritorio remoto
    - virus y vulnerabilidades detectadas en la red, Malware no removido, Adware-Aplicaciones no deseadas recurrentes.
    - Actividades asociadas a cuentas de altos privilegios, de procesos, de comunicaciones, intentos masivos de autenticación fallidos, eliminación de usuario o grupo, modificación, eliminación o bloqueo de usuario, autenticación fallida o exitosa desde host no autorizados, cambio de contraseña en horario inusual, modificación de usuarios de alto privilegios, autenticación de usuarios en múltiples host.
    - Cambio en política de auditoría, registros de auditoría borrados, cambios sobre objetos en horario no autorizado, cambios estados de instancia, cambios de configuración horaria.
    - Transacciones SAP: monitoreo de transacciones restringidas, transacciones ejecutadas en horario inusual y transacciones prohibidas.

Solicitamos de manera atenta a la entidad garantizar que dentro de los dispositivos incluidos dentro del servicio de monitoreo se encuentran aquellos capaces de enviar logs de seguridad que le permitan a la herramienta de correlación del SOC detectar las acciones y comportamientos anómalos requeridos dado que el SIEM depende directamente para su función de las fuentes y/o dispositivos que lo alimentan para luego correlacionar, aplicar la inteligencia, analítica y generar los diferentes tipos dealertamiento.

Respuesta
El proponente debe definir la solución tecnológica que permita la correlación, detección y monitoreo de eventos de la infraestructura tecnológica, aplicaciones y bases de datos (nube y On premises).

Pregunta 102
Documento: solicitud de cotización
Anexo 2- Aceptación especificaciones técnicas- Alcance del servicio

- Cuando un evento de seguridad ocurra o está en suceso, el SOC deberá identificarlo y estar en capacidad de relacionar de forma directa o indirecta con otros eventos de seguridad asociados, para ello deberá realizar:
    - Detección de actividades inusuales y recolección de evidencias en caso de incidentes de seguridad, de acuerdo con los niveles de servicio.

Solicitamos de manera atenta a la entidad indicar si en la recolección de evidenciasse tebe tener en cuenta un alcance de análisis forense o es únicamente hacer la recolección que le permita al equipo de la entidad continuar con los siguientes pasos.

Respuesta
No se debe considerar la recolección de evidencia digital. No obstante el proveedor deberá generar recomendaciones para la respuesta a los incidentes presentados.

Pregunta 103
Documento: solicitud de cotización
Anexo 13- Infraestructura premisas aws

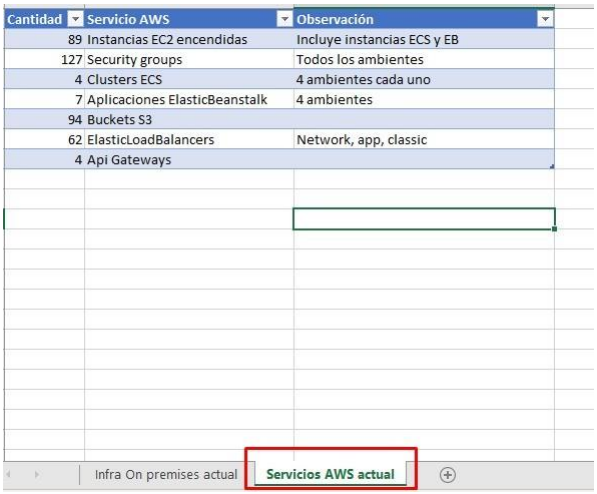
	A	B	C	D	E	F	G	H	I
1	Plataforma	OS Plaform	BD	Version B.D	Capa media	Versión S.O.	VCPUs (x66)	CPU PPC	Memory (GB)
2	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	6		8
3	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		12
4	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		8
5	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		20
6	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2019 or later (64-bit)	4		16
7	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	16		40
8	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	16		40
9	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		12
10	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		18
11	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		18
12	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		18
13	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		18
14	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		18
15	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		18
16	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		18
17	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		18
18	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2019 or later (64-bit)	10		16
19	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2019 or later (64-bit)	10		16
20	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		12
21	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		12
22	VMWare	Microsoft Windows	N/A		MS IIS	Microsoft Windows Server 2016 or later (64-bit)	4		12

Infra On premises actual | Servicios AWS actual

Solicitamos de manera atenta a la entidad indicar si para los servidores windows de la arquitectura On-premises es necesario contemplar la instalación de agentes avanzados para la funcionalidad de FIM (File Integrity Monitoring). De ser así se solicita a la entidad informar para cuantos servidores es necesario contemplar los agentes avanzados.

Respuesta
Ver pregunta 77.

Pregunta 104
Documento: solicitud de cotización
Anexo 13- Infraesctructura premisas aws

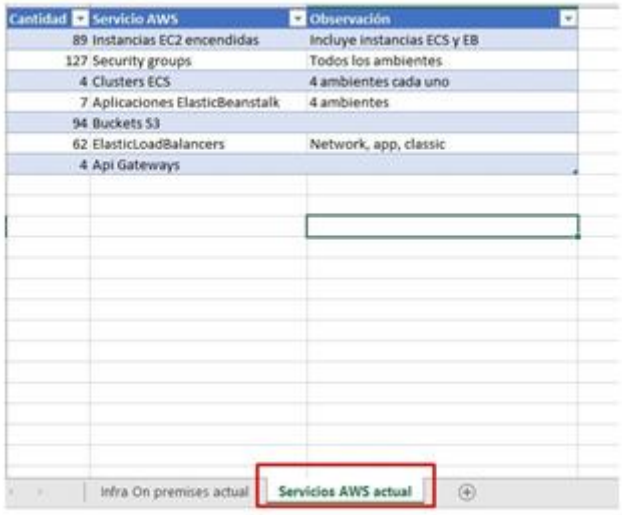


Cantidad	Servicio AWS	Observación
89	Instancias EC2 encendidas	Incluye instancias ECS y EB
127	Security groups	Todos los ambientes
4	Clusters ECS	4 ambientes cada uno
7	Aplicaciones ElasticBeanstalk	4 ambientes
94	Buckets S3	
62	ElasticLoadBalancers	Network, app, classic
4	Api Gateways	

Solicitamos de manera atenta a la entidad aclarar el alcance del monitoreo esperado en la nube de AWS, así mismo indicar si lo que se requiere monitorear es la nube ó los dispositivos que se encuentran instalados y funcionando en las instancias, de ser así se solicita amablemente compartir el inventario de los dispositivos objeto delmonitoreo que se encuentran instalados en las instancias mencionadas en el anexo13 indicando Sistema operativo, versión y cantidad.

Respuesta
Ver pregunta 3.

Pregunta 105
Documento: solicitud de cotización
Anexo 13- Infraesctructura premisas aws



Cantidad	Servicio AWS	Observación
89	Instancias EC2 encendidas	Incluye instancias ECS y EB
127	Security groups	Todos los ambientes
4	Clusters ECS	4 ambientes cada uno
7	Aplicaciones ElasticBeanstalk	4 ambientes
94	Buckets S3	
62	ElasticLoadBalancers	Network, app, classic
4	Api Gateways	

Se solicita de manera atenta a la entidad indicar si dentro de los servicios que tienenactualmente en AWS cuentan con los servicios como Cloud Trail, Cloud Watch, Kinesis y API que se requieren de parte de la entidad en el ambiente en nube parala integración y envío de los eventos a la solución de correlación.

Respuesta
Se cuenta con algunos de estos servicios. El detalle será entregado al proveedor seleccionado.

Pregunta 106
Documento: solicitud de cotización
Anexo 2 – Aceptaciones especificaciones técnicas- Solución tecnológica

- El proponente deberá proporcionar un espacio para el almacenamiento de los registros de auditoría-Logs y asegurar su almacenamiento, disponibilidad y recuperación, así como de la información generada en la ejecución del servicio contratado. Estos registros deben ser almacenados de manera cifrada por un tiempo mínimo de (6) seis meses y se debe garantizar la disponibilidad para cuando la CCB los requiera. Es importante que el proponente defina un plan de respaldo en caso de borrados accidentales o provocados.

Solicitamos de manera atenta a la entidad aclarar la expectativa en la arquitectura para dar cumplimiento a este punto dado que si se requiere que la solución de correlación este implementada en la nube de AWS de la entidad allí deberá estar elalmacenamiento dado que es una parte de la solución.

Respuesta
La solución propuesta debe ser bajo Modelo SaaS.

Pregunta 107
Documento: solicitud de cotización
Anexo 2 – Aceptaciones especificaciones técnicas- Canales de Comunicación

- El proponente deberá disponer de un centro de monitoreo de operaciones que capture la información que será entregada por las fuentes que establezca la CCB a través de canales de comunicación seguros cumpliendo los acuerdos de niveles de servicios establecidos para la prestación del servicio.

Solicitamos de manera atenta a la entidad aclarar de acuerdo a este punto si la expectativa en el despliegue de la solución es que se realice en la nube de AWS delproponente, de ser así solicitamos a la entidad permitir de manera adicional que sepueda realizar el despliegue en la nube con la que cuente el proponente.

Respuesta
La solución debe ser bajo Modelo SaaS en la nube que seleccione el proveedor, garantizando el cumplimiento de los ANS establecidos.

Pregunta 108
Documento: solicitud de cotización
Anexo 2 – Aceptaciones especificaciones técnicas- Solución tecnológica

- El proponente deberá generar o desarrollar los plugins y Application Programming Interface (API, por sus siglas en inglés), para recolección de registros de auditoria -log de los dispositivos y/o aplicaciones, en caso de requerirse según la arquitectura tecnológica propuesta por el proveedor para dar cumplimiento al alcance de la presente solicitud.

Solicitamos de manera atenta a la entidad indicar el estimado de las integraciones por API que se deben estimar durante la duración del contrato.

Respuesta
Se definirá con el proveedor seleccionado.

Pregunta 109
Documento: solicitud de cotización
Anexo 13 – infraestructura premisas aws

Solicitamos de manera atenta a la entidad confirmar para cada uno de los dispositivos que hacen parte del alcance los siguientes aspectos:

- Los dispositivos tienen la capacidad de enviar logs de seguridad.
- La plataforma SAP – HANA cuenta con la capacidad de enviar los eventos alcollector que enviara los eventos al SIEM supervisor.

Respuesta
La solución propuesta debe estar en la capacidad de obtener y procesar los logs generados por los dispositivos. Los logs de seguridad están disponibles en los distintos activos a monitorear.

Pregunta 110
Documento: solicitud de cotización
Anexo 2 – Aceptaciones especificaciones técnicas- Canales de Comunicación

- El proponente es responsable del enlace de comunicaciones entre las soluciones tecnológicas propuestas para la prestación del servicio y los recursos de la CCB en la nube de AWS u On Premises para la transferencia de los logs.

Solicitamos de manera atenta a la entidad aclarar si la solicitud hace referencia loscanales de internet que se requieren para establecer las conexiones VPN con los diferentes sitios (premisa, AWS y SOC).

Respuesta
La solución debe ser Modelo SaaS, toda la conectividad debe ser por internet.

Pregunta 111
Documento: solicitud de cotización
Anexo 2 – Aceptaciones especificaciones técnicas- Activación del servicio

- Lo que se requiera para la instalación y puesta en funcionamiento de las soluciones tecnológicas para el monitoreo deberá ser proporcionada por el proveedor. Una vez se realice la instalación, se deberá realizar la respectiva configuración y certificación de que se está recibiendo la información de la infraestructura tecnológica de la CCB. Esta infraestructura para el monitoreo debe estar instalada en la modalidad de servicio en la CCB durante el tiempo de ejecución del contrato.

Solicitamos de manera atenta a la entidad aclarar si para este ITEM se refieren con "lo que se requiera" a un proyecto llave en mano o si por el contrario hay aspectos de la arquitectura en donde la entidad este en capacidad de colocar algunos de los recursos que se requieran para la

implementación de la solución, esto con el fin deoptimizar los costos del proceso. Adicionalmente se solicita aclarar en donde debeser aprovisionada la solución dado que en este punto se solicita en modalidad de servicio en la CCB pero en otros puntos se solicita en la nube de AWS (de ser así aclarar si se requiere en la nube de la entidad o del proveedor).

Respuesta
Ver pregunta 91.

