1. BASE LEGAL

REGLAMENTO PARA LAS CONTRATACIONES DE GIRO ESPECÍFICO DEL NEGOCIO DEL BIESS

***"Art. 5. - Definiciones**. - Para efectos de la aplicación del presente reglamento, se tendrán en cuenta las siguientes definiciones: (…) **5.5 Estudio de mercado**: Es el documento que contiene la determinación del presupuesto referencial para la contratación de adquisición de bienes y servicios, incluidos los de consultoría; en base a los parámetros establecidos en este reglamento. (…) **5.6 Fase preparatoria:** Incluye la elaboración y/o modificación del Plan Operativo Anual - POA; informe de necesidad; informes técnicos de ser el caso, estudio de mercado para definir el presupuesto referencial; (…) **5.14 Presupuesto referencial:** Monto de la contratación, determinado por el área requirente previo al inicio del proceso de contratación, en base al estudio de mercado.".*

***Art. 26 Estudio de mercado.** - Deberá contener las siguientes consideraciones mínimas:*
a) Características técnicas de los servicios requeridos;
b) Contar con al menos dos proformas; salvo aquellos procedimientos de contratación que sea proveedor único y/o se demuestre justificadamente la imposibilidad de obtener al menos dos proformas;
c) De ser necesario, el área requirente podrá considerar los montos de contratos similares realizadas por el BIESS en los últimos dos años y traer los montos a valores presentes, es decir, realizar el análisis a precios actuales considerando el índice de inflación; y,
d) Determinar y justificar el presupuesto referencial.

2. CARACTERÍSTICAS TÉCNICAS DE LOS SERVICIOS REQUERIDOS

ÍTEM	SERVICIO	CANTIDAD	UNIDAD	CARACTERISTICA TECNICA
HOUSING CENTRO DE DATOS				LAS CARACTERÍSTICAS TÉCNICAS SON DETALLADAS EN EL SIGUIENTE CUADRO
1	Centro De procesamiento de Datos Principal (Guayaquil) y Componentes (RACK).	4	UNIDAD (SERVICIO RACK)	
2	Centro de procesamiento de datos alterno (Quito)y componentes (RACK)	2	UNIDAD (SERVICIO RACK)	
3	Interconexión LAN CPDP – CPDA (100Mbps)	1	UNIDAD (ENLACE)	
4	Cintoteca CPDP	1043	UNIDAD (SERVICIO)	
5	Servicio de horas de manos remotas	2	UNIDAD (SERVICIO)	
6	Servicio de mailling(Antispam), dominio biess.info.ec	1	UNIDAD (SERVICIO)	
7	Servicio de Seguridad Perimetral (Next Generation Firewall)	1	UNIDAD (SERVICIO)	
8	Servicio de Balanceo de Aplicaciones	1	UNIDAD (SERVICIO)	

9	Servicio de Web Application Firewall (WAF)	1	UNIDAD (SERVICIO)
10	Servicio de DDoS	1	UNIDAD (SERVICIO)
11	Servicio de Storage (STaaS), capacidad 10TB	10TB	SERVICIO ESPACIO DE ALMACENAMIENTO
12	Servicio de Backup (BaaS), capacidad de 50 TB	50TB	SERVICIO ESPACIO DE ALMACENAMIENTO
13	Servicio de Deep & Dark Web (1 dominio)	1	UNIDAD (SERVICIO)
14	Servicio de Brand Protection (1 dominio)	1	UNIDAD (SERVICIO)
15	Servicio de Data Leakage (1 dominio)	1	UNIDAD (SERVICIO)
SERVICIOS BAJO DEMANDA * **			
16	Puntos de red cobre	30	UNIDAD (SERVICIO)
17	Puntos de red fibra a 1GB	5	UNIDAD (SERVICIO)
18	Puntos de red fibra a 10GB	5	UNIDAD (SERVICIO)
19	Cintas (Espacio en cintoteca)	738	UNIDAD (SERVICIO)
20	Servicio de Storage (STaaS), capacidad 59 TB	59TB	SERVICIO (ESPACIO DE ALMACENAMIENTO)
21	Servicio de Backup (BaaS), capacidad de 39 TB	39TB	SERVICIO (ESPACIO DE ALMACENAMIENTO)

A continuación, los detalles de las especificaciones técnicas son:

CARACTERISTICAS TÉCNICAS

1. CENTRO DE PROCESAMIENTO DE DATOS PRINCIPAL (Guayaquil) **2. CENTRO DE PROCESAMIENTO DE DATOS ALTERNO (Quito)**	
Categoría y ubicación de los data centers	TIER III o superior tanto para el Data Center Principal (DCP) en Guayaquil y el Data Center Alterno (DCA) en Quito. El proveedor deberá demostrar documentadamente, ser propietario de la Infraestructura de Data Center, de Guayaquil y Quito.
Estándares Internacionales	Los Data Center deberán cumplir con todos los estándares de la industria de TI basado en la certificación mínimo de TIER III o superior del Uptime Institute.
	El proveedor deberá presentar al menos una certificación en diseño, construcción u operación, por cada uno de los data centers.
Ubicación física	El DCP se ubicará en la ciudad de Guayaquil, y el DCA, en la ciudad de Quito.
Energización	Todo el equipamiento rackeado debe estar energizado correctamente y deberá soportar la carga eléctrica demandada por el equipamiento tecnológico.
	El contratista deberá incluir las PDU, regletas y conectores necesarios para energizar el equipamiento alojado.
	El servicio de housing debe garantizar que los equipos a ser alojados en los DCP y DCA contarán con sistemas redundantes mínimo tipo N+1 para suministro de energía eléctrica, a través de generadores y UPS.
	El reporte mensual del contratista deberá incluir el consumo eléctrico de cada rack en referencia a la capacidad instalada
Sistemas de Enfriamiento	Sistema de enfriamiento redundante mínimo tipo N+1.
	Sistema de climatización mediante pasillos fríos/calientes, con pasillo frío auto contenido.

