EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S. A. ESP

RFI / RFQ

ESTUDIO DE MERCADO

OBJETO

Solicitud estudio de mercado para conocer información sobre servicios de análisis forense y hacking ético, identificar infraestructura a que se le puede aplicar estos servicios, así como su alcance.

BOGOTÁ D.C., ABRIL DE 2019

1. INFORMACIÓN PRELIMINAR

Se entiende por estudio de mercado el procedimiento y/o trámite que permite a ETB revisar la estructura, las características y las tendencias del mercado de bienes y/o servicios, así como identificar los segmentos que representan la mejor opción y/o menor riesgo, conocer nuevos productos y/o servicios, y comprender las diferentes condiciones y/o limitaciones relacionadas con el abastecimiento de bienes y/o servicios, incluido el análisis de precios y/o tendencias de los mismos en el mercado y la evaluación de condiciones de capacidad de los posibles interesados.

De conformidad con el Manual de Contratación de ETB, la realización del presente estudio de mercado no obliga a ETB a iniciar una o varias contrataciones, igualmente, ETB podrá a su entera discreción, terminar el presente trámite de estudio de mercado en cualquier momento, sin que por ello se entienda que deba reconocer a los interesados o participantes en el mismo, cualquier indemnización o algún tipo reconocimiento.

El interesado debe tener en cuenta que el presente estudio de mercado puede servir de base para una posterior contratación de los servicios objeto del presente estudio y que en esta fase no se constituye compromiso precontractual ni contractual entre el participante o interesado y ETB. Así las cosas, el estudio de mercado no genera compromiso u obligación para ETB con los participantes, pues no corresponde a un proceso de selección; y en desarrollo del mismo se tendrán en cuenta los principios que orientan la contratación ETB.

ETB podrá solicitar a los participantes del estudio de mercado las aclaraciones o informaciones que estime pertinente, a fin de despejar cualquier punto o aspecto dudoso o equivoco de la información suministrada. Si el participante no envía las aclaraciones o información adicional requerida y no es posible aclarar lo solicitado, la misma no se tendrá en cuenta dentro del estudio.

Con los resultados que se originen con ocasión de este estudio de mercado, eventualmente se podrán desprender uno o varios procesos de selección. Adicionalmente, dichos resultados constituyen una verificación de la información entregada por el participante a fin de establecer posibles invitados para participar en eventuales procesos de contratación con el objeto mencionado en el primer párrafo del presente documento.

2. INTRODUCCION

La EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. E.S.P., en adelante ETB, a través del presente RFI (Request for Information) está interesada en información suficiente, apropiada y confiable acerca del suministro de los servicios de Análisis Forense y Hacking Ético por demanda sobre la infraestructura de TIC, instalada en ETB.

Este RFI está estructurado de la siguiente manera:

- Objeto
- Condiciones para la presentación de la respuesta al estudio
- Capacidad técnica del interesado
- Alcance
- Requerimientos técnicos generales

3. OBJETO DEL ESTUDIO DE MERCADO

La EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. E.S.P., en adelante ETB, está interesada obtener de los interesados información suficiente, apropiada y confiable acerca del suministro de los servicios de Análisis Forense y Hacking Ético por demanda sobre la infraestructura de TIC, instalada en ETB.

4. CONDICIONES PARA LA PRESENTACIÓN DE LA RESPUESTA AL ESTUDIO

A continuación, se detallan las condiciones para la respuesta al presente estudio de mercado:

EVENTO	FECHA
1. Publicación del RFI/RFQ	2 de abril de 2019
2. Última fecha para la recepción de preguntas	Hasta 5 de abril de 2019
3. Respuestas de ETB a preguntas o solicitudes de aclaración	Hasta 9 de abril de 2019
4. Última fecha para la recepción de las propuestas	Hasta 12 de abril de 2019

1. Moneda de cotización: pesos colombianos.

Las propuestas de los interesados deberán presentarse hasta el 12 de abril de 2019 a las 14 horas, en sobre sellado, mediante carta dirigida a la Vicepresidencia Infraestructura junto con 1 copia en el medio de almacenamiento (USB) utilizado para consignar la información digital con las medidas preventivas a efectos de resguardar la información. Las propuestas deben ser entregadas en la Gerencia de Abastecimiento ubicada en la Carrera 7 No 20 - 99 piso 2. Las inquietudes y preguntas pueden formularse a través de la cuenta de correo: daniel.romerol@etb.com.co, el cual es el único canal autorizado (Gerencia de Abastecimiento).

