La Cámara de Comercio de Bogotá adelantará la invitación privada a proponer:

Objeto

"Prestar servicios de seguridad de la información dedicados a proteger la confidencialidad, integridad y disponibilidad de la información de la CCB".

Alcance del objeto: El desarrollo de las actividades contractuales comprende las siguintes actividades:

1. Acompañamiento Temporada de Renovaciones

El servicio debe comprender:

- Monitoreo de los registros de auditoria y alertas de los dispositivos de seguridad disponibles en la arquitectura tecnológica de la CCB (v.gr. firewall, balanceador de cargas, IPS, antivirus, Arcsight, Guardium, etc.)
- Respuesta a incidentes e investigación forense: el proveedor deberá gestionar los incidentes identificados en compañía de la Oficina de Gestión de Riesgos.

Estas actividades serán ejecutadas de forma presencial en las instalaciones de la CCB en el período comprendido entre el 24 de marzo al 7 de abril de 2020 (esto incluye sábados y domingos).
El proveedor deberá indicar en su cronograma de trabajo las actividades de preparación requeridas para la adecuada prestación del servicio. Estas actividades podrán iniciar el 09 de marzo de 2020.
Este servicio será prestado en las instalaciones de la Cámara de Comercio de Bogotá que la Oficina de Gestión de Riesgos indique.

Los entregables a generar como resultado de la prestación de este servicio son:

- Informe con el resultado de las actividades de preparación.
- Informe diario de incidentes atendidos.
- Informe final con hallazgos, incidentes y recomendaciones.

El pago de este servicio se realizará con la entrega a satisfacción de los entregables descritos.

2. Gestión de Vulnerabilidades

El servicio debe comprender el siguiente alcance: dos (2) ejercicios de detección y análisis de las vulnerabilidades presentes en la red de servidores y servicios de la CCB, asociados a la identificación, clasificación de vulnerabilidades por criticidad y propuesta de acciones de remediación. Los entregables mínimos esperados para cada uno de estos elementos son:

a) Herramienta(s) a utilizar, mecanismos de operación (p. ej. Conexión de un equipo o agente a la red de la CCB, horario de ejecución sugerido, forma de monitoreo, etc.) y condiciones de seguridad para evitar indisponibilidad de los servicios.
b) Descripción completa y detallada de la metodología incluyendo la forma en la que se definen los rangos de criticidad de vulnerabilidades, la identificación de falsos positivos y la categorización de vulnerabilidades reales. La valoración de vulnerabilidades debe considerar la clasificación CVE.

c) Para cada prueba un informe detallado de los resultados del análisis de vulnerabilidades, los riesgos a los que queda expuesta la organización, las alternativas de remediación y la hoja de ruta propuesta para su implementación. El informe debe permitir su compresión por parte de los responsables de gestionar la solución de estas.
d) Informe ejecutivo para el Comité de Seguridad de la Información.
e) Si entre el primer y segundo ejercicio se identifican en el mercado vulnerabilidades críticas emergentes que puedan afectar los activos de la CCB, el proveedor deberá realizar un escaneo sobre los mismos y generar un informe con los resultados obtenidos y las actividades de remediación requeridas. Este informe en ningún caso sustituirá el informe de la segunda prueba.
f) El proveedor deberá mensualmente realizar la verificación del cierre de las vulnerabilidades reportadas como remediadas por parte de la CCB y generar un informe de seguimiento con la información de avance y efectividad de las acciones tomadas.
g) El informe de la segunda prueba también debe incluir un análisis de brecha entre la primera y la segunda prueba, haciendo hincapié sobre los hallazgos del primer análisis que no han sido solucionados a la fecha.

El análisis de vulnerabilidades debe ser realizado utilizando conexiones internas y externas, considerando hasta trescientas (300) IPs entre públicas y privadas.

El pago de este servicio se realizará con la entrega a satisfacción de los entregables descritos.