Sistemas de detección de incendio	Debe disponer de sistema de detección temprana, detección convencional y extinción de incendios.
	El sistema de extinción de incendios debe estar basado en agentes no contaminantes y que no afecten el funcionamiento de los equipos ni a las personas.
Sistemas de control de accesos	Sistemas de seguridad para el acceso con al menos 5 niveles de protección de acceso, desde el control de ingreso del personal hasta la jaula o POD del BIESS (DCP y DCA).
	Seguridad Física a través de sistemas de video vigilancia, control de acceso con tarjeta de proximidad o biométrico, y personal de seguridad.
	El contratista debe garantizar el acceso al personal técnico del BIESS o sus contratistas, en un esquema 7x24x365, para la administración y gestión de equipos alojados en modo housing.
Sistema ATS (Automatic Transfer Switch)	Proveer mínimo de 2 ATS (1 en el Data center de Guayaquil y 1 en el Data Center de Quito) de energía eléctrica de 110V con 6 tomas mínimo, que se instalarán en los racks dentro del Espacio contratado que el BIESS indique, los cuales se utilizarán para conectar equipos que cuenten con una sola fuente de poder, indicados previamente por el BIESS
Disponibilidad	La disponibilidad que deben brindar los Data Centers es de mínimo 99,982% en modalidad 7x24x365 para servicio de Housing.
Servicio de Infraestructura de Red	El contratista debe contar en el DCP y DCA, con equipos de red que proporcionen al BIESS los servicios de conectividad. La red de data center del proveedor debe estar diseñada e implementada en un marco de redes de última generación, conforme a las tendencias de la industria.
	A fin de gestionar los servicios publicados del BIESS, se requiere un pool de al menos 96 direcciones IP públicas.
	El contratista deberá implementar la topología que demande el BIESS mediante esquemas redundantes, y que garanticen altas velocidades, estabilidad, escalabilidad, disponibilidad, seguridad, segmentación del networking interno, conectividad entre racks y la interconexión a los enlaces de datos e internet para los equipos a ser alojados.
	Los servicios de conectividad serán administrados por el contratista bajo las necesidades y lineamientos del BIESS.
	El contratista deberá proveer de todo el equipamiento de networking y demás elementos requeridos para garantizar la conectividad de toda la infraestructura del BIESS en el data center, entre data centers y sus oficinas remotas por medio de los contratistas de enlaces de datos.
	La red debe asegurar una topología libre de loops, sin la utilización de protocolos que introducen inestabilidad y complejidad, entregando, conexiones seguras, estables y consistentes, además debe soportar la conectividad a dependencias que demande el BIESS.
	Se debe asegurar una arquitectura global del centro de datos que soporte avanzados mecanismos de calidad de servicio (QoS) para priorizar tráfico, para el transporte de diferentes aplicaciones como real time, sistemas de misión crítica, storage traffic tanto en el Fabric como en la interconexión con la WAN y LAN.
	La configuración de switches CORE del contratista serán independientes de otros clientes, para ello se configurará un tenant exclusivo para el BIESS o el que aplique según la tecnología.
	El contratista deberá proveer de puntos de red para la conexión de todo el equipamiento conforme la tecnología ethernet y velocidades que requieran para su normal operación.
	El contratista deberá mantener el direccionamiento y segmentación IP que tiene el BIESS en la actualidad.
	Se debe brindar servicio de interconexión para permitir la conectividad hacia la infraestructura alojada en el Centro de Datos del contratista, con otro contratista de servicios externo tipo carrier, por lo que se deberá proveer de al menos de dos mangas para el acceso de la fibra de otros proveedores en cada data center.

Jaula o PODs para Racks	Los racks requeridos para los DCP y DCA, deben estar dentro de jaulas o PODs para alojamiento de equipamiento y de racks exclusivos para el BIESS, por lo cual, el acceso a las mismas debe ser asegurado con un sistema de tarjeta de proximidad o biométricos.
Rackeo de equipos	El rackeo de equipos y el cableado debe cumplir con estándares de la industria para etiquetado, distribución, instalación de cableado, así como rackeo de equipos.
	El contratista debe proveer como parte del servicio de Housing, los Blanking Panels para cubrir todos los espacios libres donde no se alojen equipos, en todos los racks requeridos en el servicio de Housing y en función de la distribución de equipos establecida por el BIESS, con el fin de evitar el retorno de aire caliente.
	El contratista debe proveer como parte del servicio de Housing, de organizadores de acuerdo con la necesidad de la organización (peinado) de los cables de cobre y fibra para los racks asignados.
Espacio de Racks	Todas las unidades de rack deben ser utilizables.
	El contratista deberá proporcionar espacio en jaula mínimo de 4 (cuatro) Racks de 42 U tipo gabinete para servidores en el DCP y un espacio de jaula mínimo de 2 (dos) racks de 42 U en el DCA, exclusivos para el BIESS, que incluya mecanismos de seguridad física y lógica.
	El DCP debe contar con un espacio vació adicional dentro de la jaula o pod equivalente a un rack de 42 unidades para ubicar un sistema de librería TS3500 del BIESS
	El DCA debe contar con un espacio vació adicional dentro de la jaula o POD, de dimensiones aproximadas a un rack de 42 unidades para ubicar un armario para almacenamiento de cintas del BIESS.
	El contratista deberá realizar la organización de nuevos equipos basada en las mejores prácticas y distribución uniforme de energía.
	En base a la necesidad el BIESS podrá aumentar o disminuir espacios físicos de rack en las jaulas, para lo cual el proveedor deberá realizar el respectivo peinado y organización en el rack intervenido
	Los racks deberán contar con los patch panels necesarios para interconexión de acuerdo a la topología y ubicación de los equipos del BIESS.
3. INTERCONEXIÓN LAN CPDP – CPDA (100MBPS)	
	Se requiere la provisión y gestión de un canal o enlace de conectividad LAN to LAN para la conexión de los 2 Data center (Tipo L2), y mantener los mismos direccionamientos IP con la propagación de todas las VLANs definidas por el BIESS en ambos data centers. Con un ancho de banda de al menos 100Mbps.
4. CINTOTECA CPDP	
	Espacio en Cintoteca para mínimo 1043 cintas en el Data Center de la ciudad de Guayaquil
	Las cintas deberán estar vigiladas por una cámara de seguridad, con una retención videos por el lapso de al menos 3 meses.
	Los videos deberán ser entregados en medio digital cada mes, como parte del servicio
	El contratista será responsable de realizar los ingresos y retiros de cintas desde las librerías hacia la cintoteca o viceversa de acuerdo a las solicitudes del BIESS. De igual manera, de la recepción de nuevas cintas.
	Estas interacciones no serán cargadas al servicio de manos remotas y serán parte del servicio.
	El Biess Cancelará por la cantidad de cintas alojadas en la cintoteca
5. SERVICIO DE HORAS DE MANOS REMOTAS	
Soporte Técnico	El Centro de Datos Físico deberá brindar soporte técnico especializado en un esquema de 24x7x365 en los componentes y servicios del Centro de Datos de acuerdo con el SLA establecido.
	El contratista asignará al menos un técnico VIP por cada Centro de Datos, mismo que se encargará de la gestión y atención rápida de los requerimientos técnicos solicitados por el BIESS.

	El contratista deberá disponer de canales de soporte para solicitar servicio de asistencia y jerarquización de problemas y fallos.
Servicio de manos remotas	El oferente debe proporcionar bajo demanda el servicio de manos remotas en un esquema 24x7x365, que incluirá realizar tareas simples, que incluyan: • Reseteo del equipo o reseteo de tarjetas, • Descripción y reporte de indicadores (display) de los equipos o consolas, • Conexiones sencillas. • Rackeo y/o desrackeo de equipos. • Observación básica del entorno. • Gestión básica de cables de red y eléctricos. Para ello el BIESS entregará las actividades que deberá ejecutar el contratista por cada evento requerido.
	Cada interacción será definida por intervalos de duración de 15 minutos.
	Se requiere un pool de horas de 24 horas por año de servicio.
	El pago se realizará por horas completadas de 60 minutos.
	En el caso de los servicios gestionados, serán administrados por el contratista y remitirá al BIESS reportes de incidentes, funcionamiento, estadísticas de uso, informes, boletines de seguridad de manera periódica según lo requiera el BIESS.
	La administración de estos servicios implica según corresponda el manejo total de la tecnología incluida la gestión de requerimientos, el contratista deberá atender en cumplimiento del SLA todas las solicitudes realizadas por el BIESS.
	El contratista entregará a la firma de contrato el procedimiento para apertura de tickets y los niveles de escalamiento conforme lo solicitado en las especificaciones técnicas.
6. SERVICIO DE MAILLING (Antispam), dominio biess.info.ec	
	Se requiere proteger el servicio de correo electrónico de notificaciones del BIESS, con un Sistema Antispam que debe funcionar detectando y alertando a la entidad de manera proactiva un incidente ante la presencia de correos Spam que afecten al servicio de mail. El equipo deberá operar en cualquiera de las siguientes modalidades: • Modo Gateway • Modo Transparente • Modo Servidor Disponer de certificación “VBSpam” de Virus Bulletin que mide el porcentaje de captura de spam vs el porcentaje de falsos positivos, el cual verifica si la solución anti-spam es capaz de: • Bloquear un gran porcentaje de correos electrónicos en un tráfico real de spam. • Una correcta identificación de todo spam, en un tráfico real donde existen correos electrónicos legítimos. Escuchar Leer fonéticamente Diccionario – Debe ser capaz de proteger correo electrónico entrante (desde Internet) y correo saliente (hacia Internet) en el protocolo SMTP. • Permitir la conexión en tiempo real a una base de datos centralizada en el fabricante para descargar actualizaciones de Antispam de forma continua.Protección contra ataques de denegación de servicio (DoS) y ataques de directorio. • Verificaciones de DNS reverso para proveer protección tipo anti-spoofing (anti-engaño) de fuentes válidas de correo. • Debe proveer mecanismos de identificación basados en un servicio de reputación global provistos por el Fabricante, capaz de rechazar conexiones SMTP desde fuentes no confiables y evitar así gran cantidad de tráfico basura, es decir, tener la capacidad de limitar conexiones SMTP a servidores no confiables o de mala reputación. • Lista de la reputación del remitente local con base en: o Número de correos con virus o Cantidad de correo no deseado

