Asunción, 21 de Junio de 2017

INFORME DE EVALUACIÓN TÉCNICA

A: DEPARTAMENTO TRANSMISION Y ACCESO.
DE: DIVISION REDES IP.
REF: EVALUACIÓN TÉCNICA DE LA OFERTA REFERENTE A LA CONTRATACION DIRECTA N°1/2017 PARA LA "ADQUISICION DE ROUTER FIREWALL CON LICENCIA UTM" ID N° 327.735

Tengo el agrado de dirigirme a Usted, con el objeto de remitir el informe sobre la Evaluación Técnica de la Oferta de la firma TECNOLOGÍA EN ELECTRÓNICA E INFORMÁTICA S.A. (TEISA) en referencia a la CONTRATACION DIRECTA N°1/2017 PARA LA "ADQUISICION DE ROUTER FIREWALL CON LICENCIA UTM" ID N° 327.735

El Criterio de Evaluacion es el siguiente según el PBC:

- Se verificará primeramente la presentación de los documentos de carácter sustancial:
  - Formulario de Oferta debidamente completado y firmado.
  - Declaración Jurada de Mantenimiento de Oferta.
  - Declaración Jurada de no hallarse comprendido en las inhabilidades del Art. 40 y la Declaratoria de integridad del Art. 20 (Res. 330/07).
  - Declaración Jurada "Derecho del Menor"
  - Constancia de SIPE
  - Certificado de Cumplimiento Tributario.
  - Patente Municipal
  - Autorización del Fabricante.
  - Copia Simple de Facturas y/o Contratos y/u órdenes de compras/servicios de los últimos tres años.
  - Planilla de Datos Garantizados.

La evaluación de los aspectos técnicos de las ofertas se indica a continuación, teniendo en cuenta el precio de referencia establecido por COPACO S.A. para la presente Contratación que es de Gs. 54.000.000 (Cincuenta y Cuatro Millones de Guaraníes).

A continuación se presenta la Evaluación Técnica de la firma TECNOLOGÍA EN ELECTRÓNICA E INFORMÁTICA S.A. (TEISA):

Lic. Rodrigo Aptola, MBA
Div. Redes IP

Para el listado de bienes y servicios principal cotiza según formato de la planilla "Lista de Precios" de la Carta de Invitación Estándar.

Ítem	Código de Catalogo	Descripción del Bien	Unidad de Medida	Presentación	Cantidad	Marca	Procedencia	Precio unitario (IVA incluido)	Precio Total (IVA incluido)
1	43222501-001	EQUIPO DE ROUTER FIREWALL CON LICENCIA UTM	*Unidad*	*Caja*	1	Fortinet	USA	47.050.291	47.050.291
								Precio Total	**47.050.291**

<u>Son Guaraníes</u>: Cuarenta y Siete Millones Cincuenta Mil Doscientos Noventa y Uno.

El precio total ofertado es de Gs 47.050.291 IVA Incluido.

En la siguiente tabla se presenta el resultado de la evaluación de cumplimiento de los documentos que componen la oferta de la firma TECNOLOGÍA EN ELECTRÓNICA E INFORMÁTICA S.A. (TEISA).

DOCUMENTOS QUE COMPONEN LA OFERTA

Requerimientos del Pliego de Bases y Condiciones.	Cumple	No Cumple
• Formulario de Oferta debidamente completado y firmado.	x	
• Declaración Jurada de Mantenimiento de Oferta.	x	
• Declaración Jurada de no hallarse comprendido en las inhabilidades del Art. 40 y la Declaratoria de integridad del Art. 20 (Res. 330/07).	x	
• Declaración Jurada "Derecho del Menor"	x	
• Constancia de SIPE	x	
• Certificado de Cumplimiento Tributario.	x	
• Patente Municipal	x	
• Autorización del Fabricante.	x	
• Copia Simple de Facturas y/o Contratos y/u órdenes de compras/servicios de los últimos tres años.	x	
• Planilla de Datos Garantizados.	x	

Lic. Rodrigo Antola, MBA
Div. Redes IP

Cumplimento de las características técnicas básicas:

Marca Ofertada: FORTINET

Modelo: FORTIGATE 200D con filtrado y soporte Bundle UTM incluido

ITEM	CARACTERISTICAS		MINIMO EXIGIDO	CUMPLIMIENTO	
				Cumple	No Cumple
1.	RENDIMIENTO Y CAPACIDAD	Performance Firewall Troughput	2950 Mbps	x	
2.		Capacidad Firewall Troughput	4.4 Mpps	x	
3.		Sesiones Concurrentes soportadas	1.900.000	x	
4.		Nuevas sesiones por segundo	76.500	x	
5.		Cantidad de Políticas de Seguridad	9.990	x	
6.		Cantidad de Usuarios Concurrentes.	Ilimitado	x	
7.	CONECTIVIDAD DE RED	Cantidad de puertos 10/100/1000Base-T – Configurables como WAN o LAN	18	x	
8.		Cantidad de bahías SFP para inserción de módulos ópticos.	2	x	
9.		Puertos USB 2.0	2	x	
10.	VPN	VPN IPSEC Troughput	1290 Mbps	x	
11.		VPN SSL Troughput	390 Mbps	x	
12.		Cantidad de Túneles IPSec Site a Site	2.000	x	
13.		Cantidad de Túneles IPSec Cliente a Site	5.000	x	
14.	ROUTING	BGP	EXIGIDO	x	
15.		OSPF	EXIGIDO	x	
16.		RIP v1/v2	EXIGIDO	x	
17.		Soporte a ruteo de multicast	EXIGIDO	x	
18.		Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas	EXIGIDO	x	
19.		Soporte a políticas de ruteo (policy routing)	EXIGIDO	x	
20.		Soporte a ruteo dinámico RIPng, OSPFv3	EXIGIDO	x	
21.		Soporte de ECMP (Equal Cost Multi-Path)	EXIGIDO	x	
22.	AUTENTICACION DE USUARIOS Y CONTROL DE ACCESO	Capacidad de integrarse con Servidores de Autenticación RADIUS	EXIGIDO	x	
23.		Capacidad nativa de integrarse con directorios LDAP	EXIGIDO	x	
24.		Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.	EXIGIDO	x	

Lic. Rodrigo Antola, MBA
Div. Redes IP

25.	TRADUCCION DE DIRECCIONES	NAT	EXIGIDO	x	
26.		PAT	EXIGIDO	x	
27.		NAT estatico	EXIGIDO	x	
28.		NAT con PAT	EXIGIDO	x	
29.	ASIGNACION DE DIRECCIONES IP	Cliente DHCP	EXIGIDO	x	
30.		Servidor DHCP	EXIGIDO	x	
31.		DHCP Relay	EXIGIDO	x	
32.	CONMUTACION EN LAYER 2	Soporte de VLAN 802.1Q	4000	x	
33.		Soporte deLi nk Aggregation Group (802.3ad) con un mínimo de 4 interfaces por grupo	EXIGIDO	x	
34.		Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs	EXIGIDO	x	
35.	ADMINISTRACION DE TRAFICO Y CALIDAD DE SERVICIO (QoS)	Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall	EXIGIDO	x	
36.		Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo	EXIGIDO	x	
37.		Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo	EXIGIDO	x	
38.		Capacidad para definir prioridad de tráfico, en al menos tres niveles de importancia	EXIGIDO	x	
39.		Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión	EXIGIDO	x	
40.		Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.	EXIGIDO	x	
41.	ALTA DISPONIBILIDAD	Soporte de Alta Disponibilidad en modo transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.	EXIGIDO	x	
42.		Soporte de Alta Disponibilidad en modo Activo-Activo	EXIGIDO	x	
43.		Soporte de Alta Disponibilidad en modo Activo-Pasivo	EXIGIDO	x	
44.		Posibilidad de definir al menos dos interfaces para sincronía para Alta Disponibilidad de forma a evitar el uso de Multicast en la red	EXIGIDO	x	
45.	CONTROL DE APLICACIONES	El equipo deberá poseer prestaciones de Control de Aplicaciones. En caso de requerir licencias, las mismas deberán ser provistas y estar activas a la entrega del equipo.	EXIGIDO	x	
46.		Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo	EXIGIDO	x	
47.		La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico	EXIGIDO	x	
48.		Las solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante	EXIGIDO	x	
49.		El listado de aplicaciones debe actualizarse periódicamente	EXIGIDO	x	

