1. BIENES REQUERIDOS

Los equipos ofertados deben ser nuevos de fábrica y que la fecha de fin de soporte del fabricante sea no menor a 5 años, a partir de la firma del Acta Entrega Recepción Parcial de bienes e instalación.

1.1. ELEMENTOS DE HARDWARE

a) ITEM 1: <u>Balanceadores de Carga con funcionalidad de WAF para los Centro de Cómputo Principal y Alterno</u> (2 Equipos Centro de cómputo Principal y 1 equipo centro de cómputo alterno)

Características generales físicas y de rendimiento
El equipo ofertado debe ser una plataforma de hardware de propósito específico denominado "appliance".
El sistema operativo debe ser de propósito específico y no uno de uso genérico, es decir un sistema operativo desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios, Seguridad de Aplicaciones basadas en IP (TCP/UDP) y Servicios Web.
Los valores de desempeño solicitados deberán ser logrados por el equipo "appliance" como un sistema independiente y autónomo que cumpla el desempeño exigido y no como la suma o agregación de varios "appliance" que logren sumar el valor solicitado.
Se debe ofrecer dos (2) equipos en alta disponibilidad funcionando en configuración de Activo – Stand by para el Centro de Cómputo principal. Se debe ofertar un (1) equipo stand alone para el centro de cómputo alterno.
Cada equipo debe cumplir con las siguientes características: • La solución debe soportar un Throughput en L4 de al menos 72831 Mbps y en L7 de al menos 36415 Mbps. • La solución debe soportar al menos 64 Millones de conexiones concurrentes en L4 • La solución debe soportar al menos 20 Gbps de Thoughput para tráfico cifrado
Cada equipo debe contar con al menos las siguientes interfaces de red: • Al menos 8 puertos SFP+, con opción de conectividad de 1 Gbps o 10 Gbps • Cada equipo debe incluir 4 transceivers de Cobre, 4 SFP+ de 10 Gbps
Cada equipo debe disponer al menos 1 puerto de administración.
Cada equipo debe estar en capacidad de contar con fuentes de poder redundantes AC, entradas de voltaje de 110 a 220 VAC que se puedan remover en caliente (hot-swap).
Los equipos deberán ser instalados en rack estándar de 19", máximo 2RU.
Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual.
La solución debe tener la capacidad de recuperar las sesiones del sistema en forma inmediata y automática, en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.
Cada equipo debe incluir al menos 64 GB de memoria RAM.
Cada equipo debe incluir al menos un disco duro de 400 GB de estado sólido (SSD).
Debe tener capacidad para que la sincronización de configuración no afecte el desempeño de los equipos.
La configuración será sincronizada entre todos los dispositivos del grupo pudiendo escoger si la sincronización se realiza de manera automática o manual.
Los equipos deben contar con aceleración basada en hardware, con la capacidad de manejar perfiles de acuerdo a las funciones que vaya a ejecutar como, las siguientes: protección WAF, manejos de ambientes de networking, y manejo de trafico de L4, TCP, UDP, IPv4, IPv6.

Funciones de administración de tráfico
La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web.
La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.
La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.
La solución debe permitir la 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.
La solución debe permitir el control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo. Estos métodos deben realizarse de manera nativa y no por medio de configuración por scripting: • Round Robin • Proporcional (Ratio) • Proporcional dinámico • Respuesta más rápida • Conexiones mínimas • Menor número de sesiones
El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.
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. • Ejecución de scripts para determinar la respuesta emulando un cliente. • Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red. • Capacidad de configurar un monitoreo basado en el número de intentos de conexión o request o intentos de request que ocurren en un período específico de tiempo. • Monitoreo de aplicaciones de mercado: o LDAP o FTP o SMTP o IMAP/POP3 o RADIUS o SIP o SNMP
La solución debe realizar todos estos métodos de persistencia de las conexiones: • Dirección IP origen • Cookies • Hash • SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia • Sesiones SSL
La solución debe tener la capacidad para crear persistencia general en protocolos TCP/UDP
La solución debe soportar los 3 métodos de persistencia por Cookie: Cookie Insert, Cookie Pasivo y Cookie Rewrite.
La solución debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.
La solución debe ser capaz de realizar un método secundario de persistencia, en caso de que el primer método no pueda ejecutarse por factores externos a la plataforma.

La solución debe permitir soporte de API para construir aplicaciones de administración o monitoreo personalizadas: • Soporte de XML, que sea base del sistema operativo. • Que permita la integración con aplicaciones como VMWare vCenter, Soporte de Java, SOAP, PowerShell y Python, ya sea directo desde el ADC o a través de la consola de administración centralizada. • Las interfaces de control deben ser accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados.
La solución debe soportar REST API.
La solución debe permitir que sea posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts.
La solución debe soportar scripts de programación basados en un lenguaje estructurado (TCL) que permita crear funcionalidades que por defecto no se encuentren en el menú de configuración u opciones y debe soportar la creación de procedimientos o funciones que pueden ser utilizadas desde cualquier otro script.
La solución debe soportar e incluir geolocalización, de manera que pueda tomar decisiones basado en una base de datos de continentes, países y de direcciones IP.
La base de datos de geolocalización debe incluir los países de América Latina.
Funciones de aceleración de tráfico
La solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de: • Memoria cache. • Compresión tráfico HTTP • Optimización de conexiones a la aplicación a nivel TCP Multiplexación de conexiones hacia los servidores
La solución debe comprimir tráfico http a través del estándar GZIP y compatible con browsers MS Internet Explorer, Google Chrome, Mozilla Firefox, Safari, Microsoft Edge, Opera.
Cada equipo debe contar con una capacidad de compresión de tráfico usando aceleración por Hardware dedicado.
La solución debe aplicar cache a listas de URLs específicas, así mismo como su exclusión.
La solución debe tener la capacidad de aplicar compresión basándose en el content-type.
La solución debe soportar el protocolo HTTP2 y funcionar como Gateway para este protocolo.
La solución debe soportar perfiles de HTTP2 los cuales puedan comprimir los encabezados http.
Estándares de red
Soporte VLAN 802.1q, Vlan tagging
Soporte de 802.3ad para definición de múltiples troncales
Soporte de NAT, SNAT
Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.
Soporte de Rate Shapping.
Debe soportar Ethernet Bridging para entornos de redes virtualizadas.
Debe soportar protocolos de enrutamiento BGP, RIP, OSPF.
Virtualización
La solución debe soportar la creación de instancias virtuales para ambientes específicos de la entidad, en donde se combinan soluciones dentro de una misma instancia en ambientes independientes que conviven en el mismo hardware: • Alta disponibilidad de aplicaciones y seguridad WAF. • Presentación de aplicaciones, balanceo de enlaces y sitios geográficos.
Cada equipo debe soportar virtualización del dispositivo que soporte al menos 12 instancias del sistema operativo corriendo simultáneamente, cada instancia usando CPU y Memoria independientes.