Pregunta 112
Documento: Solicitud de cotización
Anexo 2- Aceptación Especificaciones Técnicas – Recursos tecnológicos

La correlación, detección, monitoreo y alertamiento de la infraestructura y aplicaciones, incluye las siguientes capas:

Categoría por incluir en monitoreo	Tipo de dispositivo
Aplicaciones	Sistemas con formato SYSLOG
Bases de datos	SQLServer, DB2, RDS (Aurora MySQL, PostgreSQL, SAP – HANA)
Servicios infraestructura	Directorio activo, correo electrónico, Balanceadores de carga, IIS, WAS
Dispositivos de seguridad	Firewall, antimalware, Monitoreo de bases de datos
Recursos nube	Cloud trail, soluciones nativas de AWS: balanceadores, IAM
Soluciones Ciberseguridad	DLP, EDR, NGFWaaS, SD WAN, Múltiple factor de autenticación, CASB

Se solicita de manera atenta a la entidad garantizar que todos los dispositivos incluidos en estas categorías estén en la capacidad de enviar eventos al collector que centralizará y enviará los eventos al SIEM. Adicionalmente se solicita a la entidad confirmar la siguiente información que no se encuentra listada en el anexo 13:

- Motores de datos a monitorear
- Marca y cantidad de dispositivos de seguridad a monitorear (Firewall, antimalware, monitoreo de bases de datos, DLP, EDR, NGFWaaS, SD-WAN,múltiple factor de autenticación y CASB).
- Aplicaciones y servicios en nube y on premise

Respuesta
Ver pregunta 3.

Pregunta 113
Documento: Solicitud de cotización
Anexo 2- Aceptación Especificaciones Técnicas

Solicitamos de manera atenta a la CCB indicarnos cuál es el crecimiento de activos monitorear esperado durante la vigencia del contrato.

Respuesta
Ver pregunta 3.

Pregunta 114
Documento: Solicitud de cotización
Anexo 2- Aceptación Especificaciones Técnicas
Sugerimos de manera atenta a la entidad incluir en el proceso de implementación capacitación dictada directamente por el fabricante del servicio de correlación y monitoreo de eventos de seguridad con el fin de que la CCB tenga el conocimientodel alcance de las soluciones y se tenga mejora continua del servicio.

Respuesta
Se mantienen los requisitos solicitados. No obstante el proveedor podrá presentar los valores agregados que considere sin que estos generen costos adicionales a la CCB.

Pregunta 115
Documento: Solicitud de Cotización
Anexo 2- Aceptación especificaciones técnicas
Sugerimos de manera atenta a la entidad incluir el monitoreo de bases de datos a través del protocolo JDBC, el cual permite tener información detallada del estado dela base de datos, operaciones en tablas, usuarios bloqueados, inicios de sesión fallidos y exitosos, transacciones por segundo, entre otras.

Respuesta
La solución tecnológica propuesta debe cumplir las especificaciones técnicas y casos de uso solicitados en la invitación y garantizar el cumplimiento de los ANS.

Pregunta 116
Documento: Solicitud de Cotización
Anexo 2- Aceptación especificaciones técnicas
Sugerimos de manera atenta a la CCB cambiar el monitoreo de comandos DCL y DML por monitoreo a través de protocolo JDBC para monitorear rendimiento, disponibilidad y seguridad, dentro de los cuales se pueden revisar operaciones en tablas como CREATE/ALTER/DROP/TRUNCATE. Esto en aras de no incrementarlos costos del proyecto incluyendo plataformas adicionales.

Respuesta
Ver pregunta 115.

Pregunta 117
Documento: Solicitud de Cotización
Anexo 2- Aceptación especificaciones técnicas

Sugerimos de manera atenta a la entidad incluir en el proceso de diseño al fabricante de servicio de correlación y monitoreo de eventos de seguridad con el fin de garantizar mayor éxito durante el proceso y cierre del proyecto.

Respuesta
Se mantienen los requisitos solicitados. No obstante el proveedor podrá presentar los valores agregados que considere sin que estos generen costos adicionales a la CCB.

Pregunta 118
Documento: Solicitud de Cotización
Solicitamos saber en que moneda se deber presentar la oferta economcia (sic) si en Pesos Colombianos o se puede presentar en Dolares Americanos.

Respuesta
De conformidad con lo indicado en el numeral 5.1 PROPUESTA ECONÓMICA de la invitación, los valores deben presentarse en pesos colombianos (COP)

A su vez en el anexo 4 nota 2, igualmente se indica dicha información.

Pregunta 119
Numeral 2.11
Los proponentes deberán enviar, en archivos separados, la oferta técnica y la oferta económica de la presente invitación a través de correo electrónico, los valores deben ser expresados en PESOS COLOMBIANOS (COP).
Agradecemos a la Entidad aclarar si es posible presentar la propuesta en Dolares.

Respuesta
No se acepta su observacion. De conformidad con lo indicado en el numeral 5.1 PROPUESTA ECONÓMICA de la invitación, los valores deben presentarse en pesos colombianos (COP)

A su vez en el anexo 4 nota 2, igualmente se indica dicha información.

Pregunta 120
Numeral 3.3.3
El proponente debe ofrecer un equipo de trabajo conformado como se describe a continuación, para lo cual deberá presentar las hojas de vida y las certificaciones de experiencia y formación del personal que dispondrá para la CCB, quienes serán responsables de las actividades descritas para cada rol en el anexo técnico

El equipo de trabajo requerido en el documento debe ser contemplado en las intalaciones de la Entidad o remoto?

Respuesta
Debe ser contemplado en forma remota y tener disponibilidad para sesiones de trabajo en las instalaciones de la Entidad que sean solicitadas por el Supervisor del contrato.

Pregunta 121
Numeral 2.1
3. La CCB actualmente está en el proceso de migración de toda su infraestructura tecnológica a la nube.

En que nube se estan migrando los servicios de la Entidad?
Que servicios se estan migrando?
Que servicios se migraran a la nube?
Respuesta
La nube a la que se está realizando la migración es AWS. Ver pregunta 46

Pregunta 122
Numeral 3.1
El proponente realizará la reconfiguración de las fuentes de premisas a fuentes de nube en la solución que se presente para el servicio a medida que la CCB realice la migración de la infraestructura.

La configuración de las fuentes debe estar a cargo de los administradores de cada fuente, se debe contemplar que el proponente apoye con recomendaciones como realizar la configuración de estas fuentes a los administradores?

Respuesta
De acuerdo.

Pregunta 123
Numeral 3.1
El proponente en conjunto con la CCB definirá serie de reglas, alertas y notificaciones clasificadas y priorizadas para detectar los eventos de las fuentes que se estará monitoreando, las cuales serán reportarlas a la CCB cada vez que se encuentre en riesgo los principios de integridad, disponibilidad o confidencialidad de los activos tecnológicos.

La Entidad ya cuenta con algunas reglas de correlación o CdU prestablecidos que deban ser migrados al servicio propuesto?

Respuesta
Sí, están contemplados en los casos de uso mínimo solicitados.

Pregunta 124
Numeral 3.1
El proveedor presentará de acuerdo con su experiencia los casos de uso los cuales deberán ser aprobados por la CCB.
La Entidad cuenta con las fuentes requeridas para generar las alrtas descritas en este numeral?

Respuesta
El proponente debe definir la solución tecnológica que permita la correlación, detección y monitoreo de eventos de la infraestructura tecnológica, aplicaciones y bases de datos (nube y On premises).

Pregunta 125
Numeral 3.1
El servicio debe contemplar el monitoreo de la actividad en las bases de datos, mediante una solución tipo DAM.

Se debe contemplar el suministro de una plataforma DAM o se debe integrar una ya con la que cuente la Entidad?
En caso afirmativo de tener una plataforma DAM, que plataforma tiene?
En caso contrario de no tener una plataforma DAM, que caracteristicas de los servidores y bases de datos se deben contemplar para dimensionar la solución DAM?

Respuesta
Ver pregunta 13.

Pregunta 126
Numeral 3.1
La solución tecnológica con la prestará el servicio deberá estar aprovisionada en la nube de AWS.
La solución tecnologica propuesta por el proponente debe estar en AWS io puede estar en cualquier nube ya sea publica o privada por razones dpluralidad para todas las propuestas?
Este requerimiento es mandatorio?

Respuesta
Ver pregunta 107.

Pregunta 127
Numeral 3.3.
El proponente es responsable del enlace de comunicaciones entre las
soluciones tecnológicas propuestas para la prestación del servicio y los recursos de la CCB en la nube de AWS u On Premises para la transferencia de los logs.
Se deben contemplar canales de comunicaciones dedicados entre el datacentery los colectores o es posible realizarlo a traves de conexiones cifradas VPN?

Respuesta
Ver pregunta 107.

Pregunta 128
¿Número de dispositivos o fuentes a correlacionar?

Respuesta
Ver pregunta 3.

Pregunta 129
¿Se cuenta con un listado con caracterisitcas de referencias y cantidades de la fuentes a integrar con el SIEM?

Respuesta
Ver pregunta 3.

Pregunta 130
¿Las fuentes se encuentran en un unico sitio o estan distribuidas? ,en caso afirmativo de estar distribuidas por favor señalar las ubicaciones.

Respuesta
Ver pregunta 3.

Pregunta 131
¿La infraestrucutra a monitorear en que ambiente se encuentra? (Fisico, nube, hibrido) especificar la arquitectura.

Respuesta
Ver pregunta 3.

Pregunta 132
¿Se debe contemplar dentro de la oferta el monitroeo de disponibilidad y salud de las plataformas?

Respuesta
Ver pregunta 73.

Pregunta 133
¿La entidad cuenta con un equipo o servico de respuesta a incidentes?

Respuesta
Esta información será compartida con el proponente seleccionado.

Pregunta 134
¿Cómo plataforma de gestión de casos se puede utilizar la del servicio de SOC?

Respuesta
Sí, el proponente podrá utilizar plataformas para la gestión de casos.

Pregunta 135
¿Actualmente tiene servicio de SOC en la entidad? En caso afirmativo, se cuenta con un promedio de incidentes en el mes?

Respuesta
Esta información será compartida con el proponente seleccionado.

Pregunta 136
¿Se tiene alguna restricción a nivel de ubicación de los centros de datos del servicio?

Respuesta
El aprovisionamiento de los servicios debe realizarse dentro de las zonas de georreferenciación que se encuentren definidas en la reglamentación de la Ley 1581 de 2012.

Pregunta 137
¿Cuentan con algún deseable a nivel de servicio o que se presente como complemento al servicio de SOC?

Respuesta
El proveedor podrá presentar los valores agregados que considere sin que estos generen costos adicionales a la CCB.

Pregunta 138
Anexo 2. Numeral 3.1: El proponente realizará la reconfiguración de las fuentes de premisas a fuentes de nube en la solución que se presente para el servicio amedida que la CCB realice la migración de la infraestructura.
Se solicita a la entidad aclarar si la reconfiguración de la fuentes se realizará al 100% de los activos relacionados a qué cantidad y máquinas específicas.

Respuesta
Ver pregunta 3.

Pregunta 139
Anexo 2. Numeral 3.1
El servicio debe contemplar el monitoreo de la actividaden las bases de datos, mediante una solución tipo DAM u otra(s) que permita gestionar

Se solicita a la entidad aclarar le alcance de equipos a los cuales se les realizará estos análisis y si se contará con el apoyo del equipo interno de FUNCIÓN PÚBLICA para determinar los activos específicos.

Respuesta
Ver pregunta 3. En la Entidad no se cuenta con un equipo interno de FUNCIÓN PÚBLICA.

Pregunta 140
Anexo 2 Numeral 3.2.:
La solución tecnológica con la prestará el servicio deberá estar aprovisionada en la nube de AWS.

Se solicita a la entidad ampliar el despliegue de la herramienta utilizada en premisas de Datacenter del oferente.

Respuesta
Ver pregunta 107

Pregunta 141
Anexo 2 Numeral 3.3.: El proponente es responsable del enlace de comunicaciones entre las soluciones tecnológicas propuestas para la prestación del servicio y los recursos de la CCB en la nube de AWS u On premises para la transferencia de los logs.

Se agradece a la entidad confirmar si es correcto nuestro entendimiento acerca que el oferente provee el canal de comunicaciones únicamente y que CCB provee las condiciones de energía, colocacipon on-premises y demás condiciones físico/ambientales que puedan generar un costo adicional implcito para garantizar el correcto funcionamiento del enlace de comunicaciones

Respuesta
Ver pregunta 107.