	o Número de destinatarios inválidos o no existentes. • Posibilidad de definir listas blancas/negras por dominio o cuentas específicas, IP´s públicas, listas de terceros, capacidad de prevenir ataques de virus y ataques de directorio. • Capacidad de aseguramiento para el envío masivo de correo de tipo notificaciones de al menos una transaccionalidad de 280.000 mails diarios.
7. SERVICIO DE SEGURIDAD PERIMETRAL (Next Generation Firewall)	
	Se requiere contar con el servicio de seguridad perimetral (Firewalls), que permita el aseguramiento de la red para la infraestructura del BIESS. Características Generales El servicio deberá contar con al menos las siguientes capacidades y/o funcionalidades: Firewall (QoS, NAT/PAT) Filtrado Web IPS/IDS, Antivirus /AntiMalware /Antibot IPsec VPN VPN SSL Protección DNS Soporte del fabricante. El servicio deberá ser provisto con equipamiento de marca que conste en el cuadrante de Gartner como líder durante al menos los últimos tres años previos a la fecha de publicación del presente proceso. Los equipos firewall deben contener la última versión de software estable lanzado por el fabricante. Debe permitir derivar los registros (logs) hacia la solución de reportería y correlación de eventos de la misma marca del firewall.
	Módulo IPS Inspección profunda de paquetes, incluido el tráfico encriptado con el último TLS. Actualizaciones de firmas diarias de protección, automáticas provistas por el fabricante. Capacidad de contar con varios perfiles de protección personalizados, para protección de servicios específicos de la red.
	Filtrado Web
	Control de aplicaciones WEB.
	Integración con directorio activo para controles por usuarios, grupos, y/o equipos.
	Actualizaciones continuas de bases de datos por el fabricante u otras fuentes
	Categorización manual o personalizable de sitios web y/o aplicaciones.
	Controlar el acceso al contenido web bloqueando páginas web que contengan palabras o patrones específicos, mediante el uso de comodines, expresiones regulares, etc.
	Optimiza el uso del ancho de banda en la red al priorizar, despriorizar o bloquear el tráfico según la aplicación.
	Inspección de tráfico HTTPS
	Antivirus/AntiMalware/AntiBot
	Antivirus perimetral para protección de amenazas y ataques informáticos.
	Protección contra los últimos virus, sypware y otras amenazas conocidas a nivel de contenido.
	Motores de detección avanzados para detener malware conocido y polimórfico.
	Prevenir ataques exitosos a través de múltiples vectores de amenaza.
	Actualizaciones de bases de datos diarias del fabricante.
	Realiza la detección posterior a la infección de bots en hosts.
	Previene los daños de los bots al bloquear las comunicaciones de C&C (Comando y control) de los bots.
	Se actualiza continuamente desde una red colaborativa para combatir el cibercrimen.
	IPsec VPN y VPN SSL
	Capacidad para creación de VPN tipo IPSEC
	Se requiere de al menos 800 usuarios concurrentes VPN SSL BIESS, sin costo adicional para la institución.
	Red
	Los equipos del servicio de manera individual deben contar con al menos el siguiente Performance:
	- IPS Throughput: 13 Gbps

	- GW: 80 Gbps
	La solución debe soportar un throughput de prevención de amenazas de mínimo 7 Gbps medido con todas las características activadas.
	El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
	El contratista deberá dimensionar las interfaces físicas que se requiera y con base en las mejores prácticas del fabricante y velocidades de operación a nivel de red.
	Consola de administración
	Consola de administración de los equipos, misma que puede estar embebida en los firewalls o en un equipo diferente, appliance físico o virtual. En este caso, la consola de administración debe contar con el licenciamiento para uso, actualizaciones y soporte de fabricante durante el tiempo que dure el servicio.
	Log y Correlacionador
	La solución debe permitir almacenar por al menos 6 meses los logs generados por el firewall, correlacionar eventos y generar reportes automáticos (al menos 3) y bajo demanda.
	Los registros logs deben ser trasladados a un repositorio externo una vez que el disco del equipo de logs requiera liberar su espacio y serán almacenados por todo el tiempo que dure el contrato, y serán entregados al BIESS
	Los logs generados por el firewall son de propiedad exclusiva del BIESS y no podrán ser copiados, modificados o eliminados por el contratista para otros fines.
	Licenciamiento
	El servicio de seguridad perimetral (firewalls) deberá contar con licenciamiento de todas las características señaladas en las especificaciones y su vigencia será la misma del tiempo del contrato.
	En caso de solicitarse más características que soporten los firewalls, el contratista será encargado de agregar licenciamiento y adecuación del servicio, según lo indicado en las especificaciones generales y la metodología de trabajo.
	Otras Consideraciones
	El servicio de seguridad perimetral (firewall) deberá brindar la protección de la red LAN, WAN y DMZ del BIESS
	El contratista se encargará de realizar al menos 2 mantenimientos anuales de software sobre el servicio de seguridad perimetral (firewall). Por lo que el contratista instalará los parches de seguridad recomendados por el fabricante y en el caso de actualizaciones o upgrades de sistema operativo, se realizará siempre y cuando sea recomendado por el fabricante. Todas las operaciones de updates y upgrades serán aprobados por el BIESS.
	De ser requerido, el personal autorizado por el BIESS podrá solicitar al contratista (sin costo alguno extra), que realice configuraciones en los equipos que conforman el cluster, referente a reglas de: Firewall, NATs/PATs, control de navegación, VPN SSL, VPN IPSec, AntiBot, activación/configuración de funcionalidades propias que se encuentren licenciadas en el servicio.
	El contratista deberá realizar respaldos periódicos diarios de las configuraciones y políticas del firewall. Los respaldos deberán ser almacenados en un repositorio propio del contratista y también se entregará una copia al BIESS para su almacenamiento.
	La herramienta será administrada en conjunto por el contratista y el personal del BIESS, sin embargo, el contratista no podrá realizar ningún cambio de configuraciones, políticas, afinamientos, sin consentimiento del área responsable del BIESS.
	El contratista llevará una bitácora de cambios realizados sobre las políticas y/o configuraciones y será presentada de manera mensual al BIESS.
	Las políticas de firewall serán de uso exclusivo para el BIESS y no podrá contar con reglas, configuraciones u objetos para uso de terceros.