Cada instancia virtual debe permitir ejecutar su propia versión de sistema operativo y no ser compartido entre instancias virtuales.
Cada instancia virtual debe soportar el uso de múltiples gateways.
Características de administración general del Sistema
Para la administración de los equipos appliance se debe contar con Interfaz de línea de comandos por SSH vía CLI, interfaz de administración gráfica basada en Web seguro (HTTPS)
Los equipos deben integrarse con Directorio Activo Windows 2008 o superior, para la autenticación de usuarios para gestión.
Los equipos deben integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión.
Se debe incluir comunicación cifrada y permitir la autenticación de los equipos y de los usuarios administradores/supervisores con Certificados Digitales.
Los equipos deben soportar el envío de alertas y eventos a un Sistema Centralizado mediante: • Protocolo SysLog • Notificación vía SMTP SNMP versión.2.0 o superior.
El sistema de administración de los equipos físicos debe ser totalmente independiente de los equipos virtuales.
Los equipos deben contar con un módulo de administración tipo lights out o módulo de administración o consola central o su equivalente que permita encender, apagar y reiniciar el sistema de manera remota y visualizar el proceso de arranque.
La interfaz de administración gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real, como por ejemplo: uso de CPU, memoria, conexiones concurrentes.
La interfaz de administración gráfica debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP y HTTPS como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados.
Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej, Oracle, Microsoft) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.
Funciones Generales de Seguridad
Cada equipo debe soportar seguridad SSL con las siguientes características: • Incluir el soporte de aceleración SSL usando Hardware Dedicado • Incluir mínimo 30.000 transacciones o conexiones por segundo SSL (RSA 2K Keys) • Incluir mínimo 20.000 transacciones o conexiones por segundo SSL (EC-P256 o ECDSA P-256) • Soportar al menos 20 Gbps SSL Bulk Encryption (Thoughput SSL) • Soporte de llaves SSL RSA de al menos 2048 bits y ECC de 256 bits
La solución debe soportar mirroring de sesiones SSL. Si el equipo primario falla el equipo secundario debe mantener la sesión SSL.
El stack TLS del equipo debe soportar las siguientes funcionalidades/características: • Session ID • Session Ticket • OCSP Stapling (on line certificate status protocol) • Forward Secrecy
La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic Curve Cryptography (ECC).
Cada equipo debe contar con protección de la cookie de SYN contra ataques de SYN Flood.
La solución debe soportar firmado criptográfico de cookies para verificar su integridad.
La solución debe permitir la funcionalidad de transparent HTTPS Proxy (esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, sin

embargo, el equipo balanceador debe ser capaz de desencriptar y reencriptar el tráfico SSL sin que el balanceador termine la sesión SSL), outbound SSL inspection e inbound SSL inspection.
La solución debe soportar la extensión STARTTLS para el protocolo SMTP de manera que permita cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el puerto.
La solución debe soportar HSTS (HTTP Strict Transport Security).
La solución debe soportar e incluir un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en las siguientes categorías: • Scanners • Exploits Windows • Denial of Service • Proxies de Phishing • Botnets • Proxies anónimos
Balanceo a nivel global y de enlaces
La solución debe permitir alta disponibilidad de aplicaciones distribuidas en 2 o más datacenters, sin importar la ubicación geográfica.
Debe funcionar como un servidor DNS autoritativo para los dominios que requieren balanceo global.
Debe funcionar como un servidor DNS autoritativo de alto desempeño, permitiendo manejar un dominio completo o delegación de parte de un dominio. Debe ser autónomo sin necesidad de balancear requerimientos DNS a una granja de servidores DNS.
Debe funcionar como un servidor DNS cache autónomo, sin necesidad de balancear requerimientos DNS a una granja de servidores.
Para el balanceo global (DNS), debe permitir los siguientes métodos de balanceo estático y dinámico, de manera nativa y no a través de configuración por scripting: • Round Robin • Global Availability • Geolocalización • Capacidad del Servicio • Least Connections • Proporcional (Ratio) • Persistencia estática
Debe manejar persistencia a nivel global, manteniendo a los usuarios en un mismo datacenter por el transcurso de su sesión.
Permitir balanceo de cargas ente datacenters de acuerdo a la ubicación geográfica, soportando utilizar estas tres opciones: continente, país y dirección IP.
Debe permitir la creación de un método de balanceo global, el cual este basado en el origen y proximidad del tráfico, donde se puedan tomar decisiones de balanceo basadas en el origen de la consulta ya sea ésta proveniente de un origen público (internet) o un origen interno y distribuirla a un destino específico, de acuerdo a su posición geográfica para el caso de (internet) o una ubicación de direccionamiento interno como lo puede ser una sucursal.
Debe permitir monitoreo de la infraestructura y las aplicaciones a balancear, integrándose con otros equipos del mismo fabricante o de terceros.
Las zonas del DNS Autoritativo deben cargarse en RAM, para evitar latencias y tener tiempos de respuesta rápidos.
Debe permitir realizar balanceo de servidores DNS.
Debe soportar el protocolo DNSSEC.
Debe incluir una interfaz gráfica para la configuración y delegación de zonas DNS y subdominios.
Debe soportar registros AAAA para IPv6.
Debe soportar traducción entre DNS IPv4 y DNS IPv6.
La solución debe soportar al menos 2 Millones de respuestas DNS por segundo.

Firewall de aplicaciones Web (WAF)
Se requiere que la solución de web application firewall (WAF) esté integrada en la solución de balanceo de carga.
Los equipos deben incluir funcionalidad de Firewall de Aplicaciones (WAF) para la protección del tráfico cifrado de al menos los siguientes sitios y sus aplicaciones: - sri.gob.ec - srienlinea.sri.gob.ec - sriyyoenlinea.sri.gob.ec - cel.sri.gob.ec - celcer.sri.gob.ec
La funcionalidad de WAF debe permitir la personalización de la política, de manera que se pueda ajustar de manera granular de acuerdo al servicio específico que estará protegiendo, sus URLs, parámetros, métodos, de manera específica.
La funcionalidad de WAF debe trabajar en modo full proxy
La funcionalidad de WAF debe permitir la creación automática de políticas y deberá unificar múltiples URLs explicitas utilizando wildcards de manera de reducir la cantidad de objetos en la configuración.
La funcionalidad de WAF debe trabajar en modo simulación o learning y en modo bloqueo.
La funcionalidad de WAF debe permitir diferentes políticas de seguridad para diferentes aplicaciones
La funcionalidad de WAF debe contar con firmas preconfiguradas y permitir la creación de firmas personalizadas
La funcionalidad de WAF debe aprender el comportamiento de la aplicación automáticamente sin intervención humana
La funcionalidad de WAF debe permitir personalizar las páginas de bloqueo incluida la capacidad para responder a webservices
La funcionalidad de WAF debe contar con protección en contra de todos los ataques listados en el OWASP Top 10.
La funcionalidad de WAF debe incluir protección contra Web Scraping
La funcionalidad de WAF deberá proteger tanto aplicaciones web HTTP, como las aplicaciones web SSL y HTTPS
La funcionalidad de WAF deberá ser capaz de desencriptar e inspeccionar el tráfico SSL de las aplicaciones web, entre el cliente y el servidor y re-encriptarlo antes de su reenvío
La funcionalidad de WAF debe tener capacidad para aplicar diferentes firmas preconfiguradas y/o personalizables a diferentes aplicaciones.
La funcionalidad de WAF deberá contar con actualizaciones automáticas para las firmas preconfiguradas.
La funcionalidad de WAF deberá tener la capacidad para detectar ataques incluyendo Web Server y ataques y vulnerabilidades en la capa de aplicación.
La funcionalidad de WAF deberá tener la capacidad de aprendizaje dinámico, es decir que pueda establecer una línea base y conocer las acciones esperadas hacia las aplicaciones web. Si estas acciones no están contempladas en lo que se espera como “normal” debe alertar y bloquear.
La funcionalidad de WAF deberá aprender la estructura y elementos de la aplicación, esta información deberá estar disponible para la configuración de reglas y / o acciones de bloqueo.
La funcionalidad de WAF no debe modificar las conexiones entre los clientes y el servidor, por lo que se debe asegurar que los mismos paquetes IP origen, IP destino, puerto origen, puerto destino, número de secuencia, #ack y datos de TCP sean idénticos antes y después de ser analizados en el firewall.
La funcionalidad de WAF deberá contar con mecanismos que permitan fácilmente el rollback de una firma o regla de seguridad aplicada.
La funcionalidad de WAF debe tener la capacidad de identificar las amenazas por el país de origen.
La funcionalidad de WAF debe tener la capacidad para detallar y analizar los eventos de seguridad ocurridos, orígenes y método del ataque, dirección IP y localización geográfica del ataque.
La funcionalidad de WAF deberá ser implementada en los ambientes no productivos.