Pregunta 142
Anexo 13 Hoja 2infra on premises actual”
Se solicita a la entidad aclarar versión de B.D del servidor Microsoft Windows Serve 2008 R2 (64-bit)

Respuesta
Ver pregunta 3.

Pregunta 143
Anexo 13 Infraestructura premisas aws, Hoja “Servicios AWS actual”
Se solicita a la entidad aclarar las B.D. de los servidores (de haberlas) en las instalaciones AWS

Respuesta.
Ver pregunta 3.

Pregunta 144

3.3.2 EXPERIENCIA DEL PROPONENTE

El proponente deberá acreditar experiencia mediante la prestación de hasta cuatro (4) certificaciones de contratos ejecutados y/o en ejecución a partir del 1 de enero de 2018

Solicitamos con el mayor respeto a la entidad aceptar certificaciones de contratos ejecutados y/o en ejecución a partir del 01 de enero de 2015.

Respuesta

No se acepta su observación, se mantiene lo establecido en la invitación.

Pregunta 145

En el numeral 3.3.2. Experiencia del proponente, la entidad solicita losiguiente:

"El proponente deberá acreditar experiencia mediante la presentación de hasta 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 $1.713.600.000 antes de IVA…"

Se sugiere a la entidad que, para complementar el cumplimiento de dicho requisito se solicite que,al menos en una de las cuatro certificaciones se acredite operación de servicios de SOC 24/7 por mínimo de 3 años.

Respuesta

Se mantiene lo solicitado en la invitación.

Pregunta 146

En el numeral 3.3.3. Equipo de trabajo, la entidad relaciona las hojas de vida del equipo de trabajo. Se solicita respetuosamente a la entidad aclarar cuales son las hojas de vida que se deben presentar junto con la propuesta.

Respuesta

Ver pregunta 44.

Pregunta 147

En el numeral 3.3.3. Equipo de trabajo, la entidad solicita lo siguiente para la hoja de vida del Coordinador SOC:

Un (1) Coordinador de SOC: Profesional en ingeniería de sistemas o afines según el SNIES que tenga como mínimo 2 años de experiencia en la coordinación de operaciones de contratos cuyo objeto se relacione con la correlación, detección y monitoreo de los eventos de Seguridad, debe contar con certificación en el uso de las herramientas propuestas por el proponente, en la versión más reciente con la que se prestará el servicio.

Rol: Será el responsable de coordinar la ejecución de las actividades del contrato.

Solicitamos respetuosamente a la entidad que el requisito solicitado de la certificación en el usode las herramientas propuestas no se requiera específicamente al perfil de Coordinador SOC, dadoque el rol que tiene dicho perfil es la coordinación de actividades y para el ejercicio de sus funciones no es necesario que el perfil dependa de dichas certificaciones. Sin embargo, estamos de acuerdo que el proponente

incluya dentro de su equipo de trabajo por lo menos un profesional con la certificación en el uso de las herramientas propuestas por el proponente.

Por lo anterior sugerimos que, junto con la propuesta, se debería presente al menos un profesional que participe en el proceso de implementación y que cuente con las certificaciones de en las herramientas propuestas.

Lo anterior, garantiza la pluralidad de oferentes y no afecta la prestación del servicio.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 148
En el numeral 6.3. Segunda fase de evaluación de las ofertas, la entidad solicita lo siguiente:

Ceritifcado de seguridad de la información	Corresponde a la tenencia de un certificado de calidad ISO 27001:2013 Vigente, el cual debe ser presentado junto con la propuesta	5

Solicitamos respetuosamente a la entidad que, para el requisito, se adicione que la empresa deba tener certificado ISO 27001:2013 y que dentro del alcance de dicho certificado esten incluidos servicios que respondan al objeto del contrato: ejemplo: Servicios de SOC y/o atención de incidentes.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 149
En el numeral 3.8. Recursos tecnológicos para monitorear, del anexo 2, la entidad solicita lo siguiente:

"El proponente para la generación de la propuesta económica deberá considerar hasta 2500 EPS (eventos por segundo), y un crecimiento hasta un 15% en los 36 meses."

Solicitamos a la entidad si los eventos por segundo corresponden a la infraestructura on premise y a nube y de ser asi, solicitamos que se aclare que porcentaje de eventos por segundo corresponde a on premise y a nube.

Respuesta
Los EPS corresponden al total solicitado.

Pregunta 150:
En el numeral 2.1 Premisas, del anexo 2, la entidad solicita lo siguiente:

"La CCB actualmente está en el proceso de migración de toda su infraestructura tecnológica a la nube."

Solicitamos a la entidad informar aproximadamente en cuanto tiempo se estima que toda la infraestructura estará migrada en la nube.

Respuesta
Ver pregunta 45

Pregunta 152
Equipo de trabajo, a
Un (1) Líder de cuenta: Profesional en ingeniería de sistemas o afines según el SNIES que tenga como mínimo 2 años de experiencia en gerencia de proyectos relacionados con la prestación de servicios SOC.

Rol: Responsable permanente del contrato quien poseerá la misión completa del mismos. El proponente debe garantizar que esta persona se encuentre en la ciudad de Bogotá D.C.

Solicitamos valorar la posibilidad de ofrecer un Gerente de SOC físicamente en San José, Costa Rica y a su vez un Gerente de Proyecto físicamente en Bogotá D.C, Colombia.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 153
Equipo de trabajo,
b. Analistas de operación: Deben contar con certificación en el uso de las herramientas propuestas por el proponente, en la versión más reciente con la que se prestará el servicio.

Solicitamos considerar la posibilidad de sustituir y/o subsanar las certificaciones en el uso de las herramientas de monitoreo, por certificaciones asociadas a la gestión de la seguridad de la información y gestión de las TIC, como ISO 27001, COBIT 5, ITIL y CSFPC. Lo anterior considerando el hecho de que las herramientas de monitoreo son únicamente el medio por el cual se realizan las detecciones de amenazas, lo cual no garantiza la capacidad de los analistas de operación para gestionar de manera suficiente y adecuada ante las amenazas de seguridad que se presenten.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 154
3.2 Solución tecnológica
El proponente deberá proporcionar un espacio para el almacenamiento de los registros de auditoría-Logs y asegurar su almacenamiento, disponibilidad y recuperación, así como de la información generada en la ejecución del servicio contratado. Estos registros deben ser almacenados de manera cifrada por un tiempo mínimo de (6) seis meses y se debe garantizar la disponibilidad para cuando la CCB los requiera. Es importante que el proponente defina un plan de respaldo en caso de borrados accidentales o provocados.

Agradecemos aclarar si la retención de logs por un periodo de 6 meses la requieren en modo caliente o en modo frío.

Respuesta
Ver pregunta 1.

Pregunta155
Agradecemos aclarar si adicional al monitoreo y alertamiento de las amenazas detectadas por la plataforma, se requiere que el proveedor brinde servicios de respuesta a incidentes cibernéticos (Investigación, contención y erradicación).

Respuesta
No se requiere. No obstante el proveedor podrá presentar los valores agregados que considere sin que estos generen costos adicionales a la CCB.

Pregunta 156
En el apartado 3.1 Alcance del servicio se indica lo siguiente:
El proponente deberá diseñar el modelo adecuado para el monitoreo de los eventos de seguridad de la infraestructura tecnológica (On premises y Nube), aplicaciones y bases de datos, asegurando visibilidad, detección, prevención y el alertamiento.

1: ¿Cuantos puntos o centros de datos físicos se requiere tener en cuenta para monitorear? Este dato es indispensable para el correcto dimensionamiento de requerimientos de hardware, canal requeridos para la recolección de logs.

Respuesta
Un Centro de Datos Físico.

2: ¿Para los componentes de hardware que sean requeridos para la implementación de Sondas o Sensores necesarios para la recolección de logs serán dispuestos por parte de CCB o deben ser dispuestos por parte del proponente?

Respuesta
Ver pregunta 107

Pregunta 157
Por razones de Dimensionamiento y para poder ofrecer un modelo que minimice la transferencia de logs en AWS, solicitamos nos indiquen ¿En qué regiones está dispuesto el servicio de AWS actualmente para CCB?

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 158
En el apartado 3.1 Alcance del servicio se indica lo siguiente sobre los casos de uso a desarrollar y monitorear:
Cambio en política de auditoría, registros de auditoría borrados, cambios sobre objetos en horario no autorizado, cambios estados de instancia, cambios de configuración horaria

¿Por favor aclarar si el monitoreo de eventos de seguridad requiere también el monitoreo de eventos tipo FIM (File Integrity Monitoring)?

Respuesta
Ver pregunta 77.

Pregunta 159
En el apartado 3.2 Modelo de operación / Solución Tecnológica se indica lo siguiente:
La solución tecnológica con la prestará el servicio deberá estar aprovisionada en la nube de AWS.

¿Se requiere que la implementación de la plataforma a ofertar se encuentra dispuesta en HA?

Respuesta
El proveedor deberá cumplir con los ANS solicitados.

Pregunta 160
En el apartado 3.2 Modelo de operación / Solución Tecnológica se indica lo siguiente: *El proponente deberá proporcionar un espacio para el almacenamiento de los registros de auditoría-Logs y asegurar su almacenamiento, disponibilidad y recuperación, así como de la información generada en la ejecución del servicio contratado. Estos registros deben ser almacenados de manera cifrada por un tiempo mínimo de (6) seis meses y se debe garantizar la disponibilidad para cuando la CCB los requiera. Es importante que el proponente defina un plan de respaldo en caso de borrados accidentales o provocados.*

¿El espacio requerido para el almacenamiento de logs debe ser dispuesto de igual manera en AWS?

Respuesta
En la nube que el proveedor seleccionado defina.

Pregunta 161
En el apartado 3.3 Canales de comunicación se indica lo siguiente:
El proponente es responsable del enlace de comunicaciones entre las soluciones tecnológicas propuestas para la prestación del servicio y los recursos de la CCB en la nube de AWS u On Premises para la transferencia de los logs.

¿Por favor aclarar si es responsabilidad del proponente el aprovisionamiento del canal de comunicaciones requerido para la transferencia de logs, o si por el contrario será dispuesto por la CCB?

Respuesta
Ver pregunta 110.

Pregunta 162
Invitación / 3.3.2 Experiencia del proponente
La experiencia a acreditar solicitada puede ser presentada por sucursales del proponente en el extranjero?

Respuesta
Dado que las sucursales mantiene la unidad de firma social si se acepta la experiencia de sucursales del proponente en el extranjero.

Pregunta 163
Idioma / 2.12 Idioma
El servicio puede ser prestado por personal que hable un idioma diferente al español?

Respuesta
Si bien el personal puede hablar un idioma diferente al español, se precisa que el interlocutor del equipo de trabajo del proponente ante la CCB debe hablar en español, a su vez se aclara que en las premisas de la invitación se indica que “Todos los entregables deben ser elaborados en idioma español”.

Pregunta 164
Anexo 2 / 3.8 recursos tecnológicos a monitorear

Se solicita muy amablemente la estimación de la cantidad diaria en GB de almacenamiento requerida para el servicio. Esto dado que dependiendo del tipo de aplicación la cantidad de almacenamiento requerido por evento varia y no es suficiente información para dimensionar únicamente la información suministrada.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 165
Anexo 10 / CARTA DE COMPROMISO SOLUCIÓN TECNOLÓGICA PROPUESTA
Se solicita muy amablemente ajustar o revisar el nombre de la soluciones tecnológicas propuestas en la tabla, dado que el nombre de las soluciones a proponer allí no guardan relación con el objeto de esta invitación.

Respuesta
Se ajusta la información del anexo 10 Carta de Compromiso solución Tecnológica propuesta, mediante adenda.

Pregunta 166
Anexo 2 / 3.3 Canales de comunicación
De acuerdo a la solicitud de que el proponente debe suministrar el enlace de comunicación, se solicita muy amablemente las especificaciones para este enlace de comunicaciones (capacidad, redundancia, punto de origen y destino)

Respuesta
Ver respuesta 110.

Pregunta 167
Al numeral 1.6 Infraestructura tecnológica
Solicitamos amablemente a la entidad detallar y especificar los activos de TI y de seguridad de la entidad que harán parte de las fuentes a recolectar y correlacionar.

Respuesta
Ver pregunta 3.

Pregunta 168
Al numeral 1.6 Infraestructura tecnológica
Solicitamos amablemente a la entidad detallar y especificar los activos de TI alojados en las diferentes nubes que harán parte de las fuentes a recolectar y correlacionar.

Respuesta
Ver pregunta 3.