3. Pruebas de Ingeniería Social

El servicio debe comprender el siguiente alcance

a) Jornadas de capacitación: el proveedor deberá realizar un total de 15 actividades de capacitación presencial con una duración de 30 minutos. Los contenidos de estas actividades deben estar asociados a lineamientos prácticos para la protección de la información. La CCB informará al proveedor en cuales de sus sedes se deberán realizar estas charlas y los horarios. La mecánica y contenido de las actividades deberá ser previamente aprobado por la CCB. Las capacitaciones presenciales pueden incluir las sedes regionales (Zipaquirá, Fusagasugá, Chía y Soacha).
   Como resultado de estas actividades se deberá generar un informe que deberá contener la siguiente información:
   - Descripción de la metodología utilizada, público objetivo y contenido de cada actividad,
   - Herramientas de capacitación utilizadas,
   - N° Personas asistentes a la actividad (incluyendo como anexo las listas de asistencia),
   - Registro fotográfico de las actividades.

b) Ejercicios de ataques de ingeniería social controlados: el proveedor deberá coordinar y llevar ataques de ingeniería social controlados considerando como mínimo los siguientes vectores:
   - Física (en sitio): validar los controles de seguridad físicos de la compañía y el apego de los empleados a las políticas de seguridad de la organización. Los lineamientos mínimos que deben ser evaluados son:
     - Pretexting/Impersonate: Captura de información por suplantación del proveedor de soporte técnico o relacionado.

- Revisión de fallas en controles de accesos: el atacante intentará conseguir acceso a la organización y a sus áreas ganándose la confianza de quienes administran los puntos de acceso o con la ayuda de otro colaborador.
- Misdirection: Se deberá generar una distracción en un ambiente laboral para perpetrar acciones que permitan recolectar información de la organización, por ejemplo, toma de fotos, robo de dispositivos de almacenamiento, entre otros.

Este tipo de ejercicio deberá realizarse en 3 sedes de la CCB en Bogotá.

- Phishing: envío de correos electrónicos a colaboradores de la Organización con un enlace a un sitio Web suplantado de la CCB (con dominio similar), con el fin de que entreguen información sensible.
  Este ejercicio deberá tener un alcance de 50 empleados. Los colaboradores que participarán en el ejercicio y el sitio web a suplantar serán definidos por la CCB.

  Como resultado de estos ejercicios se deberá generar un informe que deberá contener la siguiente información de cada uno de los ejercicios realizados:
  - Descripción de la metodología utilizada y público objetivo
  - Herramientas utilizadas,
  - Resultados obtenidos (número de ataques, ataques exitosos, ataques no exitosos),
  - Los riesgos y su criticidad según los resultados obtenidos y
  - Acciones de remediación propuestas.

c) Actividades de Reforzamiento: el proveedor deberá realizar un total de 3 actividades de capacitación presencial de reforzamiento con una duración de 30 minutos. Las sedes y el contenido de las actividades serán acordadas por la CCB y el proveedor considerando los resultados obtenidos en los ejercicios de ingeniería social.

   Como resultado de estas actividades se deberá generar un informe que deberá contener la siguiente información:
   - Descripción de la metodología utilizada, público objetivo y contenido de cada actividad,
   - Herramientas de capacitación utilizadas,
   - N° Personas asistentes a la actividad (incluyendo como anexo las listas de asistencia),
   - Registro fotográfico de las actividades.

El pago de este servicio se realizará con la entrega a satisfacción de los entregables descritos.

4. Pruebas de Seguridad sobre aplicaciones

El servicio debe comprender la ejecución de pruebas de seguridad e intrusión a las aplicaciones definidas por la CCB. Las aplicaciones podrán ser Cliente-servidor, web o móvil. Estas pruebas deberán considerar la aplicación y la IP pública e interna donde esté alojada y deberá considerar como mínimo las siguientes:

- Pruebas de seguridad: Recopilación de información, autenticación y manejo de Sesiones, validación de datos, Cross Site Scripting, inyección SQL, desbordamiento de buffer, denegación de servicio, almacenamiento de datos y la privacidad, criptografía, comunicación

a través de la red, interacción con la plataforma, calidad de código y configuración del compilador.
- Pruebas de intrusión en la aplicación, sistema operativo, Red.
- Las pruebas realizadas deberán quedar documentadas en la herramienta que establece la Vicepresidencia de Tecnología.
- Las pruebas deberán estar basados en la guía Owasp para aplicaciones móviles y web.

El servicio debe comprender una bolsa de 250 horas hombre para la prestación de este alcance. La ejecución de estas pruebas para cada aplicación será solicitada por el Supervisor de contrato con 15 días hábiles de antelación indicando los objetivos de la prueba. El proveedor deberá generar un cronograma detallado para la ejecución de cada solicitud, indicando el número de horas hombre a emplear. Este cronograma deberá ser aprobado por el Supervisor de contrato antes de iniciar las pruebas.