La funcionalidad de WAF deberá contar con protecciones activadas desde el día cero (0) en el que empieza a monitorear y asegurar las aplicaciones web.
La funcionalidad de WAF debe soportar: • Restringir protocolo y versión utilizada • Multi-byte language encoding • Validar URL-encoded characters • Restringir la longitud del método de request • Restringir la longitud del URL solicitado • Restringir el número de Encabezados (headers) • Restringir la longitud del nombre de los encabezados • Restringir la longitud del valor de los encabezados • Restringir la longitud del cuerpo (body) de la solicitud • Restringir la longitud del nombre y el valor de las cookies • Restringir el número de cookies • Restringir la longitud del nombre y valor de los parámetros • Restringir el número de parámetros
La funcionalidad de WAF debe incluir protección a Web Services XML y restringir el acceso a métodos definidos vía Web Services Description Language (WSDL)
La funcionalidad de WAF debe ser Session-aware es decir identificar y forzar que el usuario tenga una sesión e identificar los ataques por usuario
La funcionalidad de WAF debe verificar las firmas de ataque en las respuestas del servidor al usuario
La funcionalidad de WAF debe permitir el enmascaramiento de información sensible filtrada por el servidor
La funcionalidad de WAF debe bloquear basado en la ubicación geográfica e incluir la base de datos de geolocalización.
La funcionalidad de WAF debe proteger contra ataque DoS /DDoS de Capa 7
La funcionalidad de WAF debe soportar tecnología JSON
La funcionalidad de WAF debe proteger como mínimo: • Ataques de Fuerza Bruta • Cross-site scripting (XSS) • Cross Site Request Forgery • SQL injection • Parameter and HPP tampering • Sensitive information leakage • Session highjacking • Buffer overflows • Cookie manipulation • Various encoding attacks • Broken access control • Forceful browsing • Hidden fields manipulation • Request smuggling • XML bombs/DoS Open Redirect
La funcionalidad de WAF debe tener la capacidad para identificar y configurar URLs que generen un gran consumo de recursos en los servidores como método de protección de ataques de denegación de servicios.
La funcionalidad de WAF debe incluir firmas de BOTS para detectar y bloquear tráfico originado por estos.
La funcionalidad de WAF debe soportar un mecanismo ANTIBOT como CAPTCHA o FINGERPRINT para mitigar ataques de denegación hacia las aplicaciones protegidas.
La funcionalidad de WAF debe ofrecer protección sobre tráfico basado en WebSockets

La funcionalidad de WAF debe identificar de manera única a los usuarios por medio de Fingerprint del navegador (Browser Fingerprint) y haciendo tracking del dispositivo.
La funcionalidad de WAF debe incluir una protección para portales de login en donde se ofusque y se encripte los parámetros de usuario y password sin necesidad de uso de agentes en el browser.
La funcionalidad de WAF debe permitir visualizar los registros, alertas de seguridad y eventos del sistema.

b) ITEM 2: <u>Equipos de Protección contra Ataques de Denegación de Servicio Distribuido (DDoS) Centros de Cómputo Principal y Alterno (1 Equipo en cada centro de datos)</u>

Características de equipos contra ataques de Denegación de Servicio Distribuido (DDoS):
El equipo ofertado debe ser una plataforma de hardware de propósito específico denominado "appliance", puede ser de un fabricante distinto al de los equipos de Balanceo de carga – WAF siempre y cuando se incluya todo lo necesario para su operación y gestión; cumpliendo las características descritas en las tablas ITEM 2 e ITEM 3.
El sistema operativo debe ser de propósito específico y no uno de uso genérico, es decir un sistema operativo desarrollado por el fabricante específicamente para protección contra ataques de Denegación de Servicio Distribuido.
El equipo debe soportar una capacidad de al menos 6.954 Mbps de tráfico cifrado.
El equipo debe tener la capacidad de mitigación de ataques de al menos 20 Gbps de Throughput.
El equipo debe contar con un puerto para la administración, tipo Integrated Lights-Out o o módulo de administración o consola central o su equivalente que permita encender, apagar y reiniciar el sistema de manera remota y visualizar el proceso de arranque.
Debe ser implementada en modo inline capa 2 para la toma de decisiones de mitigación. Se debe incluir un mecanismo de bypass para al menos 3 segmentos.
Debe incluir al menos 6 puertos 1/10 GbE SFP+, 6 transceivers SFP+ de 10 Gbps y cables necesarios
Contar con fuentes de poder redundantes AC, entradas de voltaje de 110 a 220 VAC que se puedan remover en caliente (hot-swap).
El equipo deberá ser instalados en rack estándar de 19".
La solución debe incluir funcionalidad de protección contra ataques de DDoS en capas 4-7 utilizando vectores de ataque personalizables.
La solución de protección contra ataques DoS/DDoS debe mitigar ataques DoS y Distributed DoS
Debe bloquear ataques a nivel de red como flood, sweep, teardrop, smurf attacks
Debe detectar y mitigar ataques basados en protocolos, incluyendo SYN, ICMP, ACK, UDP, TCP, IP, DNS, ICMP, ARP
La solución de protección contra ataques DoS/DDoS debe tener una capacidad de detección y mitigación menor a 18 segundos.
La solución de protección contra ataques DoS/DDoS debe permitir la creación de listas blancas (White lists) y de listas negras (black list) de direcciones IPs para excepciones o bloqueos según sea requerido.
La solución de protección contra ataques DoS/DDoS debe soportar mitigar ataques de IPv6.
La solución de protección contra ataques DoS/DDoS, referente a la detección y mitigación de ataques de denegación de servicio debe ser como mínimo mediante éstas 2 técnicas: • **Análisis de comportamiento:** La solución debe comparar el tráfico actual (variable e invariable) contra la línea base de tráfico que la solución aprende a través del tiempo. • **Firmas:** La solución debe contar con firmas predefinidas para mitigar ataques conocidos.

La solución de protección contra ataques DoS/DDoS debe soportar inspección de protocolos tunneling como GRE, IP-in-IP.
La solución de protección contra ataques DoS/DDoS debe brindar protección contra Ataques de Denegación de Servicio para el protocolo DNS.
La solución de protección contra ataques DoS/DDoS debe brindar protección contra Ataques de Denegación de Servicio para el protocolo SIP y poder controlar el tráfico SIP de acuerdo al Método SIP recibido y detectar anomalías a nivel del protocolo
La solución de protección contra ataques DoS/DDoS debe personalizar los Logs, y que la solución soporte integración Syslog.
Debe soportar Port Missuse, evitando que servicios pasando a través de puertos conocidos que buscan saltar protecciones de Firewall (por ejemplo, un servicio SSH escuchando en el puerto 80 y busque abusar de reglas orientadas a HTTP).
La solución debe proteger contra ataques DoS/DDoS (capa 7) basados en HTTP, HTTPS, DNS.
La solución de protección contra ataques DoS/DDoS debe proteger contra ataques TCP-SYN floods, TCP-SYN-ACK floods, TCP-FIN floods, TCP-RESET floods, TCP fragments flood
La solución de protección contra ataques DoS/DDoS debe proteger contra ataques UDP floods, ICMP floods, e IGMP floods
La solución de protección contra ataques DoS/DDoS debe tener protección zero-day attack
La solución de protección contra ataques DoS/DDoS debe tener protección granular Connection-Limit basados en umbrales de tráfico y conexiones.
La solución de protección contra ataques DoS/DDoS debe tener protección Connection PPS Limit
La solución de protección contra ataques DoS/DDoS debe tener protección contra herramientas conocidas de DoS
La solución de protección contra ataques DoS/DDoS debe soportar el descarte de sesiones TCP inactivas.
La solución de protección contra ataques DoS/DDoS debe soportar mitigación de ataques contra tráfico SSL (HTTPS) basado en hardware.
La solución de protección contra ataques DoS/DDoS deberá ser capaz de suspender el tráfico de un atacante por un período específico de tiempo.
La solución de protección contra ataques DoS/DDoS debe incluir un servicio de actualización del fabricante que automáticamente aprovisione al equipo con los mecanismos de defensas más recientes para afrontar ataques y la capacidad de consultar listas de fuentes maliciosas o baja reputación.
La solución de protección contra ataques DoS/DDoS debe permitir que sus parámetros de protección sean cambiados mientras la protección se encuentra en ejecución.
La solución de protección contra ataques DoS/DDoS debe incluir el derecho a la actualización automática de las firmas de seguridad por el tiempo de vigencia de la garantía técnica.
Análisis de Comportamiento:
La solución de protección contra ataques DoS/DDoS debe proporcionar protección DoS/DDoS en tiempo real, basado en análisis de comportamiento o estadístico.
La solución de protección contra ataques DoS/DDoS debe incluir un módulo que tenga en cuenta parámetros de tipo Rate Limit/blocking, connection limiting, source limiting, blacklisting,whilisting, shunning o grey list.
La solución de protección contra ataques DoS/DDoS debe tener protección contra vectores de ataques desconocidos

c) ITEM 3: <u>Consola de gestión de tráfico y administración de dispositivos</u> (1 equipo virtual appliance) (*)

