CONVOCATORIA PARA LA ELABORACIÓN DEL ESTUDIO DE MERCADO

El Servicio de Rentas Internas (SRI) a través de la Dirección Nacional de Tecnología, se encuentra en la fase de elaboración del Estudio de Mercado para la "ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL PARA EL SERVICIO DE RENTAS INTERNAS (SRI)"

Este estudio de mercado será utilizado de manera referencial previo a la publicación del proceso de adquisición.

El precio referencial de la oferta deberá considerar los siguientes aspectos:

- Las especificaciones técnicas detalladas
- La vigencia de la cotización no debe ser menor a 154 días
- La fuente de financiamiento será realizada con recursos del Banco Interamericano de Desarrollo, por lo que los oferentes deberán pertenecer a los países miembros del BID
- El plazo total del contrato es de 1185 días calendario contados a partir del siguiente día de la notificación del administrador del contrato de la disponibilidad del anticipo en la cuenta del contratista

Las cotizaciones deben ser remitidas en formato digital (firmadas), al correo institucional **renovaciontecnologica@sri.gob.ec** hasta el día 29 de junio de 2026 16:00 pm, con los siguientes datos:

Datos del oferente:

Razón Social:
RUC / ID:
Dirección:
Teléfono:
Fecha de emisión de la cotización:
Vigencia de la cotización: (no debe ser menor a 154 días)
Firma de responsabilidad.

Datos del contratante:

A nombre de: Servicio de Rentas Internas
RUC: 1760013210001

Formato Presentación Cotización:

Propuesta Económica:

DESGLOSE DE COMPONENTES					
Item	**Tipo de recurso**	**Descripción**	**Cantidad**	**Precio unitario (USD)**	**Precio Total (USD)**
1	Hardware	**Sistema de Protección de Aplicaciones Web (WAF)** Tres (3) appliances WAF: ○ Dos (2) appliances en el Centro de Datos Principal – Quito. ○ Un (1) appliance en el Centro de Datos Alterno (Guayaquil – CNT, modalidad housing).	3	$	$
2	Hardware	**Sistema de Mitigación de Ataques DDoS** Tres (3) appliances dedicados para mitigación de ataques DDoS: ○ Dos (2) appliances en el Centro de Datos Principal – Quito. ○ Un (1) appliance en el Centro de Datos Alterno (Guayaquil – CNT, modalidad housing).	3	$	$
3	Hardware	**Plataforma de Gestión Centralizada** Una (1) equipo para la consola de administración centralizada: ○ Una (1) consola principal en Quito.	1	$	$
4	Software	**Licenciamiento / Suscripción** ○ Licenciamiento/suscripción por tres (3) años equivalentes a 1.095 días calendario, para todos los componentes DDoS y WAF. ○ Derecho a recibir actualizaciones, parches, mejoras y nuevas versiones del software liberadas por el fabricante durante la vigencia del contrato, así como componentes de seguridad adicionales de protección.	1	$	$
5	Servicios	**Implementación y transferencia de conocimientos** Servicios profesionales necesarios para dejar la solución completamente operativa, lo cual incluye: ○ Servicio de configuración inicial de los sistemas DDoS y WAF. ○ Elaboración, revisión y aprobación de la arquitectura de la solución (HLD/LLD) y del plan de implementación (incluyendo contingencia y reverso), previo a la puesta en producción. ○ Integración con la infraestructura tecnológica existente del SRI.	1	$	$

		○ Migración de configuraciones, políticas y reglas desde los sistemas actuales, cuando aplique. ○ Pruebas de funcionamiento, alta disponibilidad y seguridad. ○ Puesta en producción conforme a un cronograma aprobado por el SRI. ○ Transferencia de conocimientos para al menos nueve (9) funcionarios del SRI, cubriendo aspectos operativos, administrativos y de respuesta ante incidentes.			
6	Servicios	Soporte local, mantenimiento preventivo, correctivo y asistencia que incluye: ○ Servicio de soporte local por 1.005 días calendario, en modalidad 24x7. ○ El soporte deberá cubrir todos los componentes de hardware y software de la solución. ○ Mantenimiento preventivo, mantenimiento correctivo y asistencia técnica especializada.	1	$	$
				Subtotal	**$ 0,00**
				I.V.A (15 %)	**$ 0,00**
				Total general de la oferta	**$ 0,00**

Nota: Los oferentes deberán garantizar el entendimiento y el cumplimiento de todas las especificaciones técnicas y servicios conexos requeridos

Listado de países elegibles

Lista de países miembros cuando el financiamiento provenga del Banco Interamericano de Desarrollo: Alemania, Argentina, Austria, Bahamas, Barbados, Bélgica, Belice, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Croacia, Dinamarca, Ecuador, El Salvador, Eslovenia, España, Estados Unidos, Finlandia, Francia, Guatemala, Guyana, Haití, Honduras, Israel, Italia, Jamaica, Japón, México, Nicaragua, Noruega, Países Bajos, Panamá, Paraguay, Perú, Portugal, Reino Unido, República de Corea, República Dominicana, República Popular de China, Suecia, Suiza, Surinam, Trinidad y Tobago, Uruguay, y Venezuela.