Como respuesta al presente estudio de mercado se deberá entregar la siguiente información:

1. Nombre de su compañía, NIT, fecha de constitución, presencia en Colombia y servicios, certificado de cámara de comercio de la empresa. Por favor diligenciar la siguiente tabla, de acuerdo con la información solicitada:

RAZON SOCIAL	NIT	FECHA CONSTITUCION	REPRESENTANTE LEGAL	SOCIOS	DOMICILIO

2. Respuestas RFI: ETB espera que el interesado entregue la información que se solicita en el RFI, indicando explícitamente CUMPLE o NO CUMPLE al requerimiento planteado o información solicitada por ETB, en cada uno de los puntos y luego proceder a explicar su respuesta. Se espera que todos los documentos que integren el RFI, sean redactados en idioma español.

3. Vigencia de la cotización: Indicar la vigencia de la cotización presentada.

Es importante aclarar que la presentación de la respuesta al presente estudio de mercado no representa compromiso para ninguna de las partes a excepción del compromiso que tiene ETB de mantener estricta confidencialidad sobre la información suministrada.

5. CAPACIDAD TÉCNICA DEL INTERESADO

5.1. REFERENCIAS

El INTERESADO deberá suministrar referencias de implementaciones y soporte de proyectos con el servicio ofrecido y que puedan a criterio de ETB ser visitados. Para ello es necesario informar:

a. Nombre de la operadora o cliente e información de contacto.

b. Perfil de la operadora (sector de la economía, tamaño, segmentos de cliente atendidos por los sistemas / servicios).

c. Solución suministrada y tiempo de uso en el cliente.

d. Tamaño del proyecto (p.e.: Cantidad de IP, aplicaciones WEB).

5.2. CAPACIDAD DE OPERACIÓN EN COLOMBIA

El INTERESADO deberá suministrar información sobre su infraestructura operacional en Colombia para implementación y soporte, incluyendo:

a. Organigrama del departamento de servicios, laboratorio o gerencia de proyecto

b. Dirección de las oficinas en Colombia.

c. Número total de empleados con experiencia técnica en el servicio ofrecido, indicando como certifica la experiencia.

d. Niveles de escalamiento local.

6. ALCANCE

El alcance del presente estudio de mercado (RFI) contempla la recepción de información concerniente a:

a. Desarrollar pruebas de Hacking Ético, a la infraestructura de ETB dispuesta para proveer servicios TIC identificando riesgos y entregando recomendaciones para mitigarlos.
b. Apoyar investigaciones una vez ocurrido un incidente mayor, mediante la implementación de técnicas de análisis digital forense, para soportar investigaciones judiciales o identificar causas raíz y definir los controles a implementar.
c. Ejecutar mediante procedimientos digitales forenses, la recuperación de información borrada de medios de almacenamiento.

7. CONDICIONES ECONOMICAS

7.1. Precios

Se solicita al INTERESADO diligenciar el anexo financiero en formato Excel, adjunto a este documento, indicando todos los precios solicitados.

8. REQUERIMIENTOS TECNICOS GENERALES

8.1. SERVICIO DE ANÁLISIS FORENSE POR DEMANDA

8.1.1. Se solicita al INTERESADO informar, sobre que elementos de los listados a continuación está en capacidad de prestar servicio de análisis forense y/o levantamiento de evidencia:

a) Equipos de cómputo.
b) Servidores Web.
c) Servidores de aplicación y base de datos.
d) Servidores de correo.
e) Enrutadores y switches.
f) Controles de seguridad (firewalls, IPS).
g) Dispositivos embebidos
h) Dispositivos de comunicaciones SIP
i) Cloud
j) Dispositivos móviles como Smartphone, tabletas, wearables entre otros con diferentes sistemas operativo como iOS, Android, Windows Phone, Firefox OS, Blackberry, Ubuntu Touch, Tizen, WebOs, etc.

8.1.2. ETB solicita al INTERESADO informar en que otro tipo de dispositivos se encuentra en la capacidad de realizar procesos de análisis forense y levantamiento de evidencias (diferentes al numeral inmediatamente anterior).