Características generales y de rendimiento
El equipo ofertado debe ser una plataforma de software de propósito específico denominado “Virtual appliance” el cual debe tener funciones de administrador de plataforma y visibilidad de estadísticas

El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente.
La solución proporciona un punto central de control para dispositivos físicos y virtuales y para las soluciones que se ejecutan en ellos
Se debe ofrecer como mínimo un gestor centralizado para la administración y control de la solución, así mismo este debe dar visibilidad del estado de las aplicaciones y del tráfico de las mismas.
La consola debe ser instalada sobre vmware versión 6.5 o superior.
La solución debe permitir el acceso para la administración de los equipos gestionados por una GUI basada en Web seguro (HTTPS)
La solución debe integrarse con Directorio Activo Windows 2008 o superior, para la autenticación de usuarios para gestión de la herramienta.
La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales
El sistema de administración debe ser centralizado integrando gestionando desde allí los ambientes que conforman la solución.
La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado de los ambientes en tiempo real
Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores.
Debe contar con plantillas para la implementación rápida de aplicaciones y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.
Debe poder garantizar el acceso a los servicios gestionados con acceso único para cada usuario en el cual múltiples usuarios puedan acceder al dispositivo con vistas de administrador y gestor totalmente independientes RBAC.
Soporte mejorado para soluciones de seguridad con visibilidad y análisis adicionales en eventos de denegación de servicio
La herramienta de administración centralizada debe gestionar diferentes equipos físicos o virtuales que formen parte de la solución de balanceo, WAF y DDoS provista.
La herramienta debe garantizar la visibilidad de datos de ataques DDoS
La herramienta debe estar en capacidad de administra políticas, licencias, certificados SSL, imágenes y configuraciones para dispositivos.
La consola deberá permitir: Inventario centralizado de equipos y licenciamiento Administración y configuración de los componentes de balanceo de tráfico Administración y configuración centralizada de políticas de Firewall de Aplicaciones Configuración de políticas de DDoS Programación para generar de forma automática backups. Restauración de backups completa o por objetos. Control de acceso granular basado en roles, que permita habilitar el acceso a la administración y generación de aplicaciones. Contar con funcionalidades que permitan el despliegue de nuevas aplicaciones generando las respectivas trazas de auditoria. Delegar la opción de habilitar o deshabilitar los servidores que son balanceados Administración de certificados SSL que se encuentren instalados o configurados en las soluciones Configuración de políticas de actualización de software Planeación de la capacidad mediante la generación de estadísticas de los recursos de los equipos. Generación de vistas de las aplicaciones configuradas en los equipos con todos sus componentes. Generación de plantillas de configuraciones para las capacidades y características de las soluciones.
El dispositivo deber garantizar:

Analítica de aplicaciones donde se pueda ver salud de las aplicaciones retardo y throughput. Seguimiento y control de los cambios en las configuraciones realizados sobre las soluciones. Permitir comparar y validar los cambios ejecutados sobre los archivos de configuraciones. Monitoreo centralizado del tráfico y estadísticas de todas las soluciones (CPU, memoria, número de conexiones.) Generación de logs de auditorías. Visibilidad del licenciamiento. Generación de alertas y envió de estas por correo electrónico y/o SNMP.

(*)- En caso de ofertar los equipos de los ítems 1 y 2 de diferentes fabricantes, se acepta que el ítem 3 sea entregado en dos equipos virtual appliance.

2. SERVICIOS CONEXOS REQUERIDOS

2.1. LUGAR DE ENTREGA

- El equipamiento adquirido deberá ser entregado e instalado de acuerdo a la siguiente distribución:

No.	Ítem	Lugar	Ciudad	Dirección
1	1	Quito – Centro de Cómputo	Quito	Páez 657 y Ramírez Dávalos
		Guayaquil – Centro de Cómputo	Guayaquil	Edif. World Trade Center Av. Francisco de Orellana y Justino Cornejo
2	2	Quito – Centro de Cómputo	Quito	Páez 657 y Ramírez Dávalos
		Guayaquil – Centro de Cómputo	Guayaquil	Edif. World Trade Center Av. Francisco de Orellana y Justino Cornejo
3	3	Quito – Centro de Cómputo	Quito	Páez 657 y Ramírez Dávalos

- El administrador del contrato podrá solicitar el cambio de la dirección de instalación dentro de la misma ciudad durante el período de ejecución del contrato.
- Para la entrega de los equipos se debe coordinar con el administrador del contrato.

2.2. INSTALACIÓN

- El proveedor adjudicado deberá presentar un plan de instalación que incluirá un cronograma de trabajo para la instalación de los componentes de hardware de la solución en un plazo no mayor a 15 días desde la firma del contrato, el mismo que deberá ser aprobado por el Administrador del Contrato designado por el SRI en un plazo no mayor a 10 días.
- El cronograma aprobado no sobrepasará los 60 días posteriores a la firma del contrato, y deberá contener:
    - Listado de actividades
    - Fechas
    - Duración en horas
    - Personal responsable de las actividades
    - Pruebas de inspección y funcionalidad
- El proveedor deberá inspeccionar que los equipos instalados no presenten ningún defecto o alarma en sus componentes de hardware.
- El proveedor deberá realizar pruebas que garantice el correcto funcionamiento de los componentes de hardware en cada equipo instalado.

- El proveedor deberá realizar la instalación de los componentes de hardware de la solución que comprende rackeo, energización de los equipos en los centros de cómputo del SRI especificados en “LUGAR DE ENTREGA”.
- El proveedor adjudicado deberá incluir cables, adaptadores y los accesorios necesarios para la instalación del equipo ofertado.
- Los horarios de instalación serán comunicados por el administrador del contrato mediante correo electrónico u oficio.