	Las reglas de firewall serán creadas siguiendo las buenas prácticas, con nombres de reglas estandarizadas, comentarios y demás parámetros que sean necesarios para este fin.
	El contratista deberá garantizar el buen funcionamiento de la solución, sin que se generen congestión de tráfico, sobre procesamiento de recursos u otros problemas que puedan generar un bajo perfomance de la solución.
	Servicio de Administración bajo los tiempos establecidos en el documento SLA
	De ser el caso el BIESS, podrá solicitar al contratista la reestructuración de las reglas configuradas en los diferentes módulos/blades que posee el firewall.
	De ser el caso el BIESS, podrá solicitar al contratista que realice una rearquitectura que involucre la conectividad de las diferentes vlans que convergen a los equipos que conforman el cluster y que se encuentran dentro de la LAN, WAN y DMZ del BIESS
	El contratista entregará al menos 5 usuarios nombrados con el rol de auditor con permisos de lectura únicamente para monitoreo de la solución, así como los accesos a los Dashboard generados para este servicio (modo visualización).
	El contratista entregará al BIESS la reportería de forma mensual y bajo demanda del servicio.
Contingencia.	Los servicios especializados pueden ser provistos en el sitio principal o en el sitio alterno, de acuerdo a la necesidad del BIESS.
Actualizaciones	Los servicios especializados provistos por el proveedor, deben pasar por el mantenimiento, actualizaciones o gestión de cambios, con base en las mejores prácticas, con el fin de garantizar la continuidad de los servicios.
8. SERVICIO DE BALANCEO DE APLICACIONES	
	CARACTERÍSTICAS FÍSICAS Y DE RENDIMIENTO
	Se requiere contar con el servicio de balanceo de aplicaciones
	Disponibilidad: El servicio deberá tener la posibilidad de detectar y compensar la sobrecarga de solicitudes a los servidores para no evidenciar lentitud y/o indisponibilidad de servicio.
	Throughput: La solución debe soportar al menos un Throughput Nominal de 1 Gbps para balanceo en condiciones de máxima carga.
	Crecimiento Throughput: Los equipos ofertados deben tener la Capacidad de crecimiento a por lo menos 2 Gbps por licenciamiento sin necesidad de cambiar/modificar el equipo.
	Peticiones HTTP x segundo: La solución debe soportar al menos 200.000 HTTP request por segundo.
	Crecimiento Peticiones HTTP x segundo: La solución debe tener la capacidad de crecimiento sin necesidad de cambiar el modelo/sistema, para soportar mínimo 300,000 HTTP request por segundo.
	FUNCIONES DE ADMINISTRACIÓN DE TRÁFICO
	Balanceo de Tráfico: La solución ofertada deberá realizar funciones de Balanceo de Tráfico de aplicaciones basadas en IP (TCP, UDP) y Servicios Web.
	Algoritmos balanceo: La solución debe permitir hacer control de balanceo de tráfico local con varios tipos de algoritmos especializados definidos en la solución de balanceo:
	• Round Robin
	• Respuesta rápida
	• Conexiones mínimas
	• Análisis de carga
	• Hash de URL
	Monitoreo Servidores: La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de:
	• Ping.
	• Chequeo a nivel de TCP y UDP a puertos específicos
	• Monitoreo HTTP y HTTPS

• Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos.
• Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red.
• Monitoreo en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma.
Monitoreo Aplicaciones: La solución deberá soportar mínimo el Monitoreo de aplicaciones/protocolos del mercado: LDAP, FTP, DNS, SMTP, POP3, RADIUS, SIP, SNMP.
Persistencia conexiones: Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones. El control de persistencia de las conexiones se debe realizar por los siguientes métodos: • Dirección IP origen • Dirección IP destino • Cookies • SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia • Sesiones SSL
FUNCIONES DE ACELERACIÓN DE TRÁFICO
Compresión: La solución debe ofrecer Características de Compresión de tráfico a nivel de aplicaciones:
• El sistema deberá permitir compactar el tráfico http a través del estándar GZIP, Deflate y compatible con browsers MS Internet Explorer, Google Chrome, Mozilla Firefox, Safari, etc.
• Debe incluir compresión de tráfico con capacidad de crecimiento
FUNCIONES DE SEGURIDAD
Seguridad SSL: La solución debe incluir el soporte de Aceleración SSL:
La solución debe soportar al menos 3.000 transacciones por segundo
Compatibilidad para conexiones SSL con llaves de 2048 y 4096 bits con capacidad de crecimiento por licenciamiento hasta de 5.000 sin necesidad de cambiar el equipo
Encripción: La solución ofertada debe manejar mínimo AES256; SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman
ADMINISTRACIÓN DEL SISTEMA
CLI, WEB: La solución debe permitir el acceso para la administración de la solución vía CLI (Interfaz de línea de comandos) por SSH2, interfaz de administración gráfica basada en Web seguro (HTTPS)
REPORTES Y VISIBILIDAD
Reportes: La solución debe permitir dar visibilidad del balanceo del tráfico web, para identificar las aplicaciones más utilizadas, las URLs accedidas, los usuarios con más accesos y los servidores más requeridos.
Se debe entregar al menos 5 usuarios para monitoreo y lectura al BIESS.
Visibilidad:
• La herramienta que forme parte de la solución debe proporcionar la información de manera gráfica, de tal forma que permita identificar de manera más rápida y oportuna, alguna falla/anomalía en la entrega del servicio al usuario final.
• La solución ofertada debe disponer de una consola de administración centralizada en donde se puedan ver y administrar los equipos que se encuentren en el ambiente de la entidad.
Soportar las últimas versiones de TLS y SSL
SOPORTE PARA BALANCEADO DE APLICACIONES LEGACY
Debe soportar la publicación de las actuales aplicaciones legacy del BIESS, que trabajan con TLS v1 y v1.1.