Pregunta 169
Al numeral 1.6 Infratestructura Tecnológica
Solicitamos amablemente a la entidad aclarar y especificar si el tercero encargado de la administración de la infraestructura tecnologica de la CCB realizará las tareas y actividades de configuración y aprovisionamiento necesarios para la recolección e ingesta de datos hacia los servicios del SOC a poponer.

Respuesta

El encargado de la administración de la IT será responsable de la configuración del sistema operativo de la infraestructura en AWS de la CCB. La recolección e ingesta será responsabilidad del proveedor del SOC.

Pregunta 170
Al numeral 3.1
3.1 Alcance del servicio:
El proponente realizará la reconfiguración de las fuentes de premisas a fuentes de nube en la solución que se presente para el servicio a medida que la CCB realice la migración de la infraestructura..
Solicitamos amablemente a la entidad aclarar y detallar el objetivo de este requerimiento. Es solo el reapuntamiento de las fuentes o que tipo de configuración y quien lo debe realizar, entendiendo que la entidad cuenta con un tercero que administra su infraestructura tecnológica.

Respuesta
Ver pregunta 169.

Pregunta 171
3.1 Alcance del servicio:
… Los tipos de reglas, alertas y notificaciones deben enfocarse en eventos relevantes de seguridad…
Solicitamos amablemente a la entidad aclarar y especificar si la CCB cuenta con una solución de monitoreo y administración de usuarios privilegiados.

Respuesta
No

Pregunta 172
3.1 Alcance del servicio:
… Los tipos de reglas, alertas y notificaciones deben enfocarse en eventos relevantes de seguridad…
Solicitamos amablemente a la entidad aclarar y especificar cual es la plataforma SAP de la entidad y con que módulos de SAP cuentan.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 173
3.1 Alcance del servicio:
El servicio debe contemplar el monitoreo de la actividad en las bases de datos, mediante una solución tipo DAM u otra(s) que permita gestionar como mínimo los siguientes casos de uso
Solicitamos amablemente a la entidad aclarar y especificar si cuentan con una solución de monitoreo y protección de Bases de Datos o esta debe ser provista por el proponente.

Respuesta
El proveedor debe definir y presentar la solución tencológica que de respuesta a las especificaciones técnicas solicitadas. La CCB no contará con un DAM a integrar con la solución del proveedor.

Pregunta 174
3.1 Alcance del servicio:
El servicio debe contemplar el monitoreo de la actividad en las bases de datos, mediante una solución tipo DAM u otra(s) que permita gestionar como mínimo los siguientes casos de uso.

Solicitamos amablemente a la entidad aclarar y especificar:
- Cual es la cantidad de bases de datos e instancias de la entidad y donde estan ubicadas (en premisas o en nube)
- Cual es la cantidad de servidores de bases de datos, y cual es la cantidad de cores asignados a estos servidores
- Cual es la cantidad de transacciones de bases de datos
- Cual es la referencia de bases de datos a monitorear

Respuesta
Ver pregunta 3.

Pregunta 175
3.2 Modelo de Operación:
Solución Tecnológica:
Solicitamos amablemente a la entidad aclarar y especificar si cuentan con recursos sobre ambientes virtuales para el aprovisionamiento de infraestrura, tipo servidores virtuales.

Respuesta
Ver pregunta 71

Pregunta 176
3.2 Modelo de Operación:
Solución Tecnológica:
… La solución tecnológica con la prestará el servicio deberá estar aprovisionada en la nube de AWS.
Solicitamos amablemente a la entidad validar en pro de tener opciones y pluralidad de oferentes, replantear este requerimiento en cuanto a que se limita a una única solución en la nube de AWS, teniendo en cuenta que la solución provista puede estar alojada en nubes privadas o propias del fabricante u operador, garantizando el buen desempeño de la misma y los criterios de seguridad como disponibilidad, integridad y confidencialidad de la información.

Respuesta:
Ver pregunta 71.

Pregunta 177
3.2 Modelo de Operación:
Solución Tecnológica:
...El proponente hará monitoreo constante del estado de disponibilidad, desempeño y salubridad de solución tecnológica propuesta para la prestación del servicio solicitado y generará los reportes correspondientes de caídas que se presenten y que puedan afectar los acuerdos de niveles de servicio y porcentajes de disponibilidad contratados por la CCB.
Solicitamos amablemente a la entidad aclarar y especificar si cuentan con herramientas o soluciones para el monitoreo del estado de salud de la infraestructura tecnologica a monitorear.

Respuesta
Ver pregunta 73.

Pregunta 178
En cuanto al requerimiento - "Las soluciones tecnológicas de monitoreo para la infraestructura, aplicaciones y bases de datos deberán estar incluidas por Gartner en el cuadrante mágico o peer insight en la versión más reciente.

Se solicita comedidamente a la Entidad retirar esta condición del pliego, toda vez que lo que se busca es un servicio que cubra los requerimientos y no una solución específica; esto ofrecería la posibilidad de tener una pluralidad de oferentes dentro del proceso.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 179
En cuanto al requerimiento - "El proponente deberá proporcionar un espacio para el almacenamiento de los registros de auditoría-Logs y asegurar su almacenamiento, disponibilidad y recuperación, así como de la información generada en la ejecución del servicio contratado. Estos registros deben ser almacenados de manera cifrada por un tiempo mínimo de (6) seis meses y se debe garantizar la disponibilidad para cuando la CCB los requiera. Es importante que el proponente defina un plan de respaldo en caso de borrados accidentales o provocados."

Respetuosamente solicitamos indicar si la Cámara de Comercio de Bogotá tiene alguna restricción para el procesamiento y almacenamiento de los datos o logs de la infraestructura monitoreada sobre servicios de nube (local o fuera del país). De igual forma, se solicita a la entidad aclarar si las herramientas para el cifrado de los registros tienen alguna restricción.

Respuesta
Ver pregunta 136.

Pregunta 180
Se solicita conocer la concurrencia de horarios en la que los usuarios de la CCB acceden a los aplicativos críticos de la organización.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 181
Teniendo en cuenta el requerimiento –"Transacciones SAP: Monitoreo de transacciones restringidas, transacciones ejecutadas en horario inusual y transacciones prohibidas" se solicita a la entidad atentamente aclarar y especificar a que tipo de transacciones hace referencia o qué tipo de alerta se quiere monitorear.

Respuesta
Esta información será compartida con el proponente seleccionado.

Pregunta 182
Es de nuestro entendimiento que el monitoreo que se debe realizar por parte de la herramienta de SIEM que soporta el servicio de SOC debe ser en tiempo real para cumplir los SLAs solicitados. Agradecemos aclarar si nuestro entendimiento es acertado.

Respuesta
Ver respuesta 89

Pregunta 183
Se solicita amablemente a la entidad aclarar si el oferente esta en la capacidad de ofrecer una o varias herramientas para cumplir con diferentes requerimientos.

Respuesta
El proponente debe definir la solución tecnológica que permita la correlación, detección y monitoreo de eventos de la infraestructura tecnológica, aplicaciones y bases de datos (nube y On premises).

Pregunta 184
Solicitamos amablemente aclarar si se requiere monitoreo de cambios de configuración para todos los dispositivos de la infraestructura tecnológica de la Cámara de Comercio de Bogotá.

Respuesta
De acuerdo con los solicitado en los casos de uso mínimos requeridos.

Pregunta 185
¿Teniendo en cuenta que La CCB cuenta actualmente con un servicio de SOC? De ser así por favor indicar cuál es su herramienta de SIEM y arquitectura del servicio.

Respuesta
Esta información será compartida con el proponente seleccionado.

Pregunta 186
Se solicita respetuosamente a la entidad indicar cual es la cantidad de usuarios de la CCB y concurrencia en los horarios de operación.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 187
Para el caso de uso especifico solicitado para las transacciones SAP: monitoreo de transacciones restringidas, transacciones ejecutadas en horario inusual y transacciones prohibidas, se solicita por favor aclarar cuales de los componentes de las fuentes de correlación hacen parte de la aplicación de SAP. Por favor informar si estos componentes permiten exportar logs vía Syslog.

Respuesta
Sí.

Pregunta 188
¿Las bases de datos que se presentan en el anexo información sobre bases de datos cuentan con la capacidad de exportar logs, vía Syslog (incluyendo bases de datos en AWS)?

Respuesta
La solución debe permitir monitorear las bases de datos en forma nativa.

Pregunta 189
Para la integración de las fuentes de información que se encuentras On-premise. ¿La entidad CCB cuenta con espacio en rack para la instalación de un appliance?

Respuesta
Ver pregunta 71.

Pregunta 190
Dado que la entidad CCB tiene en su alcance fuentes de información en ambiente AWS, se solicita confirmar si CCB dispone de una instancia para el despliegue de un sensor en su ambiente AWS o las instancias se debe proveer dentro del servicio. Esto puede causar valores adicionales.

Respuesta
Ver pregunta 71.

Pregunta 191
Se solicita a la entidad indicar si para el monitoreo de la base se requiere una solución de propósito especifica tipo DAM, dado que se pueden desarrollar este servicio de Monitoreo con soluciones dentro del servicio que no necesariamente son soluciones de DAM.

Respuesta
El servicio debe contemplar el monitoreo de la actividad en las bases de datos, mediante una solución tipo DAM u otra(s)

Pregunta 192
Agradecemos aclarar si la solución de SIEM deberá realizar la correlación de eventos y monitoreo en tiempo real para dar cumplimiento a los SLAs solicitados por la entidad.

Respuesta
Ver pregunta 89

Pregunta 193
Teniendo en cuenta el requerimiento- “Para las personas jurídicas, la duración de la sociedad debe ser por lo menos la vigencia del contrato y un año más.”. Se solicita a la entidad, indicar por cuanto tiempo se debe ofertar el servicio.

Respuesta
De conformidad con el numeral 4.1 de la invitación el plazo de ejecución es de 3 años, por lo tanto se debe ofertar el servicio por 3 años.

Pregunta 194
¿Se solicita amablemente a la entidad, indicar si la DB de SQL AWS está en SaaS o es PaaS SQL AWS?

Respuesta
Ver pregunta 3.

Pregunta 195
¿Se solicita a la entidad aclarar qué tipo de red LAN tiene la entidad? (Fibra-Cobre/1Gb-10Gb)?

Respuesta
Ver pregunta 71.

Pregunta 196
Se solicita amablemente a la CCB se indique si el SIEM que soporta el servicio deberá tener monitoreo de transacciones sintéticas para tener alertamiento en caso de caída de aplicaciones misionales.

Respuesta
No.

Pregunta 197
Se solicita amablemente a la CCB aclarar si en la herramienta de SIEM para el servicio de SOC debe permitir activar la funcionalidad de indicadores de compromiso para permitir identificar dispositivos y usuarios en riesgo o comprometidos.

Respuesta
Ver pregunta 74

Pregunta 198
Solicitamos amablemente a la CCB aclarar si el monitoreo solicitado para configuraciones es únicamente para bases de datos o para todos los dispositivos de la infraestructura tecnológica de la CCB que se deben incluir en el servicio.

Respuesta
El proponente debe definir la solución tecnológica que permita la correlación, detección y monitoreo de eventos de la infraestructura tecnológica, aplicaciones y bases de datos (nube y On premises) y cumplir con los casos de uso mínimos requeridos en las especificaciones técnicas de esta invitación.

Pregunta 199
Se le solicita amablemente a la CCB confirmar si tienen alguna preferencia por diseño físico o virtual para la solución de protección de bases de datos en lo que se relaciona con los appliance. ¿La entidad tendría disponibilidad de recursos en sus ambientes virtuales on-premise para el despliegue de la solución?

Respuesta
Ver pregunta 71.

Pregunta 200

Solicitamos amablemente a la entidad aclarar si es necesario monitorear la integridad de archivos para los servidores Windows y Linux

Respuesta

Ver pregunta 77.

Pregunta 201

Teniendo en cuenta – "Monitoreo de la actividad en las bases de datos" hace referencia a que la solución deberá únicamente hacer el registro de la actividad para los criterios de usuarios y comandos definidos y presentarlo en la consola de administración de la solución y permitir obtener esta información a través de reportes.

Dentro del Inventario de bases de datos, la entidad indica que posee servicios tipo DBaaS en Amazon RDS y on-premise, solicitamos a la entidad aclarar si es permitido el uso de varias soluciones o si debe ser cubierto por una única solución.