Lic. Rodrigo Antola, MBA
Div. Redes IP

50.		Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log	EXIGIDO	x	
51.		Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log	EXIGIDO	x	
52.		Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping	EXIGIDO	x	
53.		Preferentemente deben soportar mayor granularidad en las acciones	EXIGIDO	x	
54.		El equipo deberá poseer prestaciones de Control IDS/IPS. En caso de requerir licencias, las mismas deberán ser provistas y estar activas a la entrega del equipo.	EXIGIDO	x	
55.		Performance Inspeccion IPS (HTTP)	1.6 Gbps	x	
56.		El Detector y preventor de intrusos deberá de estar orientado para la protección de redes	EXIGIDO	x	
57.		El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de linea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.	EXIGIDO	x	
58.		El detector y preventor de intrusos podrá implementarse en linea y fuera de linea en forma simultánea para distintos segmentos.	EXIGIDO	x	
59.		El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad sin necesidad de instalar un servidor o equipo externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos.	EXIGIDO	x	
60.	**INSPECCION DE CONTENIDO – IDS/IPS**	Deberá soportar captar ataques por Anomalía (Anomaly detection).	EXIGIDO	x	
61.		Deberá soportar captar ataques basado en análisis de firmas en el flujo de datos en la red (signature based / misuse detection).	EXIGIDO	x	
62.		Deberá permitir configurar firmas nuevas para cualquier protocolo.	EXIGIDO	x	
63.		Deberá poseer una tecnología de detección tipo Stateful basada en Firmas (signatures).	EXIGIDO	x	
64.		Deberá soportar la actualización automática de firmas para el detector de intrusos (por 3 años)	EXIGIDO	x	
65.		El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios	EXIGIDO	x	
66.		Deberá contar con mecanismos de deteccion de ataques basados en Reconocimiento de patrones y Análisis de protocolos.	EXIGIDO	x	
67.		Deberá contar con mecanismos de deteccion de ataques basados en Detección de anomalías.	EXIGIDO	x	
68.		Deberá contar con mecanismos de deteccion de ataques basados en Detección de ataques de RPC (Remote procedure call)	EXIGIDO	x	
69.		Deberá contar con mecanismos de Protección contra ataques de Windows o NetBios	EXIGIDO	x	
70.		Deberá contar con mecanismos de Protección contra ataques de SMTP, IMAP o POP.	EXIGIDO	x	
71.		Deberá contar con mecanismos de Protección contra ataques DNS.	EXIGIDO	x	

Lic. Rodrigo Antola, MBA
Div. Redes IP

72.		Deberá contar con mecanismos de Protección contra ataques a FTP, SSH y Telnet.	EXIGIDO	x	
73.		Deberá contar con mecanismos de Protección contra ataques de ICMP.	EXIGIDO	x	
74.		Deberá contar con Alarmas mostradas en la consola de administración del equipo.	EXIGIDO	x	
75.		Deberá contar con la capacidad de cuarentena. La misma debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto	EXIGIDO	x	
76.	INSPECCION DE CONTENIDO – FILTRADO DE URL	El equipo deberá poseer prestaciones de Filtrado de Páginas Web (URL Filtering). En caso de requerir licencias, las mismas deberán ser provistas y estar activas a la entrega del equipo.	EXIGIDO	x	
77.		El equipo deberá poseer la capacidad de trabajar como un Proxy Cache	EXIGIDO	x	
78.		Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 39 millones de sitios web en la base de datos.	EXIGIDO	x	
79.		Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad sin necesidad de instalar un servidor o equipo externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.	EXIGIDO	x	
80.		Configurable directamente desde la interfaz de administración del dispositivo. Con capacidad para permitir esta protección por política de control de acceso.	EXIGIDO	x	
81.		Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida	EXIGIDO	x	
82.		Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.	EXIGIDO	x	
83.		Capacidad de filtrado de scripts en páginas web (JAVA/Active X).	EXIGIDO	x	
84.	INSPECCION DE CONTENIDO – ANTISPAM	El equipo deberá poseer prestaciones de AntiSpam. En caso de requerir licencias, las mismas deberán ser provistas y estar activas a la entrega del equipo.	EXIGIDO	x	
85.		La capacidad antispam incluída deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.	EXIGIDO	x	
86.		La capacidad AntiSpam incluída deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address)	EXIGIDO	x	