	El contratista deberá garantizar el buen funcionamiento de la solución, sin que se generen congestión de tráfico, encolamiento, sobreprocesamiento de recursos u otros problemas que puedan generar un bajo perfomance de la solución.
	METODOLOGIA: El BIESS entregará el listado de aplicaciones, las cuales deberán ser configuradas por el contratista para el balanceo de carga.
	El contratista entregará al administrador de contrato la reportería de forma mensual y bajo demanda del servicio.
Contingencia.	Los servicios especializados pueden ser provistos en el sitio principal o en el sitio alterno, de acuerdo a la necesidad del BIESS.
Actualizaciones	Los servicios especializados provistos por el proveedor, deben pasar por el mantenimiento, actualizaciones o gestión de cambios, con base en las mejores prácticas, con el fin de garantizar la continuidad de los servicios.
9. SERVICIO DE WEB APPLICATION FIREWALL (WAF)	
	Características Generales
	Servicio de Firewall de Aplicaciones Web
	Tener características de by-pass o conmutación automática en caso de falla, permitiendo de esta manera la continuidad del servicio.
	Contar con los puertos Ethernet necesarios, que soporten el correcto funcionamiento de los componentes.
	Debe soportar al menos 10 sitios del BIESS.
	Ser escalable en caso de la institución lo requiera.
	Detallar el procedimiento para el escalamiento de los componentes.
	Presentar una arquitectura que permita definir un nivel de contingencia en caso de que se presente un incidente en los componentes, considerando que no debería impactar en el funcionamiento de las aplicaciones y que por la criticidad de los servicios debe recuperarse en un tiempo no mayor a 2 horas.
	Características Específicas
	Mantener características de proxy reverso para que por medio de una misma IP y puerto poder exponer varios servicios/sistemas
	Soportar aplicaciones WEB desarrolladas al menos en lenguajes java, php, html, con servidores de aplicaciones JBOSS, Tomcat, apache, etc.
	Soportar el bloqueo de las transacciones cuyo contenido corresponde a las firmas de los ataques conocidos, dejando pasar todo lo demás.
	Soportar la detección basada en el Modelo de Seguridad Negativa (modelo explícito basado en firma de ataques conocidos).
	Adicionar y/o modificar las firmas a través del usuario administrador.
	Actualizar de forma automática, por medio de una base de conocimiento propia o de terceros de las firmas de ataques, con el objetivo de mantenerse al día, respecto de las últimas amenazas.
	Detectar ataques multi-nivel incluyendo, red, sistema operativo, Web Server Software, y ataques en la capa de aplicación.
	Incluir técnicas utilizadas dentro del estándar OWASP to 10.
	Contar con un modo de aprendizaje dinámico que permita definir cuáles son las acciones esperadas y aceptadas para los usuarios que utilizan las aplicaciones. Si estas operaciones no están contempladas en lo que se espera como "normal" debe alterar y/o bloquear.
	Contar con políticas de seguridad pre-configuradas de acuerdo a las mejores prácticas de seguridad en aplicaciones WEB que le permitan a la entidad proteger de una forma sencilla las aplicaciones desde el primer momento de la implementación de la solución.
	Detectar la estructura y elementos de la aplicación, esta información podrá ser utilizada para la configuración del modelo positivo de seguridad.
	Incluir un proceso de aprendizaje dinámico de tal forma que se tenga una línea base que considere mínimo los siguientes elementos de la aplicación: Host válidos, URLs, métodos sin importar si su origen es sobre protocolos.

	Preservar la integridad de conexiones entre cliente y el servidor (no permitir modificaciones de conexiones) y asegurar que los paquetes sean los mismos antes y después de ser analizados por el WAF.
	Definir reglas para el modelo de seguridad positivo o negativo y permitir la creación de reglas de correlación con múltiples criterios.
	Proteger las aplicaciones que utilicen protocolos http y https.
	Descifrar el tráfico SSL, de las aplicaciones web cliente-servidor y reencriptarlo antes de su reenvío.
	Descifrar el tráfico SSL para inspección en los modos: puente o sniffer. Sin terminar o cambiar la conexión.
	Contar con protección para rastrear e identificar las fuentes de ataques originadas desde proxies anónimos, direcciones IP maliciosas, botnets, y sitios de phishing.
	Permitir ajustar las fuentes de ataque para identificar y bloquear tráfico considerado malicioso.
	Ajustar dinámicamente las políticas de seguridad con base en la identificación de las fuentes de ataque o de las fuentes que denoten actividad sospechosa.
	Bloquear solicitudes de acceso basado en reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por BotNet, DDoS, Phishing o redes de anonimización.
	El contratista deberá garantizar el buen funcionamiento de la solución, sin que se generen congestión de tráfico, encolamiento, sobreprecesamiento de recursos u otros problemas que puedan generar un bajo perfomance de la solución.
	El contratista entregará al Administrador de contrato la reportería de forma mensual y bajo demanda del servicio.
Contingencia.	Los servicios especializados pueden ser provistos en el sitio principal o en el sitio alterno, de acuerdo a la necesidad del BIESS.
Actualizaciones	Los servicios especializados provistos por el proveedor, deben pasar por el mantenimiento, actualizaciones o gestión de cambios, con base en las mejores prácticas, con el fin de garantizar la continuidad de los servicios.
10. SERVICIO DE DDOS	
	Servicio de protección DDoS. Se debe contar con protección contra ataques de denegación de servicio volumétricos que atenten contra la infraestructura del BIESS. Este sistema debe contar con capacidad de contención de ataques volumétricos de hasta 1 Gbps con origen internacional o local. El sistema debe contar con los siguientes requisitos:
	La contención del ataque se debe realizar de forma automática, sin que el servicio se vea afectado
	El sistema Anti DDoS debe funcionar fuera de línea (off-line) con detección basada en flow collector y snmp.
	Tiempos y umbrales de detección personalizables
	Detección de ataques distribuidos.
	El contratista entregará dos usuarios nombrados con el rol de auditor con permisos de lectura únicamente para monitoreo de la solución, así como los accesos a los Dashboard generados para este servicio (modo visualización)
	Este servicio deberá poder ser usado tanto en el Data Center de Guayaquil o en el Data Center de Quito, según la necesidad del BIESS, por lo que el contratista realizará las gestiones necesarias para su provisión.
	El contratista deberá garantizar el buen funcionamiento de la solución, sin que se generen congestión de tráfico, encolamiento, sobreprecesamiento de recursos u otros problemas que puedan generar un bajo perfomance de la solución.
	El contratista entregará al Administrador de contrato la reportería de forma mensual y bajo demanda del servicio.
Contingencia.	Los servicios especializados pueden ser provistos en el sitio principal o en el sitio alterno, de acuerdo a la necesidad del BIESS.

Actualizaciones	Los servicios especializados provistos por el proveedor, deben pasar por el mantenimiento, actualizaciones o gestión de cambios, con base en las mejores prácticas, con el fin de garantizar la continuidad de los servicios.

11. SERVICIO DE STORAGE (STaaS), Capacidad 10 TB

- El contratista deberá proveer el servicio de espacio de almacenamiento (storage) en una nube local privada (Storage as a Service), en el Data Center Principal, con una capacidad mínima de 10 TB; el protocolo de conexión entre el ambiente del BIESS y el servicio de storage será por NFS o S3, mediante una vlan dedicada entre los ambientes del proveedor y el o los ambientes del BIESS.

-El almacenamiento deberá estar alojado en infraestructura física ubicada dentro del territorio ecuatoriano, operada directamente por el contratista. No se requiere replicación al Data Center Alterno (DCA). Se deberá asignar un espacio de 1TB en el servicio de StaaS para almacenamiento de videos de cintoteca.

12. SERVICIO DE BACKUP (BaaS), Capacidad 50 TB

El contratista deberá proveer el servicio de respaldo de datos administrado en la nube local privada (Backup as a Service), con una capacidad mínima de 50 TB, alojado en territorio ecuatoriano. El servicio deberá ser brindado 24x7 incluyendo monitoreo y soporte durante la vigencia del contrato.

- La solución deberá cumplir con las siguientes características técnicas mínimas:
  - Protección de cargas de trabajo de servidores virtuales desde una única consola centralizada y que sea administrada por la entidad
  - Definición de políticas de frecuencia y retención configurables por el administrador del BIESS.
  - Respaldo y recuperación de máquinas virtuales completas para ambiente vmware versión 6.5 y 7.x.

13.SERVICIO DE DEEP & DARK WEB (1 dominio)

El componente de visibilidad en la internet profunda deberá proveer inteligencia accionable mediante los siguientes requerimientos:

Infiltración y Monitoreo de Canales Cerrados: Rastreo continuo de menciones de la marca, palabras clave e infraestructura de la institución dentro de foros de cibercriminales, mercados de la Darknet (redes TOR, I2P, Freenet), así como en grupos y comunidades privadas de mensajería instantánea (Telegram, WhatsApp y Discord).
Alertas Tempranas de Ransomware y Vulnerabilidades: Notificación inmediata ante campañas coordinadas por grupos de Ransomware activos que identifiquen a la institución o a sus proveedores críticos como víctimas.