Respuesta

El servicio debe contemplar el monitoreo de la actividad en las bases de datos, mediante una solución tipo DAM u otra(s). El proponente debe definir la solución tecnológica que permita la correlación, detección y monitoreo de eventos de la infraestructura tecnológica, aplicaciones y bases de datos (nube y On premises).

Pregunta 202

Teniendo en cuenta los recursos tecnológicos de la entidad:

3.8 Recursos tecnológicos para monitorear

La correlación, detección, monitoreo y alertamiento de la infraestructura y aplicaciones, incluye las siguientes capas:

Categoría por incluir en monitoreo	Tipo de dispositivo
Aplicaciones	Sistemas con formato SYSLOG
Bases de datos	SQLServer, DB2, RDS (Aurora MySQL, PostgreSQL, SAP – HANA)
Servicios infraestructura	Directorio activo, correo electrónico, Balanceadores de carga, IIS, WAS
Dispositivos de seguridad	Firewall, antimalware, Monitoreo de bases de datos
Recursos nube	Cloud trail, soluciones nativas de AWS: balanceadores, IAM
Soluciones Ciberseguridad	DLP, EDR, NGFWaaS, SD WAN, Múltiple factor de autenticación, CASB

Se solicita respetuosamente a la entidad indicar, si la solución(es) ofrecidas necesitan de la instalación de agentes, más específicamente en la base de datos (SAP-HANA) y recursos Cloud.

R*espuesta*
El proponente debe definir la solución tecnológica que permita la correlación, detección y monitoreo de eventos de la infraestructura tecnológica, aplicaciones y bases de datos (nube y On premises). El proponente deberá generar o desarrollar los plugins y Application Programming Interface (API, por sus siglas en inglés), para recolección de registros de auditoria -log de los dispositivos y/o aplicaciones, en caso de requerirse según la arquitectura tecnológica propuesta por el proveedor para dar cumplimiento al alcance de la presente solicitud.

Pregunta 203
Se recomienda amablemente a la CCB se pueda contar con una solución que se integre a la red a través de hardware appliance y se complemente con agentes instalados en las bases de datos.

R*espuesta*
Ver pregunta 77.

Pregunta 204
ANEXO 2
NUMERAL 3
3.1 Alcance del Servicio
El proponente deberá presentar un modelo que minimice la transferencia de los logs teniendo en cuenta que la infraestructura y aplicaciones de la CCB estarán en la nube de AWS.

Se solicita a la entidad aclarar si dentro de esos modelos aplican , tecnológias como cifrado de información, compresión, normalización, etc. De lo contrario específicar a cuales modelos serian los aprobados para el cumplimiento de este requisito.

Respuesta
Sí.

Pregunta 205
ANEXO 2
NUMERAL 3
3.1 Alcance del Servicio
El proponente realizará la reconfiguración de las fuentes de premisas a fuentes de nube en la solución que se presente para el servicio a medida que la CCB realice la migración de la infraestructura.
Amablemente solicitamos a la entidad aclarar, si las labores correspondientes al envío de logs, de los serevidores migrados a la nube, ¿estarán a cargo de la CCB?

Respuesta
Ver preguntas 122 y 169.

Pregunta 206
ANEXO 2
NUMERAL 3
3.1 Alcance del Servicio
El proveedor presentará de acuerdo con su experiencia los casos de uso los cuales deberán ser aprobados por la CCB. Los casos de uso mínimos requeridos a monitorear son:
o Aplicación o modificación de políticas en horarios no autorizados.

o ataques de denegación de servicio (externos o internos), tráfico desde / hacia sitio con reputación sospechosa, actividades asociadas a conexión de escritorio remoto
o virus y vulnerabilidades detectadas en la red, Malware no removido, Adware-Aplicaciones no deseadas recurrentes.
o Actividades asociadas a cuentas de altos privilegios, de procesos, de comunicaciones, intentos masivos de autenticación fallidos, eliminación de usuario o grupo, modificación, eliminación o bloqueo de usuario, autenticación fallida o exitosa desde host no autorizados, cambio de contraseña en horario inusual, modificación de usuarios de alto privilegios, autenticación de usuarios en múltiples host.
o Cambio en política de auditoría, registros de auditoría borrados, cambios sobre objetos en horario no autorizado, cambios estados de instancia, cambios de configuración horaria.
o Transacciones SAP: monitoreo de transacciones restringidas, transacciones ejecutadas en horario inusual y transacciones prohibidas.

Favor aclarar con que protócolo, medios, cuentan las aplicaciones SAP para el envío de logs.
Favor confirmar, que dentro de los logs enviados, si se encuentra información de la cual se pueda extractar evidencia de transacciones restringidas, transacciones ejecutadas y transacciones prohibidas.

Respuesta
Ver pregunta 109.

Pregunta 207
El servicio debe contemplar el monitoreo de la actividad en las bases de datos, mediante una solución tipo DAM u otra(s) que permita gestionar como mínimo los siguientes casos de uso:
o Monitoreo de Usuarios:
▪ Usuarios no autorizados
▪ Usuarios Desarrolladores
▪ Usuarios de Altos privilegios

1. Amablemente solictamos a la entidad aclarar, si se debe incluir en el servicio una solución DAM.
2. Favor aclarar, si las aplicaciones de bases de datos tienen la auditoría habilitada y cuentan con medios para el envío de estos eventos de auditoría, mediante protocólos estándar o un ftp de archivo.

Respuesta
Ver pregunta 13 y 109.

Pregunta 208
ANEXO 2
3. 2 Modelo de Operación
Certificación en el uso las herramientas propuestas por EL proponente, en la versión más reciente con la que se prestará el servicio.
Solicitamos aclarar, como espera la entidad que los proponentes validen el cumplimiento de este requerimiento.

Respuesta
Con la presentación de los requisitos establecidos en el numeral 3.3.3.

Respuesta 209
ANEXO 2
3. 2 Modelo de Operación

Las soluciones serán licenciadas y deben cumplir las condiciones técnicas necesarias para realizar el monitoreo sobre la plataforma tecnológica, aplicaciones y bases de datos incluidas en el alcance de monitoreo. Por lo tanto, el proponente instalará, configurará y mantendrá las soluciones a utilizar en la prestación del servicio, recursos y complementos necesarios para la captura, correlación, análisis, monitoreo, alertas y gestión de eventos e incidentes de seguridad sobre la plataforma tecnológica de la CCB.

Favor aclarar el alcance de este servicio, entendiendo que la configuración del envío de eventos desde las diferentes fuentes a la solucion propuesta, debe ser realizada por los administradores de las plataformas tecnológicas (SAP, Bases de Datos, Firewall, etc.). Sea por los administradores de la CCB o en su defecto algun tercero encargado de las plataformas.

Respuesta
Ver pregunta 122

Pregunta 210
ANEXO 2
3. 2 Modelo de Operación
El proponente hará monitoreo constante del estado de disponibilidad, desempeño y salubridad de solución tecnológica propuesta para la prestación del servicio solicitado y generará los reportes correspondientes de caídas que se presenten y que puedan afectar los acuerdos de niveles de servicio y porcentajes de disponibilidad contratados por la CCB.

Teniendo en cuenta que las soluciones de eventos de seguridad SIEM no hacen monitoreo de disponibilidad, se solicita eliminar este requerimiento.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 211
ANEXO 2
3. 2 Modelo de Operación
o Integrar las herramientas receptoras de Registros de auditoría - Logs que ya posee la CCB, tales como antimalware, firewall y otras relacionadas en el presente documento.
Solicitamos a la entidad indicar como nos seràn entregados estos logs, con que formatos, con que protocólos, etc..

Respuesta
Se definirá con el proveedor seleccionado al inicio del contrato.

Pregunta 212
De acuerdo al numeral 3.2 solución Tecnológica
Se solicita a la entidad aclarar si es de nuestro correcto entendimiento que la CCB suministrara los recursos de CPU, RAM, Storage en la nube de la Entidad necesarios para poder implementar las maquinas necesarias para la prestación del servicio en la nube propiedad de la CCB.

Respuesta
Ver pregunta 71.

Pregunta 213

De acuerdo al numeral 3.2 solución Tecnológica

Se solicita a la entidad aclarar si es de nuestro correcto entendimiento que la CCB suministrara los recursos de CPU, RAM y Storage en el hipervisor de la Entidad necesarios para poder implementar las maquinas necesarias para la prestación del servicio en el data center on-premise propiedad de la CCB.

Respuesta

Ver pregunta 71.

Pregunta 214

De acuerdo al anexo 13 Infraestructura_premisas_aws

Se solicita muy amablemente a la entidad indique la cantidad y el sistema operativo de los dispositivos de punto final que se piensan asegurar con la solución SIEM, ya que el documento adjunto "Anexo 13 Infraestructura_premisas_aws" hace referencia a servidores y a instancias cloud pero no a la cantidad de dispositivos finales.

Respuesta

Ver pregunta 3

Pregunta 215

De acuerdo al numeral 2.1 Premisas

"La CCB actualmente está en el proceso de migración de toda su infraestructura tecnológica a la nube"

Se solicita muy amablemente a la entidad que se indique si los servidores que actualmente tiene on-premise van a presentar algún cambio en sistema operativo o motor de base datos cuando se traslade a la nube, ya que en el documento adjunto "Anexo 13 Infraestructura_premisas_aws" no se puede evidenciar esa información, y esta información se requiere para dimensionar un alcance adecuado del servicio tipo SIEM.

Respuesta

Ver pregunta 3.

Pregunta 216

De acuerdo al numeral 2.1 Premisas

"La CCB actualmente está en el proceso de migración de toda su infraestructura tecnológica a la nube."

Se solicita muy amablemente a la entidad que se indique si los servidores de base datos que actualmente tiene on-premise van a presentar algún cambio en sistema operativo o motor de base de datos cuando se traslade a la nube, ya que en el documento adjunto "Anexo 13 Infraestructura_premisas_aws" no se puede evidenciar esa información, y esta información se requiere para dimensionar un alcance adecuado del servicio tipo DAM.

Respuesta

Ver pregunta 3.

Pregunta 217

"El proponente deberá proporcionar un espacio para el almacenamiento de los registros de auditoría-Logs y asegurar su almacenamiento, disponibilidad y recuperación, así como de la información

generada en la ejecución del servicio contratado. Estos registros deben ser almacenados de manera cifrada por un tiempo mínimo de (6) seis meses y se debe garantizar la disponibilidad para cuando la CCB los requiera. Es importante que el proponente defina un plan de respaldo en caso de borrados accidentales o provocados."

Se solicita muy amablemente a la entidad que nos pueda indicar un aproximado de la cantidad de transacciones que generan las plataformas de la entidad, esto con el fin de realizar el diseño para almacenar la data del servicio de correlacionador.

Respuesta
Se compartirá con el proveedor seleccionado.

Pregunta 218
Los servicios de SOC actuales están incluyendo monitoreo y alertamientos de disponibilidad en tiempo real de los componentes para permitir a las organizaciones supervisar y controlar su ambiente e incidentes de TI de manera más óptima. ¿Este servició deberá ser incluido como valor agregado como parte del alcance?

Respuesta
El proveedor podrá presentar los valores agregados que considere sin que estos generen costos adicionales a la CCB.

Pregunta 219
Amablemente se solicita a la entidad aclarar si para realizar un diseño optimo, La infraestructura en donde será alojada la solución de correlación, detección y monitoreo de eventos de seguridad será en la nube de AWS (con el fin de minimizar la transferencia de logs), ¿esta será provista por la CCB?

Respuesta
Ver pregunta 71.

Pregunta 220
Amablemente se solicita la entidad indicar, los servicios de SOC actuales incluyen el monitoreo de integridad de archivos para detectar cambios de archivos en sistemas operativos, servidores web y aplicaciones web y así tener una mayor visibilidad e información cuando ocurra un incidente de seguridad. ¿Este servició deberá ser incluido como valor agregado como parte del alcance? ¿Para esto, cuantos servidores se deberían considerar?

Respuesta
Ver pregunta 77.

Pregunta 221
Se solicita amablemente a la entidad especificar la cantidad, tipo de dispositivos y los requerimientos de seguridad que la CCB desea monitorear.

Respuesta
Ver pregunta 3.

Pregunta 222
Se solicita muy amablemente a la entidad indicar que sistema operativo tienen las instancias de AWS.

Respuesta
Linux y Windows.