2.3. GARANTÍA TÉCNICA DE FÁBRICA

- La solución provista deberá contar con garantía técnica, por 3 años contados a partir de la firma del Acta Entrega Recepción Parcial de bienes e instalación, donde debe constar la marca, modelo, número de serie, características técnicas y ubicación de los bienes y todos los componentes que se encuentran cubiertos por la garantía.
- El proveedor adjudicado debe entregar un documento de garantía técnica emitido por el Fabricante sobre todos los bienes provistos como parte del presente contrato indicando su fecha de expiración validando que cumpla con la vigencia solicitada, en un plazo no mayor a 15 días desde la firma del contrato.
- En caso de falla, o de degradación del desempeño de alguno de los elementos de hardware o alguno de sus componentes (físicos y lógicos), o de observarse comportamientos no esperados durante la operación o capacidad de alguno de los elementos de hardware o alguno de sus componentes, el proveedor deberá proceder con el reemplazo de las partes o las piezas comprometidas, o de los equipos de la solución completos de ser necesario; nuevos y sin costo adicional para el SRI, cumpliendo con el Acuerdo de Nivel de Servicio establecido.
- Durante el periodo de vigencia de la garantía técnica, el proveedor deberá aplicar las nuevas versiones de firmware o software estables, los parches (“hotfix”) de firmware, y los cambios de configuración, que sean recomendados por el fabricante; sin costo adicional para el SRI.
- La garantía técnica debe incluir, pero no debe estar limitado a, las prestaciones que se indican a continuación:
    a) Gestión de incidentes de la solución y todos sus componentes (físicos y lógicos)
    b) Recomendación de versiones de firmware y software para el sistema
    c) Revisión del estado de la solución
    d) Acceso a la Base de Conocimientos del fabricante
    e) Acceso a la Mesa de Ayuda del fabricante
    f) Notificaciones proactivas de nuevas versiones y parches liberados
    g) Mantenimiento correctivo
- Debe estar disponible las 24 horas del día, los 7 días de la semana, durante la vigencia del contrato, cumpliendo con el Acuerdo de Nivel de Servicio establecido.
- Cubre la operación integral de la solución de balanceo geográfico de enlaces de Internet, balanceo de aplicaciones, Firewall de Aplicaciones, Sistema de Prevención de Ataques de Denegación de Servicios Distribuidos y consola de gestión, incluyendo los elementos de hardware, software, cables y conectores tanto en aspectos de la operación como de redes y seguridad informática.
- Se trabajará en base a requerimientos de atención (o casos de soporte), los cuales serán registrados con el proveedor local, para su resolución cumpliendo con el Acuerdo de Nivel de Servicio establecido. Todo el personal de la Coordinación de Seguridad Informática y de la Coordinación de Redes y Comunicaciones de la Dirección Nacional de Tecnología del SRI podrá reportar un problema o solicitar asistencia y tener acceso al seguimiento de los casos.
- El proveedor deberá entregar al Administrador del Contrato, mediante oficio o correo electrónico, en un plazo no mayor a 15 días después de la firma del contrato, el detalle de los canales de comunicación disponibles y el procedimiento para la apertura de casos y el ingreso de requerimientos, siendo obligatorios el medio telefónico, el correo electrónico y un portal de gestión de requerimientos tecnológicos (ITSM).

- En el caso de que los canales de comunicación disponibles o procedimiento de apertura de casos e ingreso de requerimientos cambien, es responsabilidad del proveedor informar de estas actualizaciones al administrador del contrato ya sea por oficio o correo electrónico.
- La atención de los casos deberá ser llevada a cabo en sitio, donde el personal del SRI indique.
- Una vez iniciados los trabajos en sitio, el proveedor deberá garantizar la permanencia de personal técnico necesario durante el tiempo que sea requerido para resolver el incidente y la solución regrese a un estado de operación normal o aceptable para el SRI, o hasta que se haya aplicado una solución temporal, workaround o hasta que se haya logrado un progreso aceptable para el SRI, autorizado por el Administrador del Contrato. Los trabajos se pueden suspender temporalmente si son necesarios recursos adicionales para poder continuar, y se reanudarán cuando éstos estén disponibles, respetando los tiempos de Acuerdo de nivel de Servicio establecidos.
- Al concluir la atención de cada caso de soporte el proveedor local deberá entregar al Administrador del Contrato un informe que deberá incluir al menos la siguiente información:
    - La fecha y hora de apertura del caso;
    - La severidad del caso;
    - El tiempo de respuesta establecido en el Acuerdo de Nivel de Servicio;
    - El tiempo de respuesta que se tuvo en el caso;
    - La novedad reportada por el SRI;
    - La causa raíz identificada;
    - La solución (temporal o definitiva) aplicada;
    - Incidentes previos que estén relacionados;
    - Las conclusiones y recomendaciones.

  El informe definitivo debe ser entregado en un tiempo máximo de 7 días laborables posteriores a la conclusión del caso.
- En los casos que aplique cambio de partes o de piezas o de equipo completo, se acepta la instalación de un equipo o parte o pieza provisional hasta la llegada del definitivo siempre y cuando el provisional sea de iguales o mejores características y capacidad con respecto al original.
- Se aceptará el cierre de un caso de soporte únicamente cuando se haya determinado y se haya aplicado una solución definitiva al evento reportado.
- En los casos de soporte que aplique cambio de partes o de piezas o de equipo completo se aceptará su cierre únicamente cuando se haya instalado la parte o pieza o equipo definitivo, según corresponda.
- Si para el análisis de un caso de soporte se requiere el levantamiento de información mediante la ejecución de algún comando especializado, o la captura de datos, o la obtención de registros de eventos (“logs”), el proveedor es el único responsable de realizar todas las acciones que sean necesarias, para obtener esta información sin perjuicio del cumplimiento del Acuerdo de Nivel de Servicio.
- Si para el análisis de un caso de soporte se requiere abrir un caso de soporte con el fabricante, es responsabilidad del proveedor hacer todas las gestiones necesarias para cubrir los requerimientos de información o de acción solicitados por el fabricante dentro de los tiempos que este último requiera.
- Asistencia desde el diagnóstico del incidente hasta la reparación de éste, pasando por procesos de entrega de la parte en sitio del incidente, ingeniero en sitio para ejecución de actividades de reemplazo físico de la parte, configuraciones necesarias de acuerdo a las partes reemplazadas, ejecución de pruebas para validar la correcta operación de la red luego de los cambios realizados, generación de informes de los incidentes atendidos en formato digital.
- Cuando el SRI lo requiera, el oferente deberá entregar en formato digital un reporte de los registros de casos de soporte realizados en un periodo determinado, el reporte deberá incluir la identificación del requerimiento, tiempos de respuesta, atención y solución para cada problema o casos reportados.
- En el caso que no se presente una solución definitiva para los casos o tampoco se haya identificado la causa raíz del problema, el Administrador del Contrato tiene la potestad de solicitar al proveedor adjudicado un “Plan de acción por garantía técnica” para identificar,

investigar y solucionar el problema. El plazo de entrega del plan de acción es de 10 días calendario.

- El tiempo máximo para la ejecución del plan de acción por garantía técnica, definido desde que el SRI acepta el plan de acción hasta que finalice la ejecución del mismo es de máximo 30 días calendario. Este tiempo se lo podrá extender siempre y cuando el SRI esté de acuerdo a la extensión y exista un documento por parte del SRI autorizando la extensión.
- El SRI tendrá la potestad de aprobar el plazo solicitado en el plan de acción por garantía técnica, en el caso de no llegar a un acuerdo el SRI definirá el plazo basado en la documentación presentada por el proveedor que sustente el plazo.

En partes, mano de obra, en sitio, y reemplazo de partes dañadas o con fallas sin cargo alguno o incluso el equipo completo, hasta obtener la operación del equipo en su totalidad según el Acuerdo de Nivel de Servicio.

2.4. SEVERIDAD

La severidad del caso registrado será establecida entre el SRI y el fabricante y/o proveedor adjudicado, categorizando el problema con niveles de prioridad con el siguiente criterio:

- **Severidad uno**
  - Pérdida de funcionalidad crítica.
  - Degradación del rendimiento del equipo respecto a la línea base recibida en la memoria técnica.
  - Pérdida de conexión del equipo.
  - Alarmas del propio equipo que evidencien una posible falla grave del mismo.

- **Severidad dos**
  - Pérdida parcial del equipo. La conectividad continúa, pero existen en modo restringido solo en ciertas funcionalidades del equipo.

- **Severidad tres**
  - No hay pérdida del equipo, se solicita una actualización o soporte en algún tipo de configuración.

2.5. ACUERDO DE NIVEL DE SERVICIO

El tiempo máximo de respuesta a los casos, definido como el tiempo desde que el SRI reporta un problema hasta que el técnico asignado inicia con la atención presencial, dependerá de la severidad establecida al caso y el nivel de soporte, según la siguiente tabla:

Severidad	Tiempo máximo de respuesta	Tiempo máximo de diagnóstico	Tiempo máximo de cambio de partes o equipo completo
Uno	2 horas	2 horas	8 horas
Dos	4 horas	4 horas	16 horas
Tres	6 horas	12 horas	No aplica

El tiempo máximo de cambio de partes, empieza a contar desde que el fabricante emite el diagnóstico correspondiente, hasta que la parte con problemas sea restaurada o reemplazada por el técnico asignado. Este tiempo se lo podrá extender siempre y cuando exista una justificación aceptada por escrito por el SRI.