Como resultado de las pruebas realizadas se deberá generar un informe por aplicación analizada que deberá contener la siguiente información: pruebas realizas, herramientas (licenciadas) utilizadas, nivel de criticidad de las vulnerabilidades detectadas y la certificación de las horas hombres empleadas.

El pago de este servicio se realizará con la entrega a satisfacción de los entregables descritos.

5. Gestión de Incidentes

El servicio debe comprender una bolsa de 100 horas hombre para la atención y respuesta a incidentes e investigación forense, incluyendo:

- Diagnóstico e investigación: debe considerar la toma de la evidencia forense requerida y las actividades necesarias para asegurar la cadena de custodia y preservar la evidencia digital conforme a la normatividad colombiana vigente,
- Presentación de recomendaciones de las acciones requeridas para la contención, erradicación y/o recuperación
- Acompañamiento a la CCB durante la ejecución de las actividades definidas para la contención, erradicación y/o recuperación

El proveedor deberá disponer de los recursos y herramientas necesarias para la ejecución del análisis y toma de evidencia forense y la cotización deberá indicar el valor de estos recursos.
La activación del proveedor para la gestión de un incidente será solicitada por el Supervisor de Contrato y la respuesta del proveedor deberá ser inmediata.
Como resultado de la atención del incidente se deberá generar un informe con las actividades ejecutadas, las conclusiones obtenidas, recomendaciones y la certificación de las horas hombres empleadas.
El pago de este servicio se realizará con la entrega a satisfacción de los entregables descritos.

CRITERIOS HABILITANTES:

EXPERIENCIA DEL PROPONENTE

El proponente debe acreditar experiencia en contratos que contemplen al menos uno de los alcances de los servicios objeto de esta invitación, mediante la presentación de:

Mínimo cinco (5) certificaciones de contratos ejecutados a partir de enero de 2017, cuya sumatoria del valor de los contratos debe ser igual o superior a $115.000.000 antes de IVA o su equivalente en dólares. La sumatoria del alcance de los contratos presentados debe cubrir como mínimo los siguientes alcances:

Gestión de vulnerabilidades

Pruebas de ingeniería social

Pruebas de seguridad sobre aplicaciones

Gestión de incidentes

EQUIPO DE TRABAJO

El proponente debe presentar dentro de su propuesta como mínimo un equipo de trabajo para el desarrollo del contrato compuesto por las siguientes personas con el perfil relacionado a continuación:

- **Un (1) Líder de SI**: Formación académica a nivel profesional o especialización o postgrado o maestría o doctorado, en los siguientes programas académicos enmarcados dentro del Núcleo Básicos del Conocimiento del SNIES:
  - Ingeniería Industrial y afines, o
  - Economía, o
  - Administración.
  - Ingeniería de Sistemas, Telemática o afines, o
  - Ingeniería Electrónica, Telecomunicaciones y afines.
- Experiencia certificada en la gerencia y ejecución de proyectos que contemplen los servicios objeto de este RFP de mínimo tres (3) proyectos ejecutados a partir de enero de 2017.

- Nota. El proponente debe asignar un (1) responsable permanente del contrato quien poseerá la visión completa del mismo, y será el responsable de coordinar y supervisar su ejecución, responder por el desempeño del personal a su cargo y mantener la comunicación formal entre el equipo y la CCB.

- Un (1) Consultor Senior en SI:
  - Formación académica a nivel profesional o especialización o postgrado o maestría o doctorado, en los siguientes programas académicos enmarcados dentro del Núcleo Básicos del Conocimiento del SNIES:
    - Ingeniería de Sistemas, Telemática o afines, o
    - Ingeniería Electrónica, Telecomunicaciones y afines.
  - Experiencia certificada en ejecución de proyectos que contemplen los servicios objeto de este RFP de mínimo tres (3) proyectos ejecutados a partir de enero de 2017.
  - Con certificación vigente en ethical hacking y Certificación de uso de la herramienta en la versión más reciente con la que se prestará el servicio. Este rol deberá tener una disponibilidad de 100% para la atención del servicio solicitado en el numeral 1.