Pregunta 223
Solicitamos amablemente a la entidad eliminar el monitoreo de comandos DCL y DML sobre base de datos, ya que este monitoreo obliga a incluir en el servicio una solución tipo DAM que incrementa considerablemente el valor del servicio para la CCB. Este monitoreo se puede realizar a través de protocolo JDBC para monitorear rendimiento, disponibilidad y seguridad, dentro de los cuales se pueden revisar operaciones en tablas como CREATE/ALTER/DROP/TRUNCATE.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 224
Solicitamos atentamente a la entidad ampliar el número de certificaciones para acreditar experiencia a cinco certificaciones esto con el ánimo de permitir pluralidad de oferentes.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 225
Solicitamos amablemente a la entidad ampliar el número de años para acreditar experiencia a 8 años quedando el requerimiento así:

"El proponente deberá acreditar experiencia mediante la presentación de hasta cuatro (4) certificaciones de contratos ejecutados y/o en ejecución a partir del 1 de enero de 2013, cuya sumatoria debe ser igual o superior a $1.713.600.000"

Esto debido a que años como el 2020 bajó considerablemente la contratación de estos servicios de consultoría y no se estaría garantizando la pluralidad de oferentes, ya que el valor solicitado para acreditar esta experiencia está siendo considerablemente alto.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 226
Solicitamos a la entidad considerar la opción de disminuir el valor para acreditar la experiencia a una suma igual o superior de $1.500.000.000, esto debido a que para contratos de SOC es muy difícil acreditar valores como los que se deben certificar en la presente invitación y no se estaría garantizando la pluralidad de oferentes.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 227
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 se deben entregar después de la presentación de la oferta.

Respuesta
Ver Nota 4 del numeral 3.3.3. de la invitación.

Pregunta 228
3. ESPECIFICACIONES TÉCNICAS
3.1 Alcance del servicio:
El proponente deberá diseñar el modelo adecuado para el monitoreo de los eventos de seguridad de la infraestructura tecnológica (On premises y Nube), aplicaciones y bases de datos, asegurando visibilidad, detección, prevención y el alertamiento

Agradecemos a la entidad confirmar los Datacenters y nubes en los cuales se encuentra alojada la infraestructura que debe ser correlacionada

Respuesta
Nube: AWS
Datacenter: Centro Empresarial salitre.

Pregunta 229
3. ESPECIFICACIONES TÉCNICAS
3.1 Alcance del servicio:
El proponente deberá diseñar el modelo adecuado para el monitoreo de los eventos de seguridad de la infraestructura tecnológica (On premises y Nube), aplicaciones y bases de datos, asegurando visibilidad, detección, prevención y el alertamiento

Agradecemos a la entidad confirmar si puede proveer servidores virtualizados para la implementación de los sensores de correlación en los datacenter y en la nubes donde se encuentra la infraestructura

Respuesta
Ver pregunta 71.

Pregunta 230
3. ESPECIFICACIONES TÉCNICAS
3.1 Alcance del servicio:
• El servicio debe contemplar el monitoreo de la actividad en las bases de datos, mediante una solución tipo DAM u otra(s) que permita gestionar como mínimo los siguientes casos de uso:

Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que la solución SIEM debe poder integrarse con soluciones tipo DAM u otras con que cuente la entidad.

Respuesta
Ver pregunta 173.

Pregunta 231
3. ESPECIFICACIONES TÉCNICAS

3.1 Alcance del servicio:

• El servicio debe contemplar el monitoreo de la actividad en las bases de datos, mediante una solución tipo DAM u otra(s) que permita gestionar como mínimo los siguientes casos de uso:

Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que no debe proveerse una solución DAM u otras para la entidad.

Respuesta
Ver pregunta 173.

Pregunta 232
3. ESPECIFICACIONES TÉCNICAS
3.2 Modelo de Operación
Certificación en el uso las herramientas propuestas por EL proponente, en la versión más reciente con la que se prestará el servicio.

Agradecemos a la entidad reconsiderar esta certificación y permitir que se sustente con curso de formacion en la herramienta SIEM y Experiencia en la gestion de la solución propuesta por el oferente.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 233
3. ESPECIFICACIONES TÉCNICAS
3.2 Modelo de Operación
• El proponente deberá registrar todos los eventos e incidentes de seguridad que se detecten, asignarle un número único de identificación con el fin de realizar un seguimiento de las acciones tomadas sobre las respuestas ante los incidentes reportados y llevar estadísticas e indicadores con base en este registro.

Agradecemos a la entidad confirmar si se usara la herramienta ITSM de la entidad para el registro de incidencias de seguridad detectadas por por la operación del SOC.

Respuesta
Ver pregunta 70.

Pregunta 234
3. ESPECIFICACIONES TÉCNICAS
3.2 Modelo de Operación
Las soluciones tecnológicas de monitoreo para la infraestructura, aplicaciones y bases de datos deberán estar incluidas por Gartner en el cuadrante mágico o peer insight en la versión más reciente.

Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que la solución SIEM propuesta por el oferente debe encontrarse en Garner o peer insight.

Respuesta
De acuerdo.

Pregunta 235

3.2 Modelo de Operación

El proponente deberá proporcionar un espacio para el almacenamiento de los registros de auditoría-Logs y asegurar su almacenamiento, disponibilidad y recuperación, así como de la información generada en la ejecución del servicio contratado. Estos registros deben ser almacenados de manera cifrada por un tiempo mínimo de (6) seis meses y se debe garantizar la disponibilidad para cuando la CCB los requiera. Es importante que el proponente defina un plan de respaldo en caso de borrados accidentales o provocados.

Agradecemos a la entidad confirmar el tiempo de logs disponibles para consulta y el tiempo de retención de logs almacenados.

Respuesta

Ver pregunta 1.

Pregunta 236

3. ESPECIFICACIONES TÉCNICAS

3.3 Canales de Comunicación:

El proponente es responsable del enlace de comunicaciones entre las soluciones tecnológicas propuestas para la prestación del servicio y los recursos de la CCB en la nube de AWS u On Premises para la transferencia de los logs.

Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que se requiere el dimensionar un canal de internet dedicado para poder recepcional los logs provenientes de la infraestructura de la entidad.

Respuesta

No. Ver pregunta 71.

Pregunta 237

3. ESPECIFICACIONES TÉCNICAS

3.6 Acuerdos de Niveles de Servicio:

'• Los cambios y parametrizaciones solicitadas por la CCB deberán ser ejecutadas según los siguientes tiempos:

o Tiempo de atención máximo: 30 minutos

o Tiempo de Solución Máximo: Según complejidad:

▪ Complejidad baja: 60 minutos

▪ Complejidad media: 180 minutos

▪ Complejidad alta: 720 minutos

Al inicio del contrato entre el proveedor y la CCB se definirá los casos
específicos a considerar en cada tipo de complejidad

Agradecemos a la entidad confirmar reconsiderar el manejar un solo tiempo de atención y permitir tiempos de acuerdo a criticidades como por ejemplo:

Alta: 30 Min

Media: 60 Min

Baja: 120 min

Respuesta

Se mantienen los requisitos solicitados.

Pregunta 238
3. ESPECIFICACIONES TÉCNICAS
3.6 Acuerdos de Niveles de Servicio:

'• Los cambios y parametrizaciones solicitadas por la CCB deberán ser ejecutadas según los siguientes tiempos:
o Tiempo de atención máximo: 30 minutos
o Tiempo de Solución Máximo: Según complejidad:
▪ Complejidad baja: 60 minutos
▪ Complejidad media: 180 minutos
▪ Complejidad alta: 720 minutos
Al inicio del contrato entre el proveedor y la CCB se definirá los casos específicos a considerar en cada tipo de complejidad

Agradecemos a la entidad reconsiderar los tiempos de solución dado que la implementación de cambios y/o parametrizaciones en la solución pueden depender de ajustes en las fuentes que se correlacionan. En esta situación proponemos considerar un tiempo de Escalamiento para poder determinar el tiempo requerido por un tercero para terminar de ajustar una solicitud de cambio o parametrización.

Respuesta
Se mantienen los requisitos solicitados.

Pregunta 239
ANEXO 10
CARTA DE COMPROMISO SOLUCIÓN TECNOLÓGICA PROPUESTA

En caso de resultar adjudicatario del presente proceso, me comprometo a garantizar y cumplir los requerimientos técnicos solicitados para cada componente en el numeral X con la siguiente solución tecnológica:

Componente	Aplicación tecnológica Propuesta:
Autenticación de Usuarios	
Endpoint Detection and Response (EDR)	
Firewall como servicio (FWasS)	
Cloud Access Security Broker (CASB)	
Data Loss Prevention (DLP)	
Web Application Firewalls (WAF)	

Agradecemos a la entidad ajustar la información del componente técnico del anexo 10 ya que no corresponde con el objeto del contrato.

Respuesta
Se ajusta la información del anexo 10 La Carta de Compromiso solución Tecnológica propuesta mediante adenda.

Pregunta 240

3.3.3 EQUIPO DE TRABAJO

'Un (1) Coordinador de SOC: Profesional en ingeniería de sistemas o afines según el SNIES que tenga como mínimo 2 años de experiencia en la coordinación de operaciones de contratos cuyo objeto se relacione con la correlación, detección y monitoreo de los eventos de Seguridad, debe contar con certificación en el uso de las herramientas propuestas por el proponente, en la versión más reciente con la que se prestará el servicio.

Agradecemos a la entidad reconsiderar la certificación en el uso de la herramienta propuesta y permitir presentar certificaciones asociadas a seguridad de la información o seguridad informática o Curso de formacion en la solucion SIEM.

Respuesta

Se mantienen los requisitos solicitados.

Pregunta 241

3.2 Modelo de Operación

'La solución tecnológica con la prestará el servicio deberá estar aprovisionada en la nube de AWS.

Agradecemos a la entidad confirmar si toda la solución SIEM debe estar implementada en AWS, si se permite una solucion hibrida para las fuentes on premise un sensor en sede, base de datos logs e inteligencia (alertas, analitica, reportes) en AWS.

La entidad esta en la capacidad de suministrar el hardware o instancias cloud para el despliegue de sensores para la solucion SIEM?

Respuesta

Ver pregunta 71.

Pregunta 242

3.3.3 EQUIPO DE TRABAJO.

'El proponente deberá velar por la permanencia del equipo de trabajo presentado en la propuesta. En caso de que sea estrictamente necesario realizar algún cambio, el proponente deberá entregar para aval de la CCB la hoja de vida del nuevo consultor, el cual deberá tener las mismas o mejores calidades, transferencia de conocimiento y experiencia exigida en la invitación y deberán entregar las certificaciones que así lo acrediten.

Agradecemos a la entidad especificar los tiempos de espera para reemplazo de miembros de equipo de trabajo y la implicación en acuerdos de servicio y/o facturación.

Respuesta

Estos tiempos serán acordados entre el proponente y la entidad al inicio del contrato. Ver cláusula 5 del proyecto del contrato.

Pregunta 243

3.1 Alcance del servicio

'El servicio debe contemplar el monitoreo de la actividad en las bases de datos, mediante una solución tipo DAM u otra(s) que permita gestionar como mínimo

los siguientes casos de uso.

Agradecemos a la entidad aclarar si se debe proporcionar una solucion DAM para el monitoreo de las actividades en base de datos o debe cumplir otras actividades como bloqueo de usuarios comportamientos anomalos etc.

Respuesta

Ver pregunta 173.

Pregunta 244

3.1 Alcance del servicio

'El proponente debe realizar un monitoreo a los análisis de tendencia de amenazas y riesgos disponibles en internet o en centros de respuesta a incidentes que permita informar a la CCB alertas, tendencias, ataques y amenazas provenientes desde el ciberespacio y puedan afectar la infraestructura o los servicios que la CCB presta. Asimismo, el proponente debe disponer de servicios de inteligencia ante Ciber Amenazas.

De forma permanente el SOC realizará una valoración de las amenazas existentes en la región y el mundo, determinando cuál de estos exponen a un riesgo a CCB, resumiendo los resultados en Boletines o informes extraordinarios de SOC.

Agradecemos a la entidad especificar el tipo de entregable esperado y la periodicidad mínima del mismo.

Respuesta

De acuerdo con lo establecido en el numeral 3.5. Reportes y 3.6 Acuedos de niveles de servicio, Tiempo máximo de generación y envio de informes.

Pregunta 245

3.8 Recursos tecnológicos para monitorear

'La infraestructura actual de recursos tecnológicos a monitorear está compuesta
por los activos listados en el anexo 13.