Lic. Rodrigo Antola, MBA
Div. Redes IP

87.		La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM	EXIGIDO	x	
88.		En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.	EXIGIDO	x	
89.	ADMINISTRACION	Soporte de Interfaz CLI	EXIGIDO	x	
90.		Soporte de Interfaz WEB (HTTP y HTTPS)	EXIGIDO	x	
91.		Puerto serial dedicado para administración.	EXIGIDO	x	
92.		Comunicación cifrada y autenticada con username y password, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet)	EXIGIDO	x	
93.		Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.	EXIGIDO	x	
94.		El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS.	EXIGIDO	x	
95.		El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningun software adicional.	EXIGIDO	x	
96.		Soporte de SNMP versión 2	EXIGIDO	x	
97.		Soporte de servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos	EXIGIDO	x	
98.	ALIMENTACION ELECTRICA Y DIMENSIONES	Tensión de operación	Alterna, 220VCA	x	
99.		El equipo deberá poseer la capacidad de montaje en Rack de 19"	EXIGIDO	x	

Lic. Rodrigo Antola, MBA
Div. Redes IP

Conclusión sobre el cumplimiento de las Especificaciones Técnicas de la oferta presentada por la firma TECNOLOGÍA EN ELECTRÓNICA E INFORMÁTICA S.A. (TEISA) en referencia a la CONTRATACION DIRECTA N°1/2017 PARA LA "ADQUISICION DE ROUTER FIREWALL CON LICENCIA UTM"

La propuesta técnica de la firma TECNOLOGÍA EN ELECTRÓNICA E INFORMÁTICA S.A. (TEISA) CUMPLE con las Especificaciones Técnicas mínimas solicitadas en la Carta de Invitación Estándar Contratación Directa N°1/2017 "ADQUISICION DE EQUIPO ROUTER FIREWALL CON LICENCIA UTM"

Es mi informe,

Lic. Rodrigo Antola, MBA
E.D. Div. Redes IP

Foliado del 01 al 183 incluida esta Foja

Se adjunta:

Nota Presentada por la firma TECNOLOGÍA EN ELECTRÓNICA E INFORMÁTICA S.A. (TEISA) de fecha 29 de mayo de 2017. (Foliado del 1 al 8)

COPACO S.A.

INFORME LEGAL

A	:	PRESIDENTE DE DIRECTORIO
DE	:	GERENCIA OPERATIVA DE CONTRATACIONES
REF.	:	INFORME LEGAL CONTRATACION DIRECTA Nº 1/2017 (ID.Nº 327.735) para la Adquisición de Equipos Router Firewall con Licencia UTM
FECHA	:	24 de Julio de 2017.

A fin de dar cumplimiento a lo Establecido en la Carta Invitación Estándar Datos de la Contratación (DDLC), **Punto 20 Para la evaluación y comparación de las ofertas, la Convocante utilizará los siguientes criterios**:

De conformidad al artículo 34, penúltimo párrafo de la Ley N° 2051/03 "De Contrataciones Públicas", las ofertas se aceptarán siempre que provengan de personas físicas o jurídicas que cuenten con la solvencia técnica, económica y legal suficiente para responder a los compromisos asumidos frente al Estado Paraguayo y que su actividad comercial o industrial se encuentre vinculada con el tipo de bienes, servicios u obras a contratar.

- *No estar comprendido en las prohibiciones o limitaciones para contratar conforme a lo establecido en la Resolución 849/2015 "Por el cual se aprueba un criterio de evaluación para la calificación de la capacidad legal del oferente con respecto a las prohibición prevista en los incisos a y b del Art. 40 de la Ley 2051/03 De Contrataciones Públicas. Este requisito se acredita con la documentación indicada en el* ***Anexo E.***
- *El Comité de Evaluación confirmará que el oferente no se encuentra comprendido en las prohibiciones establecidas en el Art. 40, incisos "a" y "b" de la Ley 2051/03 en base al siguiente análisis:*

En primer lugar, verificara que el oferente haya proporcionado en forma satisfactoria la Declaración Jurada de no hallarse comprendido en las prohibiciones y limitaciones establecidas en el Articulo 40 de la Ley N° 2051/03 que se incluye como Formulario 4 del Anexo D.

RESULTADO:

La Firma Oferente TECNOLOGIA EN ELECTRONICA E INFORMATICA S.A., ha presentado correctamente la Declaración Jurada de no hallarse comprendido en las prohibiciones y limitaciones establecidas en el Articulo 40 de la Ley N° 2051/03 que se incluye como Formulario 4 del Anexo D "Formularios".