8.1.3. Se solicita al INTERESADO informar, si para el servicio de Análisis Forense, está en la capacidad de ejecutar las siguientes fases:

a) Recolección de Evidencias.
b) Aseguramiento o preservación de evidencias.

c) Análisis de la evidencia.

d) Presentación de resultados.

e) Asesoría y/o acompañamiento para sustentar investigaciones en ámbito judicial en caso de requerirse.

8.1.4. Se solicita al INTERESADO informar, si para el servicio, está en la capacidad de ejecutar análisis forense y levantamiento de evidencias en activos con las siguientes condiciones:

- Encendidos y operando
- Apagados conectados
- Apagados y desconectados
- Desconectados, apagados y con mucho tiempo de no uso (más de un año).
- Dañados o con fallas de hardware:

  En caso de dispositivos de almacenamiento con daños físicos, ETB requiere que se indique la metodología usada para atender este tipo de incidentes, indicando hasta dónde puede llegar el oferente y cuánto tiempo máximo se tomaría para el proceso de evaluación de daños y posibilidades de recuperación (triage).

8.1.5. ETB solicita al INTERESADO informar, si el servicio de levantamiento y análisis de evidencia se puede ejecutar en infraestructura virtual como en infraestructura física. ¿Qué condiciones o requisitos aplican para esquema virtual?

8.1.6. ETB solicita al INTERESADO informar, como el servicio de levantamiento de evidencia digital contempla las siguientes fases y garantiza que la información se mantiene integra en el tiempo:

- Levantamiento de evidencia digital sobre los elementos que ETB requiera de acuerdo al alcance.
- Elaboración de la cadena de custodia sobre la evidencia.
- Preservación de la evidencia.
- Análisis de la evidencia digital.
- Presentación de la evidencia.

8.1.7. Se solicita al INTERESADO informar, el software o licenciamiento empleado para la prestación del servicio de manera que se garantice que ETB no incurrirá en costos de este licenciamiento.

8.1.8. Se solicita al INTERESADO informar los formatos empleados para la entrega de evidencia a ETB y el tipo de herramientas que ETB debe emplear para su visualización, es importante aclarar que ETB no desea adquirir licenciamiento especial para este propósito por lo que se solicita sean abiertas; y no requieran un software propietario para su análisis.

8.1.9. Para la adquisición de la evidencia, el interesado debe contar con los medios necesarios considerando que las interfaces de comunicación presentes en ETB son LAN / WAN, USB 20. Y 3.0, Firewire 400/800, IEEE 1394, UART / Serial, etc.

8.1.10. ETB solicita al INTERESADO informar, en que otro tipo de interfaces de comunicación se encuentra en la capacidad de realizar procesos de levantamiento de evidencias (diferentes al numeral inmediatamente anterior).

8.1.11. Se solicita al INTERESADO informar y explicar, los requisitos para acceder al servicio.

8.1.12. Se solicita al INTERESADO informar los mecanismos técnicos y/o procedimentales con los que debe contar ETB, para que El INTERESADO pueda proveer el servicio adecuadamente y que la evidencia sea válida en un proceso judicial, incluyendo aquellos los elementos fundamentales para el inicio del manejo de cadena de custodia, aislamiento de elementos afectados y las actividades mínimas del primer respondiente que serían aplicables en ETB.

8.1.13. Se solicita al INTERESADO informar con cuales estándares, normas técnicas, metodologías y buenas prácticas del Análisis Forense está alineado el servicio para aspectos como la identificación, recolección y manejo de la evidencia digital y no digital cumpla los requerimientos de autenticidad, precisión y suficiencia entre otros.

8.1.14. Se solicita al INTERESADO relacionar las herramientas con las cuales cuenta para el apoyo del análisis forense (Software y Hardware).

8.1.15. Se solicita al INTERESADO informar, con que normatividad legal actualmente definida cumple el servicio, de manera que se pueda presentar la evidencia ante tribunales, en caso de que ETB llegue a tomar la decisión.

8.1.16. Se solicita al INTERESADO informar, si ETB podrá efectuar validaciones de capacidad (Ej.: Laboratorios y equipos, hardware licenciado, equipos forenses, etc.) en las instalaciones del INTERESADO, en cualquier horario y con total acceso.