El tiempo máximo de cambio de partes o de equipo completo de ser necesario, dependerá de la severidad establecida al caso, según la tabla indicada.

Servicio hasta la conclusión del trabajo

Una vez que el técnico asignado llega a las instalaciones del SRI, este deberá dar servicio hasta que se solucione la falla y el equipo se encuentre en operación, o se haya aplicado una solución temporal, workaround o hasta que se haya logrado un progreso razonable autorizado por el personal del SRI.

El trabajo se puede suspender temporalmente si son necesarios partes o recursos adicionales y se reanudará cuando estos estén disponibles, respetando el tiempo máximo de solución de acuerdo con los tiempos máximos previamente establecidos.

Se deberá entregar el informe de resolución de casos o problemas dentro de 7 días laborables posteriores a la solución del problema

2.6. MIGRACIÓN Y TRANSFERENCIA DE CONOCIMIENTOS

- El proveedor adjudicado será responsable de migrar todos los elementos que forman parte de la solución en los sitios indicados en “LUGAR DE ENTREGA”.
- Los horarios para la migración serán comunicados por el administrador del contrato mediante correo electrónico u oficio.
- El SRI brindará todas las facilidades de acceso y permisos necesarios para la ejecución de los trabajos de implementación y pruebas de funcionamiento en horario laborable o no laborable sin costo adicional, previo a la coordinación con el Administrador del Contrato.
- La migración comprende el alistamiento del software de todos los componentes de la solución que deberá ser ejecutado por el proveedor adjudicado en sitio y serán supervisados por el personal técnico de la institución.
- Se deberá realizar la migración con la finalidad de dejar completamente migrados y operativos todos los equipos que componen la solución ofertada a conformidad del SRI, incluyendo:
    i. Análisis y definición del mejor diseño y arquitectura que se adapte a la topología actual de la infraestructura tecnológica del SRI. Incluye la migración de las soluciones de Balanceo y Seguridad (WAF y DDoS).
    ii. Migración, configuración y afinamiento de todos los elementos de la solución, de acuerdo a lo definido en el diseño y arquitectura.
    iii. Acompañamiento en sitio durante el tiempo que se determine necesario para la estabilización de los elementos de la solución por parte del proveedor adjudicado.

- La migración de la solución de Balanceo, Seguridad de aplicaciones WAF y DDoS debe ser ejecutada en sitio por parte del fabricante, con acompañamiento en sitio por parte del proveedor local.
- El equipo de trabajo que participará en la migración deberá disponer de todas las herramientas y el material de trabajo que se requieran necesarios (laptop, conectores, patch cords, etiquetadora.) para desempeñar adecuadamente sus actividades en el SRI.
- Todos los gastos incurridos que requiera la migración (traslados, viáticos, hospedaje) están a cargo del proveedor, el SRI no incurrirá en ningún gasto adicional.

- El proveedor adjudicado deberá entregar la siguiente documentación como parte de la migración:
  a) Plan de migración de la solución que deberá ser entregado en un plazo no mayor a 15 días desde la firma del contrato, el mismo que deberá ser aprobado por el Administrador del Contrato designado por el SRI en un plazo no mayor a 10 días; y, que contendrá al menos:
     i) Cronograma de trabajo para las actividades de migración, número de horas que invertirán los técnicos asignados para la migración y número de horas del personal del SRI para la participación de los trabajos, responsables de cada actividad. Indicar el tiempo de afectación (down time) a los servicios del SRI.
     ii) Diseño detallado propuesto (LLD, por sus siglas en inglés). El diseño debe ser certificado por el fabricante.
     iii) Arquitectura detallada y debe ser avalada por el fabricante.
     iv) Personal asignado para la prestación de los servicios conexos.
     v) Estrategia para evitar impactos de disponibilidad,
     vi) Diagramas
     vii) Configuraciones

     La duración del plan debe ser de máximo 60 días calendario a partir de la firma del Acta Entrega Recepción Parcial de bienes e instalación.

  b) Memoria técnica de migración que deberá ser entregada en un plazo de 10 días posterior a la entrega del servicio conexo de migración en medio digital e impreso; y, contendrá al menos:
     i) Esquemático de conexión física final.
     ii) Proceso de implementación.
     iii) Configuración de la solución.
     iv) Inventario y descripción detallada de los elementos de la solución.
     v) Umbrales saludables de operación (ej. CPU, RAM) referenciales.
     vi) Pruebas de funcionamiento, conectividad y detección de errores en las interfaces.
     vii) Mecanismos de respaldo y de restauración de configuración.
     viii) Mecanismos de recuperación y de cambio de contraseñas de gestión.
     ix) Mecanismo de depuración de registros de eventos (logs).
     x) Métodos básicos de detección y resolución de problemas (Base de Conocimientos Básica).

- El proveedor adjudicado deberá incluir todo el software, conectores, cables, adaptadores y los accesorios necesarios para la migración.
- El proveedor adjudicado deberá incluir los manuales de Uso y Operación (físicos o digitales) de los elementos de la solución en español o inglés con al menos las instrucciones de manejo para el adecuado funcionamiento de la solución.
- Se deben establecer al menos dos reuniones con el Líder del Proyecto para revisar: el diseño, arquitectura, diagramas, configuraciones, y plan de migración.
- Para la migración de los equipos de los Data Centers de Quito y Guayaquil, el proveedor deberá realizar el levantamiento de información, de acuerdo a:
  Visitas coordinadas a los Centros de Cómputo de Quito y Guayaquil.
  Verificación física de equipos, cables, conexiones.
  Verificación lógica de instalación, software, configuraciones, seguridades.
  El proveedor, luego de la inspección y levantamiento de la información, deberá entregar al administrador del contrato el plan de migración.

- Debido a que el equipamiento a ser incorporado en la arquitectura de red del SRI es de alta tecnología y complejidad, se requiere contar con la transferencia de conocimientos sobre la infraestructura instalada de al menos 40 horas para 10 funcionarios del SRI.
- Para la transferencia de conocimientos se debe considerar que el proveedor adjudicado debe presentar al administrador del contrato el plan de transferencia de conocimiento en un plazo de 10 días calendario posterior a firma del Acta Entrega Recepción Parcial de bienes e instalación.

- El administrador del contrato deberá aprobar el plan presentado en un máximo de 10 días calendario a partir de la entrega por parte del proveedor adjudicado, en el caso de generarse alguna observación o cambio el proveedor tendrá hasta 5 días calendario para entregar del plan definitivo.
- El temario deberá basarse en cursos oficiales del fabricante, personalizados sobre administración, gestión y troubleshooting de la solución provista, de al menos 40 horas para 10 funcionarios del SRI.
- Se deberá realizar en un horario y lugar a convenir y validado por el SRI, el lugar estará a cargo del oferente.
- La logística de la transferencia de conocimiento será responsabilidad del proveedor adjudicado.
- El oferente deberá proveer de todo el material y facilidades necesarias para la realización de la transferencia de conocimientos."
- El servicio de transferencia podrá ser brindado de manera virtual en laboratorios provistos y preparados por el proveedor o fabricante.