Agradecemos a la entidad indicar si se cuenta con algun servicio nativo de AWS para recolección y almacenamiento de logs para los recursos alojados en ésta nube pública.

Respuesta

Ver pregunta 71.

Pregunta 246

3.1 Alcance del servicio:

Transacciones SAP: monitoreo de transacciones restringidas, transacciones ejecutadas en horario inusual y transacciones prohibidas.

Para realizar la integracion de SAP es necesario la sigueinte informacion para dimensionar el driver:

· Por favor lista únicamente los SID de producción de SAP ver imagen ejemplo.

A	B	C
Producto SAP	Numero de Sistemas de Produccion	Número de Usuários Nombreados en Produccion (Apenas para Sistemas Transacionales)
BW	1	N/A (no transacional)
ECC	1	11.345
GRC Nfe	1	N/A (no transacional)
PI	1	N/A (no transacional)
Portal	1	N/A (no transacional)

Para los sistemas de producción transaccionales (donde ocurre procesos de negocios), necesitamos el número de usuarios en su sistema de producción.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Pregunta 247
1.6 Infraestructura tecnológica
La infraestructura tecnológica de la CCB está compuesta por una red híbrida servidores físicos y virtuales, así como servicios en la nube. Cada línea de negocio de la entidad cuenta con aplicaciones propias para el desarrollo de sus actividades y la prestación de servicios. Las estaciones de trabajo operaran con Sistema operativo Windows. La Vicepresidencia de Tecnología gestiona un Sistema de respaldo de información que incluye cintas, discos y almacenamiento en la nube. La administración de la infraestructura tecnológica de la CCB está a cargo de un tercero.

Agradecemos a la entidad confirmar la direccion exacta del Centro de datos donde se encuentra ubicada la Infraestructura Onpremise que que debe ser integrada con el SIEM.

Respuesta
Centro Empresarial Salitre.

Pregunta 248
1.6 Infraestructura tecnológica
Certificación en el uso las herramientas propuestas por EL proponente, en la versión más reciente con la que se prestará el servicio..

Agradecemos a la entidad confirmar cuales son los tiempos de Migracion que tiene establecidos para el movimiento de su core a la nube, toda vez que esta actividad puede afectar el dimensionamiento de los sensores a implementar y sus capacidades.

Respuesta
Ver pregunta 45.

Pregunta 249
3.3.2. EXPERIENCIA DEL PROPONENTE
...contratos ejecutados y/o en ejecución a partir del 1 de enero de 2018
Se solicita por favor permitir acreditar servicios con ejecución desde el 1 de enero de 2015 independientemente de la fecha de inicio del contrato toda vez que, consideramos, lo pertinente es acreditar servicios prestados en los últimos años sin que necesariamente sean contratos iniciados recientemente.

Respuesta
Se mantienen los requerimientos solicitados.

Pregunta 250
3.3.2. EXPERIENCIA DEL PROPONENTE
...constar la ejecución de las siguientes actividades
Consiserando que los servicios de SOC contienen actividades que podrían ser mencionadas de manera diferente por cada contratante pero que su alcance es el mismo, se solicita por favor permitir presentar certificados de contratos que incluyan servicios de SOC relacionando actividades pero que el nombre de éstas no sea excluyente o inhabilitante.

Respuesta
Se mantienen los requerimientos solicitados.

Pregunta 251
3.3.2. EXPERIENCIA DEL PROPONENTE
...indicar el monto ejecutado del contrato antes de IVA a la fecha de cierre de la invitación.
Teniendo en cuenta que la fecha de cierre del presente proceso es a futuro y que los contratantes no podría acreditar valores ejecutados a futuro; se solicita por favor permitir presentar certificados que acrediten valores contratados toda vez que la información de los mismos podrá ser verificada por la CCB.

Respuesta
Se mantienen los requerimientos solicitados.

Pregunta 252
3.3.2. EXPERIENCIA DEL PROPONENTE
Experiencia Global
Entendemos la importancia y la relevancia del proyecto que se desea contratar en el marco del presente proceso en el cual se busca un prestador de servicios altamente competitivo, con respaldo en el mercado no solo nacional sino internacional y que por tanto se pueden presentar empresas con alcance global. A este entendimiento llegamos dada la posibilidad de acreditar experiencia en moneda diferente a pesos colombianos.

Es importante destacar la figura establecida en el Artículo 260 del Código de comercio modificado por el artículo 26 de la ley 222 de 1995 la cual dispone que: “Una sociedad será subordinada o controlada cuando su poder de decisión se encuentre sometido a la voluntad de otra u otras personas que serán su matriz o controlante, bien sea directamente, caso en el cual aquélla se denominará filial o con el concurso o por intermedio de las subordinadas de la matriz, en cuyo caso se llamará subsidiaria.”

Por lo anterior, es claro que una matriz, sus subordinadas y las sociedades controladas directa o indirectamente por la matriz o subordinada, a pesar de ser personas jurídicas independientes, dependen entre ellas, y se puede afirmar que la experiencia de una de ellas NO es diferente a la de la otra.

En consecuencia, solicitamos de la manera más respetuosa se considere aceptar que el proponente pueda acreditar la experiencia como proveedor de servicios obtenida por la sociedad matriz, por sociedades controladas directa o indirectamente por la matriz y/o por empresas filiales y/o subordinadas, no solo en Colombia sino en otros países, de acuerdo con la condición establecida y en armonía con el artículo descrito.

Respuesta
Se acepta su observación, lo anterior se aclarará mediante adenda.

Pregunta 253
6.3 SEGUNDA FASE DE EVALUACION DE LAS OFERTAS: Calificación
Precio
Para la Segunda Fase de Evaluación de las Ofertas que corresponde a la calificación de las mismas se dispone unos criterios para la asignación de puntajes donde uno de ellos es el menor valor; teniendo en cuenta la facultad de la CCB para llamar a una negociación según lo dispone el numeral 1.14, por favor indicar la forma en que se dará a conocer a los proponentes el resultado de su calificación y la forma en que será posible realizar observaciones a las propuestas competidoras.

Respuesta
Como se indica en el citado numeral, en caso en que la CCB decida realizar la etapa de negociación, informará a los proponentes el procedimiento establecido para tal fin. Por consiguiente, de llegarse a presentar la etapa de negociación se informará por correo electrónico a el proponente con mayor puntaje o a los proponentes que hayan cumplido los requisitos mínimos habilitantes exigidos en la presente invitación, o a los proponentes empatados, para que presenten una contraoferta en relación a la oferta inicialmente presentada. Las propuestas de los demás proponentes no se darán a conocer.

Pregunta 254
6.3 SEGUNDA FASE DE EVALUACION DE LAS OFERTAS: Calificación
El proponente que este inscrito, certifique o cuente con algún sello sobre trabajo en programas y/o aportes a la sostenibilidad (medio ambiente o impacto social enmarcados en los ODS de las Naciones Unidas) de un tercero idóneo como Pacto Global, ICONTEC con su sello de sostenibilidad, Estándares GRI o Sistema B, o podrá obtener el puntaje, el proponente que acredite su condición como Sociedad Comercial de Beneficio e Interés Colectivo, o Sociedades BIC. Calidad que se verificará en el Certificado de Existencia y Representación Legal expedido por la Cámara de Comercio correspondiente, obtendrá 1 punto.
Aporte a la sostenibilidad… De auerdo a las condiciones establecidas, entendemos que para obtener el punto de calificación se podrá presentar el certificado ISO14001 vigente. Por favor indicar si nuestro entendimiento es correcto.

Respuesta
Su entendimiento es correcto.

Pregunta 255
3.3.3. EQUIPO DE TRABAJO
El proponente debe ofrecer un equipo de trabajo conformado como se describe a continuación, para lo cual deberá presentar las hojas de vida y las certificaciones de experiencia y formación del personal que dispondrá para la CCB,
Considerando que los proponentes plantean una oferta manifestando la capacidad de contar con los profesionales para ejecutar el servicio sin la necesidad de tener compromisos precontractuales laborales en etapa de oferta y con miras a posibles adjudicaciones, que la presentación de hojas de vida no debería ser vinculante dado que entre adjudicación e inicio del contrato se pueden presentar cambios en el personal propuesto por decisiones propias de los profesionales y que el proponente puede presentar un esquema de roles y perfiles con el cual se comprometa toda vez que no es posible asegurar recursos específicos asociados a una operación que aún no ha sido adjudicada; agradecemos a la entidad el solicitar la presentación de las hojas de vida previo a la firma del acta de inicio del contrato.

Respuesta
Se mantienen los requerimientos solicitados.

Pregunta 256
5.2. FORMA DE PAGO.
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.

Se solicita respetuosamente a CCB fijar un plazo para emitir el recibo a satisfacción de los mismos.

Respuesta
Esto será acordado con el proponente seleccionado.

Pregunta 257
ANEXO 5
PROYECTO DEL CONTRATO CONTRATO DE XXXXXX
6) OBLIGACIONES DEL CONTRATISTA:
l) Responder ante LA CÁMARA y ante terceros por todas las fallas, errores y omisiones que se presenten en la ejecución del presente contrato y por los perjuicios que con ello se generen.

Se solicita respetuosamente a CCB modificar e incluir a la redacción de este númeral: "por fallas, errores y omisiones imputables exclusivamente al Contratista"

Respuesta
Se acepta su observación, se ajustará la minuta mediante adenda.

Pregunta 258
ANEXO 5
PROYECTO DEL CONTRATO CONTRATO DE XXXXXX
24) CONFIDENCIALIDAD
"...Esta obligación se mantendrá por término indefinido, aún después de terminada la relación que llegue a vincular o no formalmente a las partes…"
Se solicita respetuosamente a CCB limitra el termino de cofidencialidad, proponemos que sea de 5 años, una vez terminada la relación de contractual.

Respuesta
Se acepta su observación, se indica que la cláusula será ajustada vía adenda.

Pregunta 259
ANEXO 5
PROYECTO DEL CONTRATO CONTRATO DE XXXXXX
32) CLÁUSULA DE APREMIO.
En el caso de mora o simple retardo en el cumplimiento de las obligaciones estipuladas en el contrato dentro del plazo, o en la comunicación expresa en la cual se indique el término en el que deban cumplirse cualquiera de las obligaciones establecidas en el presente contrato, o el incumplimiento de la obligaciones pactadas o cumplimiento imperfecto o defectuoso de las mismas, EL CONTRATISTA pagará a LA CÁMARA, a título de penalidad de apremio, por cada día de mora o retardo, el equivalente al 0,1%

del valor total estimado del contrato sin que supere el diez por ciento (10%) del valor del mismo, por cada evento

Se solicita respetuosamente a la CCB eliminar esta clausula en la medida que su aplicación es diaria, y es en relación con cada incumplimiento, lo que puede resultar bastante gravoso para el contratista, y la idea es conminar al cumplimiento y no poner al contratista en una situación de déficit. Igualmente se tiene la penalización anticipada de la cláusula penal, descuentos por incumplimientos de las ANS por lo que podría presentarse la aplicación de una doble sanción por un mismo hecho.

Respuesta
No se acepta su observación, se precisa que no se eliminará la cláusula de apremio. Lo anterior, con el fin de salvaguardar los recursos de la CCB.

Pregunta 260
ANEXO 5
PROYECTO DEL CONTRATO CONTRATO DE XXXXXX
PARÁGRAFO TERCERO: EFECTOS DE LA TERMINACIÓN.
La CAMARA se reserva el derecho de exigir la indemnización de los perjuicios causados por alguna de las causales de terminación indicadas en esta cláusula, salvo si el contrato termina por mutuo acuerdo en el que expresamente se pacte que no se pagará indemnización de perjuicios alguna o por el agotamiento de su objeto.
Se solicita respetuosamente a la CCB limitar la idemnización de perjuicios mediante la siguiente redacción sugerida donde se resalta la expresión a incluir: "La CAMARA se reserva el derecho de exigir la indemnización de los perjuicios causados por alguna de las causales de terminación indicadas en esta cláusula, los cuales no serán mayor al valor del contrato, salvo si el contrato termina por mutuo acuerdo en el que expresamente se pacte que no se pagará indemnización de perjuicios alguna o por el agotamiento de su objeto".

Respuesta
No se acepta su observación.