8.1.17. ETB solicita que el INTERESADO presente la cantidad de horas y el precio por hora para el suministro de los siguientes servicios, diligenciando en el anexo financiero en la pestaña “HORAS A. FORENSE”, de los siguientes elementos objeto de análisis:

Elementos objeto del análisis
Recuperación de información una vez no haya sido sobre escrita. Disco duro de tamaño 500 G
Recuperación de información una vez no haya sido sobre escrita. Disco duro de tamaño de un (1) Tera.
Recuperación de información una vez no haya sido sobre escrita. Disco duro de tamaño de dos (2) Teras.
Recuperación de información una vez no haya sido sobre escrita. Disco duro de tamaño de cinco (5) Teras.

Búsquedas hasta por 10 criterios en un disco de tamaño de 500 Gigas o Análisis forense de incidente de seguridad (Identificar vector de ataque, actividad maliciosa en el equipo afectado, indicar medidas de recuperación/protección)
Búsquedas hasta por 10 criterios en un disco de tamaño de un (1) Tera o Análisis forense de incidente de seguridad (Identificar vector de ataque, actividad maliciosa en el equipo afectado, indicar medidas de recuperación/protección)
Búsquedas hasta por 10 criterios en un disco de tamaño de dos (2) Teras o Análisis forense de incidente de seguridad (Identificar vector de ataque, actividad maliciosa en el equipo afectado, indicar medidas de recuperación/protección)
Búsquedas hasta por 10 criterios en un disco de tamaño de cinco (5) Teras o Análisis forense de incidente de seguridad (Identificar vector de ataque, actividad maliciosa en el equipo afectado, indicar medidas de recuperación/protección)
Determinar si el disco duro ésta operando correctamente y verificar porque se produce el mal funcionamiento. En caso de mal funcionamiento, investigar con el objetivo de encontrar la razón, o posibles razones por las cuales ocurrió el daño de un disco de tamaño de 500 Gigas.
Determinar si el disco duro ésta operando correctamente y verificar porque se produce el mal funcionamiento. En caso de mal funcionamiento, investigar con el objetivo de encontrar la razón, o posibles razones por las cuales ocurrió el daño de un disco de un (1) Tera.
Determinar si el disco duro ésta operando correctamente y verificar porque se produce el mal funcionamiento. En caso de mal funcionamiento, investigar con el objetivo de encontrar la razón, o posibles razones por las cuales ocurrió el daño de un disco de dos (2) Teras.
Determinar si el disco duro ésta operando correctamente y verificar porque se produce el mal funcionamiento. En caso de mal funcionamiento, investigar con el objetivo de encontrar la razón, o posibles razones por las cuales ocurrió el daño de un disco de cinco (5) Teras.
Determinar si el disco duro ésta operando correctamente y verificar porque se produce el mal funcionamiento. En caso de mal funcionamiento, investigar con el objetivo de encontrar la razón, o posibles razones por las cuales ocurrió el daño de un disco de diez (10) Teras.

8.2. SERVICIO DE HACKING ÉTICO POR DEMANDA

8.2.1. Se solicita al INTERESADO informar, la metodología empleada para solicitar un servicio la cual debe incluir como mínimo el objeto, alcance, recursos, actividades y tiempos de entrega.

8.2.2. Se solicita al INTERESADO informar, cuales son las normas y/o estándares sobre las cuales se basan las actividades de hacking ético.

8.2.3. Se solicita al INTERESADO informar, si está en capacidad de prestar el servicio de Hacking Ético sobre aplicaciones web expuestas a Internet para consulta y consumo masivo, incluir como lo realiza.

8.2.4. Se solicita al INTERESADO informar, si está en capacidad de prestar el servicio de Hacking Ético sobre aplicaciones web desarrolladas in house y/o por terceros.

8.2.5. Se solicita al INTERESADO informar, si está en capacidad de prestar el servicio de Hacking Ético sobre la siguiente infraestructura, adicional informar si hay requisitos o restricciones y especificarlas:

a) Servidores Web.

b) Servidores de e-mail.

c) Servidores de aplicación

d) Equipos de red de telecomunicaciones (Enrutadores y conmutadores/Switches de piso o core, entre otros).

e) Controles de seguridad (firewalls, IPS, proxies).

f) Aplicaciones web y Web Services.

g) Servidores con diferentes sistemas operativos (Linux, Solaris, Windows, etc.)

h) Aplicaciones para prestación de servicios de VOZ IP

i) Servidores de bases de datos

j) Dispositivos Embebidos (CPEs, ONT, STB, Teléfonos IP)

k) Equipos de cómputo o consolas de gestión

l) Dispositivos Embebidos (CPEs, ONT, STB, Teléfonos IP)

m) Aplicaciones Móviles

8.2.6. Se solicita al INTERESADO informar, si el servicio puede ser ejecutado desde cualquiera de los siguientes perímetros o zonas definidas:

a) Red interna de ETB.