2.7. MANTENIMIENTO PREVENTIVO

- El período de vigencia del mantenimiento preventivo de la solución y todos sus componentes debe ser de 3 años contados a partir de la suscripción del Acta Entrega Recepción Parcial de bienes e instalación.
- Mantenimiento preventivo será periódico anual y cubrirá a la solución y todos sus componentes asociados.
- Se debe garantizar el rendimiento de los elementos de la solución, incluyendo de ser necesario la mano de obra, atención en sitio en horario 24x7 y adición de nuevas partes o incluso cambio completo de los elementos de hardware o software sin cargo alguno, hasta obtener el rendimiento del equipo de acuerdo a la capacidad de desempeño solicitada.
- El cronograma de mantenimientos preventivos a realizarse será notificado al proveedor mediante oficio por el administrador del contrato, ya sea por oficio o correo electrónico, con al menos 10 días de anticipación, las fechas y horarios definitivos del cronograma para cada mantenimiento, teniendo en cuenta lo siguiente:
    - La ventana de mantenimiento general para los equipos del data center principal de Quito es normalmente en el segundo semestre del año.
    - La ventana de mantenimiento general del data center alterno de Guayaquil es normalmente en el primer semestre del año.
- El primer mantenimiento preventivo será ejecutado al menos nueve meses posteriores a la firma del Acta Entrega Recepción Parcial de bienes e instalación.
- Las visitas se harán en horario laboral o fuera de horario laboral, según como disponga el administrador del contrato.
- El servicio de mantenimiento preventivo consistirá en la revisión física y lógica de los elementos de que son parte de la solución, así como la aplicación de las rectificaciones o mejoras que sean necesarias.
- El proveedor deberá presentar el plan de mantenimiento preventivo anual dentro del primer mes del periodo del servicio para aprobación del administrador del contrato. Este plan deberá ser presentado anualmente durante la vigencia del contrato.
- El plan de mantenimiento preventivo anual debe incluir el tiempo estimado de mantenimiento y/o indisponibilidad de los equipos.
- Upgrade de Firmware, incluirá el derecho a actualizaciones y parches de firmware para el correcto funcionamiento del hardware, acompañamiento y/o asesoría en instalaciones o actualizaciones de software (si aplica)
- Entrega de un informe de mantenimiento preventivo anual en medio digital en el que se incluya las actividades del mantenimiento preventivo, y recomendaciones para cada equipo (si aplica)

- El SRI durante la vigencia del contrato de mantenimiento podrá solicitar bajo demanda cambios sobre la arquitectura implementada, diseño, funcionamiento y configuración de la infraestructura implementada, sin costo adicional para el SRI.
- En caso de que la aplicación de algún parche o actualización de hardware o software, o la modificación de algún parámetro de configuración de hardware o software, llevada a cabo por el proveedor, genere la falla, o error, o degradación, o comportamiento no esperado de la solución o alguno de sus componentes, el proveedor deberá aplicar la remediación correspondiente; sin costo adicional para el SRI, cumpliendo con el Acuerdo de Nivel de Servicio establecido.
- Al concluir cada visita y sus actividades, en un tiempo máximo de 10 días calendario posteriores, el proveedor deberá entregar al Administrador del Contrato un informe definitivo que deberá incluir al menos la siguiente información:
    - La fecha y hora de la visita;
    - Los resultados de las actividades de revisión y de diagnóstico llevadas a cabo en la visita;
    - El listado de parches de hardware y software instalados, de ser el caso;
    - El listado de actualizaciones de hardware y software instaladas, de ser el caso;
    - Los cambios de configuración y de políticas de seguridad aplicados, de ser el caso;
    - Los hallazgos relevantes, en caso de haberlos;
    - Las conclusiones del estado del sistema;
    - Las recomendaciones de mejora en configuración, o de incremento de capacidad o mejora de diseño, en caso de ser necesario;

  En los casos que las actividades de remediación tomen más de dos semanas, se deberá adjuntar un plan de actividades.
- El proveedor deberá realizar la revisión, monitoreo y afinamiento de la solución cuando el personal del SRI reporte la existencia de incidentes o de problemas de seguridad informática asociados al sistema en sí o a servicios tecnológicos que dependan del mismo.
- Cada vez que sea requerido por el SRI el proveedor deberá dar soporte para la modificación de la arquitectura, la modificación del diseño, la modificación de la topología, o el afinamiento de la operación del sistema, así como la documentación asociada; sin costo adicional para el SRI, cumpliendo con el Acuerdo de Nivel de Servicio establecido.
- Cada vez que sea requerido por el SRI el proveedor deberá elaborar y entregar la documentación correspondiente a los cambios tecnológicos que se planeen llevar a cabo en la solución, en el formato establecido en el procedimiento de gestión de cambios tecnológicos del SRI.

3. PLAZO DE EJECUCIÓN

El plazo de ejecución de este contrato será de 3 años y 60 días (1.155 días) a partir de la suscripción del contrato desglosado de la siguiente manera:

- El plazo de entrega del Sistema de Balanceo de Carga con funcionalidad de Seguridad (incluye instalación), será de máximo 60 días a partir de la firma del contrato.
- El plazo para la migración y transferencia de conocimientos del sistema de Balanceo de carga incluye funcionalidad de Seguridad (DDoS y WAF) es de 60 días calendario contados a partir de la firma del Acta Entrega Recepción Parcial de bienes e instalación.
- El plazo de vigencia de los servicios de mantenimiento preventivo y garantía técnica será de 3 años (1.095 días) contados a partir de la fecha de firma del Acta Entrega Recepción Parcial de bienes e instalación.

4. FORMA DE PAGO Y CONDICIONES DE PAGO

El Servicio de Rentas Internas pagará al proveedor, de la siguiente manera:

Bienes -Instalación/Garantía Técnica:

- Contra entrega: Cien por ciento (100%) del precio de los bienes y la Instalación/Garantía Técnica, a partir de la entrega total de los equipos instalados en las oficinas del SRI, con la planilla de pago y la suscripción del Acta Entrega Recepción Parcial de bienes e instalación.

Servicio de Migración y transferencia de conocimiento:

- El pago del valor total por la migración y transferencia de conocimientos de la solución ofertada de Balanceo de Carga incluidas las funcionalidades de Seguridad (DDoS y WAF) se realizará con la presentación de la planilla de pago y la suscripción del Acta Entrega Recepción Parcial de Migración y Transferencia de Conocimientos.

Mantenimiento preventivo:

- El servicio de mantenimiento preventivo se pagará en tres partes iguales, a la entrega a satisfacción del servicio correspondiente dentro de cada año. Para estos pagos se requerirá la presentación de la solicitud o planilla de pago y la suscripción del Acta de Entrega Recepción de este servicio del período correspondiente.

5. AJUSTE DE PRECIOS

Los precios de las ofertas deberán ser fijos, considerando que la entrega de los principales componentes de los costos del contrato, se completan en un periodo menor de 18 meses; de conformidad al numeral 2.24 de la Política para la Adquisición de bienes y obras financiadas por el BID (GN-2349-9).

6. PENALIDADES O MULTAS

- Se aplicará al proveedor adjudicado una penalidad del 0,15% del monto correspondiente a las obligaciones pendientes de ejecutar, por cada día de retraso en la entrega de los bienes e instalación.

- Se aplicará al proveedor adjudicado una penalidad del 0,10% del monto correspondiente a las obligaciones pendientes de ejecutar, por cada día de retraso en la entrega de:
    - Plan de instalación de la solución ofertada.
    - Garantía Técnica emitido por el fabricante.
    - Canales de comunicación para apertura de casos.
    - Plan de acción por garantía técnica.
    - Plan de migración y plan de transferencia de conocimiento.
    - Memoria técnica de migración de la solución y transferencia de conocimiento.
    - Certificado de trabajo de al menos un especialista del fabricante que acompañará en sitio al proyecto.
    - Certificación de participación en al menos 2 proyectos de instalación e implementación de la arquitectura propuesta ofertada, para el especialista asignado.
    - Certificación técnica de nivel profesional o avanzado en la marca ofertada del

especialista asignado.

- **Garantía técnica:** Por cada hora o fracción que el proveedor se exceda del tiempo establecido en el Acuerdo de Nivel de Servicios se aplicarán las siguientes penalidades sobre el monto correspondiente a las obligaciones pendientes:
    - 0,70% para casos de severidad 1,
    - 0,40% para casos de severidad 2, y
    - 0,20% para casos de severidad 3.

- **Mantenimiento preventivo:** Por cada hora o fracción que el proveedor se exceda del tiempo establecido en el Acuerdo de Nivel de Servicios se aplicarán las siguientes penalidades sobre el monto correspondiente a las obligaciones pendientes:
    - 0,70% para casos de severidad 1,
    - 0,40% para casos de severidad 2, y
    - 0,20% para casos de severidad 3.