Pregunta 261
De acuerdo con lo descrito en el documento “INVITACIÓN A PROPONER” de la Convocatoria pública 3000000777 Prestar los servicios de SOC (PDF) – Página 16, el cual menciona lo siguiente:

3.3.2 EXPERIENCIA DEL PROPONENTE.

El proponente deberá acreditar experiencia mediante la presentación de hasta 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 $1.713.600.000 antes de IVA, en las cuales debe constar la ejecución de las siguientes actividades: (i) correlación, detección y el monitoreo de eventos de seguridad de infraestructura tecnológica; (ii) captura, integración, correlación, análisis, alertamiento, escalamiento y reportes de los eventos, alarmas e incidentes de seguridad de la información; y (iii) generación de recomendaciones para la respuesta a eventos de seguridad de la información.

Observaciones:

a) Solicitamos amablemente a la entidad permitir certificaciones de contratos ejecutados y/o en ejecución a partir del 1 de enero de **2017**, toda vez que estos contratos no son muy

comunes en Colombia y se han venido ejecutando desde los últimos 5 años, lo cual permite la pluralidad de participación de oferentes.

Respuesta: Se mantienen los requisitos solicitados.

b) Solicitamos amablemente a la entidad aceptar que el objeto y/o alcance de las certificaciones de contratos ejecutados y/o en ejecución tengan incluido el servicio SOC, debido a que las entidades públicas y/o privadas no desglosan en las certificaciones, contratos y actas, las actividades (i), (ii) y (iii) solicitadas por la entidad. Por consiguiente, las actividades (i), (ii) y (iii) solicitadas por la entidad normalmente se deben ejecutar en un servicio SOC, teniendo en cuenta que no solo cubre las actividades mencionadas por la entidad sino también servicios de administración, monitoreo y soporte, entre otras actividades, lo cual permite la pluralidad de participación de oferentes.

Respuesta: Se mantienen los requisitos solicitados.

Pregunta 262

De acuerdo con lo descrito en el documento "INVITACIÓN A PROPONER" de la Convocatoria pública 3000000777 Prestar los servicios de SOC (PDF) – Página 21, el cual menciona lo siguiente:

CRITERIOS DE EVALUACIÓN		
CRITERIO	DESCRIPCIÓN	PUNTOS*
Certificado de seguridad de la información	Corresponde a la tenencia de un certificado de calidad ISO 27001:2013 Vigente, el cual debe ser presentado junto con la propuesta	5

Observaciones:

a) Solicitamos amablemente a la entidad incluir en la descripción del criterio de evaluación que el alcance de la certificación debe contener al menos "El SGSI para la Operación del Centro de Operaciones de Seguridad (SOC) da soporte a los procesos de relacionados con los servicios de Administración, implementación, Monitoreo, Mantenimiento, Soporte, gestión de vulnerabilidades, incluyendo servicio en la Nube, lo cual no limita la pluralidad de participación de oferentes y si beneficia a la entidad.

Respuesta: Se mantienen los requisitos solicitados.

b) Solicitamos amablemente a la entidad aclarar que el certificado debe ser emitido a nombre del proponente singular y para cada uno de los miembros en consorcio o unión temporal en Colombia.

Respuesta: Se mantienen los requisitos solicitados.

c) Solicitamos amablemente a la entidad aclarar que el certificado debe ser mínimo 27001:2013, toda vez que ya existen nuevas actualizaciones como 27001:2014, entre otras.

Respuesta: Se mantienen los requisitos solicitados.

Pregunta 263

De acuerdo con lo descrito en el documento “INVITACIÓN A PROPONER” de la Convocatoria pública 3000000777 Prestar los servicios de SOC (PDF) – Página 21, el cual menciona lo siguiente:

III. FECHA DE CIERRE DE LA INVITACIÓN: 9 de noviembre de 2021, hasta las 4:00:00 p.m. Las propuestas deben ser remitidas a través de correo electrónico al e-mail Idamis.casas@ccb.org.co, para lo cual se tomará la fecha y hora de recepción del correo.
Observaciones:
Solicitamos amablemente a la entidad ampliar el tiempo del cierre de la invitación hasta el 12 de noviembre del 2021, debido a que los fabricantes requieren de más tiempo para entregar los precios y autorizaciones de las herramientas que se utilizaran para el correcto funcionamiento de la solución a monitorear.

Respuesta
Mediante adenda se amplió el plazo de cierre, para el 16 de noviembre de 2021 a las 2:00:00 p.m.

Pregunta 264
Sugerimos amablemente a la entidad que se aporte junto con la oferta y se asigne puntaje a la certificación ISO 45001 vigente, la cual está relacionado con el objeto del contrato, teniendo en cuanta que el proceso se desarrolla a nivel de servicios con recurso humano y se debe tener en cuenta los requisitos del Sistema de Gestión en Seguridad y Salud Ocupacional efectivo para la ejecución del contrato en beneficio de la entidad.
Respuesta
Se mantienen los requisitos solicitados.

Pregunta 265
Solicitamos amablemente a la entidad aclarar si el servicio SOC objeto de este contrato se ejecutó en años anteriores y cuál es el canon mensual con IVA y su duración en meses / años.

Respuesta
No se cuenta con este servicio.

Pregunta 266
Solicitamos amablemente a la entidad aclarar si el servicio SOC objeto de este contrato se tiene con algún proveedor actual y cuándo vence dicho contrato.

Respuesta
Ver pregunta 265.

Pregunta 267
Solicitamos amablemente a la entidad aclarar si la entidad cuenta con una herramienta de gestión SOC, cuál es el nombre del fabricante, referencia y cantidad de licencias.

Respuesta
Esta información será compartida con el proveedor seleccionado.

Atentamente,

Cámara de Comercio de Bogotá
[Fin del documento]

ANEXO 1 Bases de Datos

VERSION	Edicion	version detallada	Fisico/Virtual	Sitema Operativo	Cores (fisicos o virtuales) Asignados al servidor de BDD	Detalle Procesador	cantidad de bases de dattos
SQLServer 2016	ENTERPRISE	Microsoft SQL Server 2016 (SP2-CU17) (KB5001092) - 13.0.5888.11 (X64) Mar 19 2021 19:41:38 Copyright (c) Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393:) (Hypervisor)	Virtual	Windows server 2016	2 procesadores, 16 core	Intel(R)_Xeon(R)_CPU_E5-2698_v3_@_2.30GHz	6
SQLServer 2016	ENTERPRISE	Microsoft SQL Server 2016 (SP2-CU17) (KB5001092) - 13.0.5888.11 (X64) Mar 19 2021 19:41:38 Copyright (c) Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393:) (Hypervisor)	Virtual	Windows server 2016	2 procesadores, 16 core	Intel(R)_Xeon(R)_CPU_E5-2698_v3_@_2.30GHz	6
SQLServer 2016	ENTERPRISE	Microsoft SQL Server 2016 (SP2-CU17) (KB5001092) - 13.0.5888.11 (X64) Mar 19 2021 19:41:38 Copyright (c) Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393:) (Hypervisor)	Virtual	Windows server 2016	1 procesador 6 core	Intel(R)_Xeon(R)_Gold_6148_CPU_@_2.40GHz	3
SQLServer 2019	ENTERPRISE	Microsoft SQL Server 2019 (RTM-CU5) (KB4552255) - 15.0.4043.16 (X64) Jun 10 2020 18:25:25 Copyright (C) 2019 Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393:) (Hypervisor)	Virtual	Windows server 2016	1 procesador 8 core	Intel(R)_Xeon(R)_CPU_E5-2698_v3_@_2.30GHz	30
SQLServer 2019	ENTERPRISE	Microsoft SQL Server 2019 (RTM-CU5) (KB4552255) - 15.0.4043.16 (X64) Jun 10 2020 18:25:25 Copyright (C) 2019 Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393:) (Hypervisor)	Virtual	Windows server 2016	1 procesador 8 core	Intel(R)_Xeon(R)_CPU_E5-2698_v3_@_2.30GHz	3
SQLServer 2017	ENTERPRISE	Microsoft SQL Server 2017 (RTM-CU25) (KB5003830) - 14.0.3401.7 (X64) Jun 25 2021 14:02:48 Copyright (C) 2017 Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393:) (Hypervisor)	Virtual	Windows server 2016	1 procesador, 6 core	Intel(R)_Xeon(R)_Gold_6148_CPU_@_2.40GHz	11
SQLServer 2017	ENTERPRISE	Microsoft SQL Server 2017 (RTM-CU25) (KB5003830) - 14.0.3401.7 (X64) Jun 25 2021 14:02:48 Copyright (C) 2017 Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393:) (Hypervisor)	Virtual	Windows server 2016	1 procesador, 6 core	Intel(R)_Xeon(R)_Gold_6148_CPU_@_2.40GHz	1
SQLServer 2017	ENTERPRISE	Microsoft SQL Server 2017 (RTM-CU25) (KB5003830) - 14.0.3401.7 (X64) Jun 25 2021 14:02:48 Copyright (C) 2017 Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393:) (Hypervisor)	Virtual	Windows server 2016	1 procesador, 6 core	Intel(R)_Xeon(R)_Gold_6148_CPU_@_2.40GHz	8
SQLServer 2017	ENTERPRISE	Microsoft SQL Server 2017 (RTM-CU25) (KB5003830) - 14.0.3401.7 (X64) Jun 25 2021 14:02:48 Copyright (C) 2017 Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393:) (Hypervisor)	Virtual	Windows server 2016	1 procesador, 6 core	Intel(R)_Xeon(R)_Gold_6148_CPU_@_2.40GHz	2
SQLServer 2016	ENTERPRISE	Microsoft SQL Server 2016 (SP2-CU17) (KB5001092) - 13.0.5888.11 (X64) Mar 19 2021 19:41:38 Copyright (c) Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2012 R2 Standard 6.3 <X64> (Build 9600:) (Hypervisor)	Virtual	Windows server 2012 R2	2 procesadores, 24 core	Intel(R)_Xeon(R)_Gold_6148_CPU_@_2.40GHz	19
SQLServer 2016	ENTERPRISE	Microsoft SQL Server 2016 (SP2-CU17) (KB5001092) - 13.0.5888.11 (X64) Mar 19 2021 19:41:38 Copyright (c) Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2012 R2 Standard 6.3 <X64> (Build 9600:) (Hypervisor)	Virtual	Windows server 2012 R2	2 procesadores, 24 core	Intel(R)_Xeon(R)_Gold_6148_CPU_@_2.40GHz	4
SQLServer 2016	ENTERPRISE	Microsoft SQL Server 2016 (SP2-CU17) (KB5001092) - 13.0.5888.11 (X64) Mar 19 2021 19:41:38 Copyright (c) Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2012 R2 Standard 6.3 <X64> (Build 9600:) (Hypervisor)	Virtual	Windows server 2012 R2	2 procesadores, 24 core	Intel(R)_Xeon(R)_Gold_6148_CPU_@_2.40GHz	3
SQLServer 2016	ENTERPRISE	Microsoft SQL Server 2016 (SP2-CU17) (KB5001092) - 13.0.5888.11 (X64) Mar 19 2021 19:41:38 Copyright (c) Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2012 R2 Standard 6.3 <X64> (Build 9600:) (Hypervisor)	Virtual	Windows server 2012 R2	2 procesadores, 24 core	Intel(R)_Xeon(R)_Gold_6148_CPU_@_2.40GHz	2
SQL SERVER 2017	ENTERPRISE	Microsoft SQL Server 2017 (RTM-CU25) (KB5003830) - 14.0.3401.7 (X64) Jun 25 2021 14:02:48 Copyright (C) 2017 Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2016 Standard 10.0 <X64> (Build 14393:) (Hypervisor)	Virtual	Windows server 2016	2 procesadores, 20 core	Intel(R)_Xeon(R)_CPU_E5-2698_v3_@_2.30GHz	11
SQLServer 2017	ENTERPRISE	Microsoft SQL Server 2017 (RTM-CU25) (KB5003830) - 14.0.3401.7 (X64) Jun 25 2021 14:02:48 Copyright (C) 2017 Microsoft Corporation Enterprise Edition: Core-based Licensing (64-bit) on Windows Server 2019 Standard 10.0 <X64> (Build 17763:) (Hypervisor)	Virtual	Windows server 2019 Standard	2 procesador 8 Core	Intel(R)_Xeon(R)_Gold_6148_CPU_@_2.40GHz	1
DB2 Version 11.1			Virtual	RredHat Linux 7.5	8 quad core	power Pseries 8 ppc64-le	
MySQL			AWS RDS	AWS RDS	db.m5.2XLarge		
AURORA 5.6			AWS RDS	AWS RDS	db.t2-Medium	vCPU	