Servicio De Scraping

Con la finalidad de incorporar mecanismos para detectar la copia de los diferentes componentes de los sitios web del BIESS, el servicio deberá incorporar una funcionalidad avanzada de recolección, extracción y procesamiento automatizado de datos procedente de fuentes externas a la red institucional (incluyendo Clear Web, Deep Web y Dark Web), orientada a la identificación proactiva y continua (24/7) de riesgos digitales específicos contra el BIESS, tales como fugas de credenciales de correos institucionales, suplantación de identidad digital de la marca (phishing y typosquatting) y filtración de información confidencial o código fuente."

Alertas de Anomalías y Resúmenes con IA Generativa: Capacidad de generar alertas automáticas ante picos inusuales de menciones de la institución (detección de anomalías) y resúmenes ejecutivos utilizando modelos de Inteligencia Artificial Generativa entrenados en el lenguaje del cibercrimen

14. SERVICIO DE BRAND PROTECTION (1 dominio))

El servicio contratado no debe limitarse a la detección, sino que debe garantizar la remediación efectiva de las amenazas externas bajo las siguientes condiciones:

Desmantelamiento Multivector: Capacidad de ejecutar solicitudes de remoción efectivas contra portales de *Phishing*, abuso de marca en anuncios de motores de búsqueda pagados (Google Ads), aplicaciones móviles falsas en tiendas oficiales/no oficiales, ataques de *Typosquatting* (dominios maliciosos similares) y perfiles falsos en redes sociales principales (Facebook, Instagram, LinkedIn, X, TikTok, YouTube).

Garantía de Persistencia (Re-up Protection): Monitoreo continuo post-remediación que asegure que si un contenido malicioso o sitio fraudulento previamente dado de baja vuelve a aparecer en un periodo de al menos quince (15) días, sea detectado y mitigado de forma automática como un re-incidente sin generar costos adicionales. **Protección Integral y Detección de Clonación de Sitios Web:** capacidad de inspección y rastreo avanzado mediante tecnología de balizamiento digital OnePixel mediante la inserción de un recurso técnico imperceptible y automatizado dentro del código fuente del sitio web oficial	
15. SERVICIO DE DATA LEAKAGE (1 dominio)	
	El servicio/plataforma deberá cumplir obligatoriamente con las siguientes capacidades de monitorización en tiempo real
	Monitoreo Continuo de Credenciales Corporativas: Capacidad de identificar credenciales institucionales expuestas (dominios específicos de la entidad) provenientes de brechas de datos masivas (*Big Leaks*) y repositorios públicos o privados.
	Detección de Credenciales por Infostealers: Identificación precisa de credenciales de usuarios, empleados o clientes comprometidas a través de malware especializado de tipo *infostealer*, recolectando metadatos del contexto de la infección (fecha aproximada, país, IP del equipo infectado y URLs afectadas).
	Detección de Secretos y Llaves de Código: Capacidad de escanear y alertar sobre la exposición involuntaria de llaves de configuración, contraseñas en texto plano, tokens y llaves criptográficas/privadas expuestas en repositorios de código público como GitHub, plataformas de commits o sitios de intercambio de texto (*Paste sites* como Pastebin, Ghostbin, ControlC, entre otros).
	Validación de Exposición de Bases de Datos: Capacidad de insertar registros o tokens simulados (*Tracking Tokens*) dentro de las bases de datos de la institución para detectar de manera proactiva si la información interna ha sido filtrada, facilitando el proceso de auditoría y aislamiento de la fuente de la fuga.
	Monitoreo de Datos Sensibles en Almacenamiento Cloud: Vigilancia activa de archivos institucionales o información confidencial expuesta en plataformas colaborativas o repositorios de almacenamiento en la nube.

CONDICIONES GENERALES	
Tiempo del servicio	La duración del servicio deberá ser de 365 días calendario
Responsabilidad	Cualquier inconveniente que pudiera suscitarse por problemas relacionados a los servicios de Data Center (condiciones físicas), será responsabilidad del contratista, para ello debe contar con técnicos especialistas que residan en la ciudad de Quito y Guayaquil respectivamente.
SLA	El Oferente adjudicado deberá entregar el SLA elaborado por el BIESS, firmado previa suscripción del contrato.
Varios	El contratista debe notificar al BIESS las ventanas de mantenimiento programadas para su infraestructura y se comprometerá en notificar con la debida anticipación (no menor a 7 días calendario), indicando los tiempos de inicio, indisponibilidad y finalización de la operación. Como parte del servicio, el BIESS requiere realizar al menos 2 veces al año, Pruebas de continuidad del Negocio u otras pruebas técnicas de contingencia, por lo tanto, se requiere que el contratista del soporte necesario para realizar estas pruebas y activación del Sitio Alterno sin que esto represente un costo adicional para la institución. En caso de que el BIESS requiera de alguna característica que soporten los equipos utilizados de los servicios gestionados, el contratista será encargado de verificar la factibilidad técnica, y configurar el servicio conforme lo indique la metodología de trabajo. Se realizará los ajustes en los valores con base en el valor convenido. Todos los servicios gestionados deben acoplarse a la arquitectura y modo de funcionamiento requeridos por el BIESS. Por lo que el contratista podrá y/o deberá realizar adecuaciones en el/los Data Centers, configuraciones, o inclusive incorporar elementos de hardware o software de ser

	necesario para este fin, sin que esto represente costo adicional para el BIESS. El oferente deberá realizar una visita técnica, a los centros de procesamiento Principal y Alterno, con el fin de identificar los componentes y recursos necesarios para la correcta energización, re acondicionamiento, controles ambientales y otros necesarios para el correcto funcionamiento de la infraestructura en cumplimiento a las prácticas de datacenter TIER III. El contratista debe realizar una evaluación para validar compatibilidad de los aplicativos del BIESS con la solución propuesta de balanceo y protección de seguridad WAF de servicios gestionados; misma que será registrada en una acta que avala que las actividades aquí solicitadas fueron realizadas. Debido a que el presente proceso involucra el manejo de tecnología especializada en los Centros de Procesamiento de Datos Principal y Alterno, el personal técnico del BIESS requiere la transferencia de conocimiento mínimo de 8 ó 12 horas por cada una de las soluciones en servicios gestionados como Firewall, Balanceadores, WAF, AntiDDoS. Adicionalmente, el contratista deberá proporcionar plataformas de acceso web bajo demanda que permitan al personal técnico consultar contenidos, cursos y materiales complementarios en línea, asegurando la disponibilidad continua de recursos de capacitación más allá de las sesiones presenciales. Los instructores designados deberán contar con certificación oficial del fabricante en la tecnología impartida. Al finalizar la transferencia, se entregará un certificado de participación respaldado por la empresa, garantizando que la capacitación cumple con los estándares de actualización periódica exigidos por el fabricante. Esta transferencia de conocimiento se realizará en las fechas y horas acordadas entre las partes. Todos los gastos de materiales correrán por parte del contratista. El contratista entregará un temario por cada solución para revisión y aprobación del administrador de contrato. El temario se basará en el temario oficial del fabricante para la certificación equivalente a administración de la solución. Él o los instructores deberán estar certificados en la tecnología de la cual estén brindando la transferencia de conocimientos. Se deberá entregar un certificado con respaldo de la empresa al culminar la misma.