- En el caso de no realizarse las visitas de mantenimiento preventivo de acuerdo al cronograma notificado por el administrador del contrato, se aplicará una penalidad del 0,50% del monto de las obligaciones pendientes por cada día de retraso.

- En caso de no presentar el plan de mantenimiento preventivo anual, dentro del primer mes del periodo del servicio se aplicará una penalidad del 0,50% del monto de las obligaciones pendientes por cada mes de retraso.

- **Informes de Casos de Soporte y Mantenimiento**: En el caso de no entregarse los informes de los casos de soporte de garantía técnica o mantenimiento preventivo dentro de los plazos establecidos, se aplicará una penalidad correspondiente al 0,50% del monto de las obligaciones pendientes por cada día de retraso.

La Contratista autoriza expresamente al Servicio de Rentas Internas, para que descuente el valor correspondiente a las multas de la planilla que presente para el pago.

Si el valor de las multas impuestas llegare a superar el 5% del precio del contrato, el Servicio de Rentas Internas podrá darlo por terminado de manera anticipada y unilateral, declarando al Contratista como incumplido.

No habrá lugar a la imposición de las multas, cuando se comprobare fuerza mayor, caso fortuito o hechos imputables al Servicio de Rentas Internas. En tales casos, dentro de un término de cinco (5) días, contado a partir del hecho producido, la Contratista comunicará la causa por la que ha incumplido sus obligaciones, y el Servicio de Rentas Internas a su vez, tendrá un término de cinco (5) días, contado a partir de la recepción de la comunicación, para aceptar o no los argumentos alegados.

7. LUGAR DE ENTREGA

Ver lugar de entrega e instalación

8. OTROS PARÁMETROS REQUERIDOS

El oferente debe presentar la siguiente documentación:

Otros Documentos

No.	Descripción	Cantidad	Observaciones
1	Autorización del fabricante (actualizado al año en curso) de ser distribuidores autorizados por parte del fabricante de la marca ofertada.	1	La autorización debe ser emitida por el fabricante de los equipos
2	Certificado del fabricante indicando que todos los componentes involucrados en la oferta son nuevos de fábrica, sin uso, sin componentes reconstruidos y su garantía técnica cubre a todos sus componentes.	1	El certificado debe ser emitido por el fabricante de los equipos
3	Documentación técnica, catálogos y manuales provistos por el fabricante, que permitan verificar las características requeridas, indicando nombre del manual y número de página correspondiente. Con el fin de validar el cumplimiento de las especificaciones solicitadas.	1	Documento emitido por el fabricante

9. REQUISITOS PARA CALIFICACION POSTERIOR

CAPACIDAD LEGAL

El Oferente no deberá constar como inhabilitado para contratar con el Estado Ecuatoriano en el Sistema Oficial de Contratación del Estado (SOCE). Esta verificación contempla la inhabilitación por causas que se enmarquen en las determinadas en la Sección VI Fraude y Corrupción y Prácticas Prohibidas, numeral 1.1, literal (a) de estos documentos de licitación. Esto será verificado directamente por el Comprador.

CAPACIDAD FINANCIERA

El Oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos financieros:

Índice de Solvencia: (total de activos / total de pasivos) = 1.00

Patrimonio: mayor o igual a ciento ochenta mil dólares de los Estados Unidos de América con 00/100, (USD 180.000,00).

Las **reglas para la determinación** de los requisitos financieros serán las siguientes:

- **i.** Para el índice de solvencia, se obtendrá respecto al último ejercicio fiscal anterior a la fecha de presentación de las ofertas.
- **ii.** Para el patrimonio se tomará el valor de la evidencia documentada del último ejercicio fiscal.
- **iii.** Para oferentes en Asociación en participación, consorcio o asociación (APCA): Cada uno de los miembros del APCA deberán cumplir con los índices señalados.

La **evidencia documentada** que se requiere para acreditar el cumplimiento de estos requisitos es:

i. Copia simple de los estados financieros, declaraciones, o documentación equivalente en el país de origen, presentados a autoridad competente, o auditados independientemente. La documentación deberá venir denominada en dólares de los Estados Unidos de América. De estar denominados en otra moneda, incluirán la conversión a dólares de los Estados Unidos de América utilizando la tasa transaccional para la venta

del tipo de cambio publicada en la página del Banco Central del Ecuador https://www.bce.fin.ec/index.php/component/k2/item/260-consulta-por-monedas-extranjeras, a la fecha del último día del ejercicio fiscal correspondiente.

Si por la normativa del país de origen, los estados financieros, declaraciones o documentación equivalente no son exigibles a la fecha de presentación de ofertas, el oferente indicará esta situación y podrá presentar los estados financieros, declaraciones o documentación equivalente del ejercicio fiscal inmediato anterior.

EXPERIENCIA Y CAPACIDAD TÉCNICA

EXPERIENCIA GENERAL

No.	Descripción	Cantidad	Observaciones
1	Originales o copias de Certificados o actas de entrega recepción emitidos por clientes que acrediten al oferente experiencia en instalación o implementación o mantenimiento de soluciones tecnológicas que incluyan al menos una de las siguientes funcionalidades: Balanceadores de Carga, Waf y anti DDos a las requeridas en el alcance del proceso usando la marca propuesta.	Hasta 5	Certificados de experiencia emitidos dentro de los 5 últimos años. La sumatoria de los presupuestos de los contratos debe alcanzar un monto equivalente o superior a $850.000,00 sin incluir impuestos. Hasta 5 contratos.

PERSONAL TÉCNICO

1. El equipo de trabajo del proveedor, que se encargará de la instalación, migración y transferencia de conocimientos y mantenimiento, estará compuesto por el siguiente equipo:

Cant	Rol / Función	Nivel de estudios	Titulación académica	Descripción de la Experiencia	Certificación Técnica
1	Líder del Proyecto	Título Universitario	Ingeniería Comercial, Licenciatura o ingeniería en Sistemas, Electrónica, Telecomunicaciones o afines	Mínimo 2 certificados emitidos por empresas públicas o privadas donde se hayan instalado o implementado soluciones tecnológicas de redes o seguridad informática para validar la experiencia en Administración de Proyectos en los últimos cinco (5) años.	PMP o PRINCE2 vigente emitido por el instituto certificador correspondiente
1	Técnico de Instalación, Migración y Transferencia	Título Universitario	Licenciatura o ingeniería en Sistemas, Electrónica,	Mínimo participación en 2 proyectos de instalación o implementación de la	Certificación Técnica vigente nivel profesional o avanzado

	de Conocimientos		Telecomunicaciones o afines	marca ofertada. Certificados emitidos por el proveedor o clientes.	emitida por el fabricante de la marca ofertada
1	Técnico de Mantenimiento	Título Universitario	Licenciatura o Tecnología o Ingeniería Sistemas, Electrónica, Telecomunicaciones o afines	Mínimo participación en 2 proyectos que incluyan servicios de mantenimiento de la marca ofertada. Certificados emitidos por el proveedor o clientes.	Certificación Técnica vigente nivel profesional o avanzado emitida por el fabricante de la marca ofertada

2. Se puede aceptar que el mismo recurso que realiza la instalación realice el trabajo de migración, transferencia de conocimientos y mantenimiento siempre y cuando no interfiera con las actividades y plazos a cumplir.

3. Si en el transcurso del periodo de implementación, alguna de las personas es reemplazada, deberá ser por otra con perfil similar o superior al solicitado. El Administrador del Contrato aprobará el cumplimiento del perfil requerido.

4. El oferente adjudicado, deberá contar con el acompañamiento de un especialista del fabricante durante el diseño y migración de los bienes, por lo cual máximo en 15 días posteriores a la suscripción del contrato deberá entregar la siguiente documentación emitida por el fabricante:

    4.1. Certificado de trabajo de al menos un especialista del fabricante que acompañará en sitio al proyecto.

    4.2. Certificación de participación en al menos 2 proyectos de instalación e implementación de la arquitectura propuesta ofertada, para el especialista asignado.

    4.3. Certificación técnica de nivel profesional o avanzado en la marca ofertada del especialista asignado.