Inciso a)

Verificará los registros de personal de la convocante para detectar si el oferente o sus representantes, se hallan comprendidos en el presupuesto del inciso "a" del Artículo 40.

ACCION:
Se ha remitido Memorándum Nº 114 de fecha 6.07.2017, a la Gerencia de Talento Humano de la COPACO S.A., (FS. 194 al 196) a fin de determinar si se registran como empleados de la Compañía los representantes de la firma:

TECNOLOGIA EN ELECTRONICA E INFORMATICA S.A.

- ✓ Elbio Oviedo: Representante Legal, con C.I.Nº 4.710.768.-
- ✓ Galo Efrain Eguez Balsocca: Presidente, con C.I.Nº 1.120.085.-
- ✓ Gustavo Adolfo Eguez Gill: Director Titular, con C.I.Nº 924.606.-

RESULTADO:

Conforme respuesta de la Gerencia de Talento Humano de fecha 7.07.2016 (fs.195): conforme a archivos de la División Registros y Legajos los mismos no se registran como empleados en la Compañía.

Inciso b)

Verificará por los medios disponibles, si el Oferente y los demás sujetos individualizados en las prohibiciones contenidas en la Ley N° 1626/00 "De la Función Pública", aparecen en la base de datos del SINARH o bien de la Secretaria de la Función Pública.

Ma. José Ibarra Caballero
Gerente Operativo de Contrataciones
UOC-COPACO S.A.

207

Si se constata que alguna de las personas mencionadas en el párrafo anterior figura en la base de datos del SINARH, el Comité analizara acabadamente si tal situación le impedirá ejecutar el contrato de que se trate, exponiendo los motivos para aceptar o rechazar la oferta, según sea el caso.

El Comité podrá recurrir a fuentes públicas o privadas de información, para verificar los datos proporcionados por el Oferente.

Si el Comité confirma que el Oferente o sus integrantes, poseen impedimentos la oferta será rechazada y se remitirán los antecedentes a la Dirección Nacional de Contrataciones Públicas (DNCP) para los fines pertinentes....".

ACCION:

Se procedió a la verificación via electrónica en el sitio http//www.documentos.gov.py de la Secretaria General de la Función Pública – Consulta de ser o no Funcionario/a Público/a, a fin de verificar por los medios disponibles si los siguientes aparecen en la base de datos del SINARH o bien en la Secretaría de la Función Pública:

TECNOLOGIA EN ELECTRONICA E INFORMATICA S.A.

- ✓ Elbio Oviedo: Representante Legal, con C.I.Nº 4.710.768.-
- ✓ Galo Efrain Eguez Balsocca: Presidente, con C.I.Nº 1.120.085.-
- ✓ Gustavo Adolfo Eguez Gill: Director Titular, con C.I.Nº 924.606.-

RESULTADO:
Conforme certificados adjuntos Nos. 212993; 212997;212999; (fs. 197 al 205), La Secretaria De la Función Pública certifica que los mismos no registran datos ser funcionario público

ANALISIS Y CONCLUSION:

Por tanto conforme a las verificaciones efectuadas en el sitio web http//www.documentos.gov.py de la Secretaria General de la Función Pública y la Gerencia de Talento Humano de la COMPAÑÍA PARAGUAYA DE COMUNICACIONES S.A., realizadas con relación calificación de la capacidad legal de los oferentes y sus representantes de la Contratación Directa de referencia respecto a las Prohibiciones y Limitaciones establecidas en el Art. 40 Inc "a" y "b" de la Ley Nº 2051/03, (Resolución DNCP N° 849/15) se concluye que, los mismos no se encuentran Inhabilitados,

Además, fin de dar cumplimiento a lo Establecido en la Carta Invitación Estándar Datos de la Contratación (DDLC), **Punto 20 Para la evaluación y comparación de las ofertas, la Convocante utilizará los siguientes criterios**:

(b) ANALISIS DE LOS PRECIOS OFERTADOS

ACCION:
Se procedió a la verificación del precio Ofertado por la firma TECNOLOGIA EN ELECTRONICA E INFORMATICA S.A.

RESULTADO:

Consideramos que no se dieron las condiciones descriptas en las Resoluciones DNCP Nº 956/16 y 1173/16 para solicitar desglose de los precios.

Atentamente,

MARIA JOSE IBARRA OLHAGARAY
Gerente
Gerencia Operativa de Contrataciones