- Un (1) Consultor Senior en Gestión de Incidentes: debe contar con:
    - Formación académica a nivel profesional o especialización o postgrado o maestría o doctorado, en los siguientes programas académicos enmarcados dentro del Núcleo Básicos del Conocimiento del SNIES:
        - Ingeniería de Sistemas, Telemática o afines, o
        - Ingeniería Electrónica, Telecomunicaciones y afines.
    - Experiencia certificada en ejecución de proyectos que contemplen los servicios objeto de este RFP de mínimo tres (3) proyectos ejecutados a partir de enero de 2017.
    - Con mínimo una de las siguientes certificaciones: CIHE- Certified Incident Handling Engineer, CDFE - Certified Digital Forensics Examiner, CHFI - Computer Hacking Forensic Investigator Pentest. Este rol deberá tener una disponibilidad para la atención del servicio solicitado en los numerales 1 y 5.
- Un (1) Consultor Junior en SI: debe contar con
    - Formación académica a nivel profesional o especialización o postgrado o maestría o doctorado, en los siguientes programas académicos enmarcados dentro del Núcleo Básicos del Conocimiento del SNIES:
        - Ingeniería de Sistemas, Telemática o afines, o
        - Ingeniería Electrónica, Telecomunicaciones y afines.
    - Experiencia certificada en ejecución de proyectos que contemplen los servicios objeto de este RFP de mínimo un (1) proyecto ejecutado a partir de enero de 2017. Este rol deberá tener una disponibilidad de 100% para la prestación del servicio solicitado en el numeral 1.

INDICADORES FINANCIEROS:

Los proponentes deberán presentar con su oferta los estados financieros con corte fiscal del año inmediatamente anterior, de interés general o particular, que permitan la fácil consulta o determinación de las variables a tener en cuenta. Sólo se considerarán estados financieros certificados con corte al 31 de diciembre de 2018, bajo normas NIIF.

Para las sociedades extranjeras sin sucursal en Colombia o en caso de sociedades extranjeras con sucursal en Colombia que presenten propuesta a nombre de la Casa Matríz, se tendrá en cuenta la última fecha de corte financiero que según su normatividad aplique, la cual debe ser señalada.

La capacidad financiera exigida es la siguiente:

Índice	**Mínimo requerido**	**Calificación**
Capital de trabajo	>= $ 40.000.000	20%
Razón corriente	>= 1,1	20%
Endeudamiento	<=75%	20%

Patrimonio	>= $ 240.000.000	20%
Utilidad Neta	>= 0	20%
Total		100%

Se considerará que cumple con la capacidad financiera requerida para asumir el contrato el proponente que obtenga como mínimo el 80% de los ítems requeridos en el cuadro antes citado.

Nota 1: La CCB podrá verificar la coherencia de la información financiera de los proponentes que se encuentren matriculados o inscritos en el registro mercantil de la CCB.

Nota 2: La CCB verificará que el proponente no se encuentre en liquidación o bajo condiciones financieras o de cualquier otra índole que pudieran implicar un riesgo no admisible para la CCB. Así mismo la oferta que no cumpla con la totalidad de las condiciones financieras exigidas no será considerada.

Los interesados en participar lo pueden hacer manifestado su interés al correo electrónico maria.gutierrez@ccb.org.co, indicando el nombre y NIT de su empresa y allegando vía correo electrónico una certificación de haber prestado servicios relacionados con el objeto de esta invitación.

Una vez haya manifestado el interés de participar, la CCB conformará un listado de proveedores interesados a los cuales se les enviará vía mail las condiciones definitivas de la invitación.

Plazo para manifestar interés: 22 de enero de 2020, hasta las 4:00 p.m.

El interesado que no se encuentre inscrito como proveedor potencial de la Cámara de Comercio de Bogotá lo puede hacer en el siguiente link en donde podrá realizar su inscripción totalmente gratis de manera virtual, fácil y rápida: http://www.ccb.org.co/Proveedores-y-contratistas/Conviertase-en-proveedor-de-la-CCB, hasta el 23 de enero de 2020.

Colaborador de la CCB con quien puede contactarse: NORMA CAMPOS TRUJILLO, teléfono: 5941000 ext. 2809; Correo electrónico: norma.campos@ccb.org.co

Fecha aproximada de apertura de la invitación: 29 de enero de 2020.

La Cámara de Comercio de Bogotá se reserva el derecho de adelantar o no la presente invitación o de modificar y/o cambiar alguna de las condiciones descritas en el presente documento.

La Cámara de Comercio de Bogotá se reserva el derecho de invitar o no a los proveedores que manifiesten interés.

Las condiciones definitivas de la Invitación serán remitidas vía correo electrónico en la fecha en que se de apertura a la invitación.