b) Internet.

c) Redes de Gestión o de consolas.

d) Accesos VPN de cliente: desde cualquier sistema operativo.

e) Redes o accesos de clientes.

f) DMZ.

g) Acceso inalámbrico (WIFI)

8.2.7. Se solicita al INTERESADO informar, las metodologías empleadas para la prestación del servicio.

8.2.8. Se solicita al INTERESADO suministrar el perfil del personal que ejecuta el servicio incluyendo la experiencia, conocimientos específicos y las certificaciones que acrediten que es idóneo para ejecutar dichas actividades.

8.2.9. Se solicita al INTERESADO informar, si el servicio de Hacking Ético contempla la búsqueda y reporte de (entre otras):

- Acceso a información de recursos de red o servicios de ETB (Direcciones IP, nombres de dominio, infraestructura existente, entre otras).
- Acceso a información de configuración de los dispositivos del alcance.
- Modificación de la configuración de los dispositivos del alcance.
- Acceder a información de clientes o información del tráfico que cursa a través de los dispositivos, ya sea por transmisión en claro o mediante el descifrado de la información.
- Acceder a información de usuarios y contraseñas de acceso a los dispositivos del alcance.
- Realizar una desfiguración (defacement) de la página web de administración o los mensajes de bienvenida (banner) de las interfaces de administración de los dispositivos del alcance.
- Generar condiciones de negación de servicio que permitan:
- Impedir el acceso a la administración de los dispositivos del alcance.
- Impedir el correcto funcionamiento de los dispositivos del alcance, al limitar o bloquear sus funcionalidades de enrutamiento de paquetes bloqueando los servicios de navegación de los clientes.

- Elevación de privilegios que permitan realizar modificaciones o acceso a información que requieran un usuario privilegiado, a través de un usuario de bajos privilegios o sin ningún tipo de privilegios.
- Ejecución remota de comandos o de código en las plataformas analizadas, así como las pruebas necesarias para verificar vulnerabilidades de desbordamiento de buffer.
- Acceder, controlar y/o modificar información de los equipos de los clientes y/o usuarios a través de un ataque exitoso al dispositivo del alcance o mediante la identificación de puertas traseras (Backdoors) habilitados por el fabricante.
- Hacer uso de los servicios provistos por ETB sin estar autorizado para ello, valiéndose de debilidades en los sistemas de Autenticación o Autorización, o por la inexistencia de los mismos.
- Hacer uso de elemento de ETB como parte de un ataque o abuso hacia otro elemento de la red de ETB, de un cliente o un tercero (pivoting).
- Otras afectaciones de la Confidencialidad, Integridad o Disponibilidad de los dispositivos del alcance o de la información de los clientes y/o usuarios.

8.2.10. Se solicita al INTERESADO informar, si el servicio de Hacking Ético contempla los siguientes métodos de explorar vulnerabilidades y/o obtener privilegios elevados de acceso, sin limitación:

- Vulnerabilidades de aplicaciones Web, como inyección de SQL, inyección de código, validación inadecuada de la entrada y errores de lógica de aplicaciones, etc.
- Minería de credenciales de inicio de sesión
- Craqueo de contraseña por fuerza bruta
- Explotación de las vulnerabilidades de desbordamiento de buffer y cadena de formateo
- Secuestro de sesión

8.2.11. Se solicita al INTERESADO informar, si el servicio de Hacking Ético cuenta con la capacidad de realizar: ingeniería social, infección de equipos con malware, uso de credenciales obtenidas a través de otros ataques.

8.2.12. Se solicita al INTERESADO informar que otro tipo de pruebas o esquemas de explotación puede ejecutar, para la identificación de escenarios de riesgo especificados dentro del alcance.

8.2.13. Se solicita al INTERESADO describir los informes que entrega como resultado de la ejecución del servicio de Hacking Ético, Informe Detallado, informe ejecutivo, certificación de nivel de seguridad, otros. Favor detallar el propósito de cada informe y su contenido en términos generales.

8.2.14. Se solicita al INTERESADO informe como garantiza que el servicio de Hacking Ético presenta información objetiva, medible y sin opiniones, criterios personales o interpretaciones subjetivas.