SERVICIOS BAJO DEMANDA
16. Puntos de red cobre
Posterior al inicio del servicio, el BIESS a través del Administrador de Contrato solicitará bajo demanda nuevos puntos de red, para lo cual, El contratista debe proporcionar los patch cords de Cbre que se requieran para la conectividad desde los switches del contratista hacia los equipos a ser alojados. Todos los patch cords utilizados en nuevas solicitudes de conexión deben ser nuevos y certificados de fábrica.
17. Puntos de red fibra a 1GB
Posterior al inicio del servicio, el BIESS a través del Administrador de Contrato solicitará bajo demanda nuevos puntos de red, para lo cual, El contratista debe proporcionar los patch cords de fibra que se requieran para la conectividad desde los switches del contratista hacia los equipos a ser alojados. Todos los patch cords utilizados en nuevas solicitudes de conexión deben ser nuevos y certificados de fábrica.
18. Puntos de red fibra a 10GB

Posterior al inicio del servicio, el BIESS a través del Administrador de Contrato solicitará bajo demanda nuevos puntos de red, para lo cual, El contratista debe proporcionar los patch cords de fibra que se requieran para la conectividad desde los switches del contratista hacia los equipos a ser alojados. Todos los patch cords utilizados en nuevas solicitudes de conexión deben ser nuevos y certificados de fábrica.
19. Cintas (Espacio en cintoteca)
el BIESS a través del Administrador de Contrato solicitará bajo demanda de espacio adicional de almacenamiento de cintas en cintoteca, con las mismas condiciones descritas anteriormente en el punto 4 “Cintoteca CPDP”. El contratista deberá llevar el reporte de cintas adicionales en el informe mensual de Housing.
20. SERVICIO DE STORAGE (STaaS), Capacidad 59 TB
el BIESS a través del Administrador de Contrato solicitará bajo demanda del servicio de Storage (STaaS) adicional, con las mismas condiciones descritas anteriormente en el punto 11 “Servicio de Storage (STaaS)”.
21. SERVICIO DE BACKUP (BaaS), Capacidad 39 TB
El BIESS a través del Administrador de Contrato solicitará bajo demanda del servicio de Backup (BaaS)adicional, con las mismas condiciones descritas anteriormente en el punto 12 “Servicio Backup (BaaS)”.

Para la prestación del servicio, se ha determinado que el BIESS al ser una entidad de banca pública que administra información financiera y transaccional crítica, cuya disponibilidad, integridad y confidencialidad son indispensables para la prestación ininterrumpida de los servicios institucionales, la ejecución de operaciones financieras crediticias y el cumplimiento de las disposiciones regulatorias en materia de gestión de riesgos y continuidad del negocio, se requiere que el proveedor del servicio sea propietario tanto del Data Center Principal como del Data Center Alterno. Esta condición garantiza el control directo, permanente e integral sobre la infraestructura física y tecnológica que soportará los servicios contratados, eliminando la dependencia de terceros para la administración, mantenimiento, ampliación, acceso y recuperación de la infraestructura crítica. Asimismo, mitiga riesgos operativos asociados a la terminación o modificación de contratos de uso o arrendamiento, restricciones de acceso, controversias, cambios de condiciones operativas, insolvencia o decisiones comerciales de terceros que puedan comprometer la disponibilidad de los servicios. La propiedad de ambos Data Centers fortalece la capacidad del proveedor para ejecutar de manera inmediata los planes de continuidad del negocio y recuperación ante desastres, garantizando la disponibilidad permanente de la infraestructura, la atención oportuna de incidentes críticos y la resiliencia operativa requerida para soportar los servicios tecnológicos esenciales de la institución, reduciendo significativamente la exposición a riesgos que podrían afectar la estabilidad de la operación y la prestación de los servicios institucionales.

3. PROFORMAS:

Con la finalidad de realizar un estudio de proveedores locales que estuvieran en la posibilidad de brindar el servicio gestionado de Data Center, se realizaron invitaciones telefónicamente a posibles proveedores de lo cual se obtuvo, la aceptación por parte de CNT, a una reunión presencial a fin de darles a conocer las condiciones generales del servicio requerido.

La Corporación Nacional de Telecomunicaciones (CNT E.P.), mediante Oficio Nro. CNTEP-GNNEG-SC-SO-2026-0573-O de fecha 15 de mayo de 2026 (referenciado en el archivo BIESS-CTEC-2026-0012-

E.pdf), ratificó oficialmente la imposibilidad técnica de brindar de forma inmediata los servicios de housing y moving, motivo por el cual no remitió la cotización respectiva

En base a los múltiples acercamientos con los posibles proveedores no se obtuvo manifestaciones de interés de proveedores nacionales que estuvieran interesados en ofrecer el servicio objeto de esta contratación, gestiones que llevaron varios meses y que finalmente se determinó la imposibilidad de obtener más de una cotización para el servicio objeto de esta contratación.

Mediante correo electrónico de 17 de junio de 2026, se solicitó la presentación de proformas al proveedor actual, quien presento la cotización para el servicio objeto de esta contratación.

Cotización obtenida:

			TELCONET S.A		
			991327371001		
ÍTEM	**SERVICIO**	**CANTIDAD**	***PROFORMA***		
HOUSING CENTRO DE DATOS			*VALOR UNIT.*	*VALOR MENSUAL*	*VALOR TOTAL*
1	Centro De procesamiento de Datos Principal(Guayaquil)y Componentes (RACK).	4	$4.400,00	$17.600,00	$211.200,00
2	Centro de procesamiento de datos alterno (Quito)y componentes (RACK)	2	$5.650,00	$11.300,00	$135.600,00
3	Interconexión LAN CPDP – CPDA (100 Mbps)	1	$1.600,00	$1.600,00	$19.200,00
4	Cintoteca CPDP	1043	$7,50	$7.822,50	$93.870,00
5	Servicio de horas de manos remotas	2	$80,00	$160,00	$1.920,00
6	Servicio de Mailling (Antispam), dominio biess.info.ec	1	$1.650,00	$1.650,00	$19.800,00
7	Servicio de Seguridad Perimetral (Next Generation Firewall)	1	$7.530,00	$7.530,00	$90.360,00
8	Servicio de Balanceo de Aplicaciones	1	$6.310,00	$6.310,00	$75.720,00
9	Servicio de Web Application Firewall (WAF)	1	$5.460,00	$5.460,00	$65.520,00
10	Servicio de DDoS	1	$2.390,00	$2.390,00	$28.680,00
11	Servicio de Storage (STaaS), capacidad 10 TB	10	$20,00	$200,00	$2.400,00
12	Servicio de Backup (BaaS), capacidad 50 TB	50	$90,00	$4.500,00	$54.000,00
13	Servicio de Deep & Dark Web (1 dominio)	1	$700,00	$700,00	$8.400,00
14	Servicio de Brand Protection (1 dominio)	1	$600,00	$600,00	$7.200,00
15	Servico Data Leakage (1 dominio)	1	$250,00	$250,00	$3.000,00

			SUBTOTAL	**$68.072,50**	**$816.870,00**
SERVICIOS BAJO DEMANDA					
16	Puntos de red cobre	30	$15,00	$450,00	$2.250,00
17	Puntos de red fibra a 1GB	5	$17,00	$85,00	$425,00
18	Puntos de red fibra a 10GB	5	$28,00	$140,00	$700,00
19	Cintas (Espacio en cintoteca)	738	$7,00	$5.166,00	$25.830,00
20	Servicio de Storage (STaaS), capacidad 59 TB	59	$20,00	$1.180,00	$5.900,00
21	Servicio de Backup (BaaS), capacidad de 39 TB	39	$90,00	$3.510,00	$17.550,00
			SUBTOTAL	**$10.531,00**	**$52.655,00**
			SUBTOTAL	$78.603,50	$869.525,00
			IVA	$11.790,53	$130.428,75
			TOTAL	$90.394,03	$999.953,75