8.2.15. Se solicita al INTERESADO informar, si el servicio de Hacking Ético contiene en la fase de análisis el descarte de falsos positivos. Favor describir la metodología con que lo ejecuta.

8.2.16. Se solicita al INTERESADO informar, si al finalizar el proceso, las vulnerabilidades encontradas se agrupan por criticidad y por dominio tecnológico (Servidores, Dispositivos de comunicación, Aplicación, etc.).

8.2.17. Se solicita al INTERESADO incluir en la valoración todos los bienes y servicios requeridos para cumplir a cabalidad con el servicio.

8.2.18. Se solicita al INTERESADO informar las actividades y fases que se realizan durante el proceso de Hacking Ético, ETB espera como mínimo los siguientes, indique si alguna no se cumple y aquellas adicionales que considere deben incluirse:

a) Reconocimiento: Realizar el reconocimiento de la aplicación o de los segmentos de red
b) Escaneo:
   - Identificar servicios y hosts activos y determinar aquellos con problemas o vulnerabilidades.
   - Determinar qué vulnerabilidades son favorables a ataques y tienen más posibilidad de lograr comprometer los activos definidos en el alcance de las pruebas.
c) Ataques a contraseñas.
d) Explotación: Explorar y explotar vulnerabilidades clave identificadas.
e) Diagramación: Desarrollar los diagramas de red de acuerdo a la exploración realizada.
f) Tomar acceso:
   - Atacar los sistemas específicos y tratar de obtener acceso directo a datos confidenciales y privilegios de acceso de administrador o privilegios elevados en sistemas vulnerables, si es posible.
   - Identificar elementos y servicios de red alcanzables desde el sistema comprometido.
   - Utilizar el acceso para comprometer sistemas y redes internos, si es posible
   - Demostrar debilidades de seguridad, específicas o sistemáticas, si las hay.

- Realizar un reconocimiento de otros dispositivos conectados mediante redes TCP/ UDP al dispositivo contemplando nuevos elementos de análisis para una posible ampliación del alcance.

g) Cubrir rastros: Documentar las acciones que se realizaron o realizarían en pro de cubrir las acciones realizadas en el activo vulnerado o al que se logró acceso.

8.2.19. Se solicita al INTERESADO informar, si el servicio de Hacking Ético contempla los escenarios de pruebas de caja negra, caja blanca y caja gris. A su vez indicar si las pruebas de caja blanca contemplan:

a) Usuario Asignado: Pruebas ejecutadas a sistemas o plataformas con credenciales de acceso para uso de los servicios privilegiados del servicio o tecnología.

b) Sin usuario asignado: Sin credenciales de acceso.

8.2.20. ETB solicita que el INTERESADO presente **la cantidad de horas y el precio por hora para el suministro de los siguientes servicios,** diligenciando en el anexo financiero en la pestaña "HORAS HAC. ETICO ", de los **siguientes elementos objeto de análisis:**

Unidad	Elementos objeto del análisis
1	Sitio Web con 1 a 5 páginas web[1]
1	Grupo de Servidores con sistemas Operativos Linux de 1 a 5
1	Grupo de Servidores con sistemas Operativo Solaris de 1 a 5
1	Grupo de Servidores con sistemas Operativo Windows de 1 a 5
1	Servidor de e-mail (Exchange, Postfix, Qmail, etc)
1	Enrutador de Core o Acceso (Alcatel, Juniper, Cisco, Huawei, etc)
1	Plataformas para servicio voz IP: Asterisk, redes NGN; IMS, servidor de aplicación de voz, SBC Session Border Controller (oracle, broadsoft, Huawei,etc.)

[1] Página Web: Hosting virtual o Hosting dedicado, asociado a un dominio o subdominio, o una página de gestión.

1	Enrutador CPE (Cisco, etc) de 1 a 5
1	Switch core (Alcatel, Cisco, etc) de 1 a 5
1	Redes Inalámbricas compuesta por 1 CPEs (router) y de 1 a 4 Access Point (Aruba, Ruckus, etc)
1	Firewalls Checkpoint, Fortinet, Palo Alto, ETC.
1	IPS (McAfee, HP, Fortinet)
1	Proxy- proxy reverse.
1	Administrador de ancho de Banda
1	Grupo de servidores de bases de datos (Oracle, SqlServer, Mysql, Postgres, etc) de 1 a 5
1	Dispositivo Embebido (CPEs, ONT, STB, Teléfonos IP)

Fin documento