4. MONTOS DE CONTRATOS SIMILARES REALIZADOS POR EL BIESS

En cumplimiento del literal c del artículo 26 del Reglamento para las Contrataciones de Giro Espeícfico del Negocio del BIESS, se procedió con la revisión histórica en el portal web institucional del Banco del Instituto Ecuatoriano de Seguridad Social (BIESS), específicamente en el módulo de consulta de procesos de contratación, con la finalidad de identificar los procesos de contratación efectuados en los últimos dos años. Esta verificación interna permitió constatar que la institución ha gestionado y contratado este servicio el año 2025 bajo la modalidad de Giro Específico del Negocio, conforme el siguiente detalle:

AÑO DE CONTRATACIÓN	*NRO. DE CONRATO*	*OBJETO DE CONTRATACIÓN*	*MONTO SIN IVA*	*CONTRATISTA*
2025	*BIESS-CJUR-GE-006-2025*	*CONTRATACIÓN DE SERVICIOS GESTIONADOS DE DATA CENTER*	*$ 784.400,00*	*TELCONET S.A.*

5. DETERMINACIÓN DEL PRESUPUESTO REFERENCIAL:

El literal b) del artículo 26 del Reglamento para las Contrataciones del Giro Específico del Negocio del BIESS establece que, para la determinación del presupuesto referencial entre otros aspectos, señala que se deberán obtener al menos dos proformas; sin embargo, la misma disposición prevé también como excepción aquellos procedimientos de contratación en los que, de manera debidamente justificada, resulte imposible obtener el referido número de cotizaciones.

En este contexto, la Coordinación de Tecnología, realizó las gestiones correspondientes para obtener proformas de proveedores que operan en el mercado nacional; sin embargo, no fue posible contar con al menos dos cotizaciones, debido a las características altamente especializadas del objeto contractual y a los requisitos técnicos que demanda la prestación del servicio objeto de esta contratación.

El servicio gestionado de Data Center requerido por el BIESS constituye una infraestructura tecnológica crítica para la operación institucional, por cuanto soporta el procesamiento y almacenamiento de información financiera y transaccional cuya disponibilidad, integridad y confidencialidad son indispensables para garantizar la prestación ininterrumpida de los servicios institucionales, la ejecución de las operaciones crediticias y el cumplimiento de las disposiciones regulatorias aplicables en materia de gestión integral de riesgos, seguridad de la información y continuidad del negocio. En este sentido, el servicio comprende el alojamiento de la infraestructura tecnológica tanto en un Data Center Principal como en un Data Center Alterno; por lo tanto, se presume que estas condiciones técnicas y operativas han incidido en la decisión de los proveedores de abstenerse de presentar cotizaciones.

Determinación del Presupuesto referencial:

Como resultado de las gestiones efectuadas y considerando las condiciones técnicas descritas, únicamente el proveedor actual Telconet S.A. presentó una cotización conforme a los requerimientos establecidos por el BIESS. En consecuencia, y al haberse evidenciado la imposibilidad material de obtener una segunda proforma de proveedores que cumplan integralmente con las condiciones técnicas requeridas, se justifica la determinación del presupuesto referencial con una sola cotización, al amparo de la excepción prevista en el literal b) del artículo 26 del Reglamento para las Contrataciones del Giro Específico del Negocio del BIESS, por cuanto constituye la única alternativa técnicamente viable para garantizar la continuidad del negocio, la seguridad de la infraestructura tecnológica y la mitigación de los riesgos operativos asociados a la prestación del servicio.

ÍTEM	SERVICIO	CANTIDAD				*VALOR TOTAL*

	HOUSING CENTRO DE DATOS		***VALOR UNIT.***	***VALOR MENSUAL***	***MESES DEL SERVICIO***	***ANUAL***
1	Centro De procesamiento de Datos Principal(Guayaquil)y Componentes (RACK).	4	$4.400,00	$17.600,00	12	$211.200,00
2	Centro de procesamiento de datos alterno (Quito)y componentes (RACK)	2	$5.650,00	$11.300,00	12	$135.600,00
3	Interconexión LAN CPDP – CPDA (100 Mbps)	1	$1.600,00	$1.600,00	12	$19.200,00
4	Cintoteca CPDP	1043	$7,50	$7.822,50	12	$93.870,00
5	Servicio de horas de manos remotas	2	$80,00	$160,00	12	$1.920,00
6	Servicio de Mailling (Antispam), dominio biess.info.ec	1	$1.650,00	$1.650,00	12	$19.800,00
7	Servicio de Seguridad Perimetral (Next Generation Firewall)	1	$7.530,00	$7.530,00	12	$90.360,00
8	Servicio de Balanceo de Aplicaciones	1	$6.310,00	$6.310,00	12	$75.720,00
9	Servicio de Web Application Firewall (WAF)	1	$5.460,00	$5.460,00	12	$65.520,00
10	Servicio de DDoS	1	$2.390,00	$2.390,00	12	$28.680,00
11	Servicio de Storage (STaaS), capacidad 10 TB	10	$20,00	$200,00	12	$2.400,00
12	Servicio de Backup (BaaS), capacidad 50 TB	50	$90,00	$4.500,00	12	$54.000,00
13	Servicio de Deep & Dark Web (1 dominio)	1	$700,00	$700,00	12	$8.400,00
14	Servicio de Brand Protection (1 dominio)	1	$600,00	$600,00	12	$7.200,00
15	Servico Data Leakage (1 dominio)	1	$250,00	$250,00	12	$3.000,00
			SUBTOTAL	**$68.072,50**		**$816.870,00**
	SERVICIOS BAJO DEMANDA					
16	Puntos de red cobre	30	$15,00	$450,00	5	$2.250,00
17	Puntos de red fibra a 1GB	5	$17,00	$85,00	5	$425,00
18	Puntos de red fibra a 10GB	5	$28,00	$140,00	5	$700,00
19	Cintas (Espacio en cintoteca)	738	$7,00	$5.166,00	5	$25.830,00
20	Servicio de Storage (STaaS), capacidad 59 TB	59	$20,00	$1.180,00	5	$5.900,00
21	Servicio de Backup (BaaS), capacidad de 39 TB	39	$90,00	$3.510,00	5	$17.550,00
			SUBTOTAL	**$10.531,00**		**$52.655,00**
				SUBTOTAL		$869.525,00
				IVA		$130.428,75
				TOTAL		$999.953,75

El presupuesto referencial es de USD $869.525,00 (Ochocientos sesenta y nueve mil quinientos veinte y cinco 00/100 dólares de los Estados Unidos de América) más IVA por considerarse el más conveniente para los intereses de la Institución.

6. FIRMAS DE RESPONSABILIDAD

NOMBRES Y APELLIDOS	CARGO	FIRMA
Elaborado por:	Ing. Carla Corrales Hidalgo Analista Senior de Infraestructura Tecnológica	Validar únicamente en FirmaEC. Firmado electrónicamente por: CARLA TATIANA CORRALES HIDALGO
Revisado por:	Ing. Tatiana Aldaz Directora de Infraestructura Tecnológica	Validar únicamente en FirmaEC. Firmado electrónicamente por: TATIANA PAOLA ALDAZ FLORES
Aprobado por:	Ing. Richard Osorio Coordinador de Tecnología	Validar únicamente en FirmaEC. Firmado electrónicamente por: RICHARD EDUARDO OSORIO SALCEDO