Territorios elegibles

Guadalupe, Guyana Francesa, Martinica, Reunión – por ser Departamentos de Francia.
Islas Vírgenes Estadounidenses, Puerto Rico, Guam – por ser Territorios de los Estados Unidos de América.
Aruba – por ser País Constituyente del Reino de los Países Bajos; y Bonaire, Curazao, Sint Maarten, Sint Eustatius – por ser Departamentos de Reino de los Países Bajos.

Hong Kong – por ser Región Especial Administrativa de la República Popular de China

ESPECIFICACIONES TÉCNICAS
ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL

1. ALCANCE

El presente proceso de contratación comprende la provisión integral de una solución de seguridad perimetral para el Servicio de Rentas Internas (SRI). La solución estará orientada a la mitigación de ataques de Denegación de Servicio Distribuido (DDoS) y a la protección de aplicaciones web (WAF), con despliegue en el Centro de Datos Principal de Quito y en el Centro de Datos Alterno de Guayaquil.

3.1 COMPONENTES DE HARDWARE

Sistema de Protección de Aplicaciones Web (WAF)

Tres (3) appliances WAF:

- Dos (2) appliances en el Centro de Datos Principal – Quito.
- Un (1) appliance en el Centro de Datos Alterno (Guayaquil – CNT, modalidad housing).

Sistema de Mitigación de Ataques DDoS

Tres (3) appliances dedicados para mitigación de ataques DDoS:

- Dos (2) appliances en el Centro de Datos Principal – Quito.
- Un (1) appliance en el Centro de Datos Alterno (Guayaquil – CNT, modalidad housing).

Plataforma de Gestión Centralizada

Una (1) equipo para la consola de administración centralizada:

- Una (1) consola principal en Quito.

3.2 LICENCIAMIENTO Y SOPORTE DE FÁBRICA

Incluye el licenciamiento completo de todas las funcionalidades de seguridad requeridas incluyendo:

Licenciamiento / Suscripción

- Licenciamiento/suscripción por tres (3) años equivalentes a 1.095 días calendario, para todos los componentes DDoS y WAF.
- Derecho a recibir actualizaciones, parches, mejoras y nuevas versiones del software liberadas por el fabricante durante la vigencia del contrato, así como componentes de seguridad adicionales de protección.

Soporte de Fábrica

- Servicio de soporte del fabricante 24x7 durante 1.095 días, que incluya:
  Atención de incidentes.
  Acceso a la base de conocimientos.
  Reemplazo de hardware defectuoso conforme a SLA.
  Posibilidad de apertura directa de casos por parte del personal del SRI.

3.3 IMPLEMENTACIÓN Y TRANSFERENCIA DE CONOCIMIENTOS

El contratista deberá brindar los servicios profesionales necesarios para dejar la solución completamente operativa, lo cual incluye:

- Servicio de configuración inicial de los sistemas DDoS y WAF.
- Elaboración, revisión y aprobación de la arquitectura de la solución (HLD/LLD) y del plan de implementación (incluyendo contingencia y reverso), previo a la puesta en producción.

- Integración con la infraestructura tecnológica existente del SRI.
- Migración de configuraciones, políticas y reglas desde los sistemas actuales, cuando aplique.
- Pruebas de funcionamiento, alta disponibilidad y seguridad.
- Puesta en producción conforme a un cronograma aprobado por el SRI.
- Transferencia de conocimientos para al menos nueve (9) funcionarios del SRI, cubriendo aspectos operativos, administrativos y de respuesta ante incidentes.

3.4 SOPORTE LOCAL Y MANTENIMIENTO

Contempla la prestación de servicios de soporte local especializado, incluyendo:

- Servicio de soporte local por 1.005 días calendario, en modalidad 24x7.
- El soporte deberá cubrir todos los componentes de hardware y software de la solución.
- Mantenimiento preventivo, mantenimiento correctivo y asistencia técnica especializada.

2. INFRAESTRUCTURA ACTUAL

A continuación, se detalla la infraestructura tecnológica del SRI relevante para la integración del sistema objeto de contratación. Esta información ha sido levantada a la fecha del presente documento y puede variar en función de la operación y las necesidades institucionales.

La información sobre la infraestructura actual se presenta únicamente con fines referenciales y de contexto técnico, en ningún caso constituye un requerimiento de continuidad tecnológica, ni condiciona la selección de la solución ofertada.

4.1 EQUIPOS DE SEGURIDAD ACTUALES

La siguiente tabla resume el estado de los equipos que conforman la arquitectura actual de seguridad perimetral del SRI (DDoS, WAF):

	Descripción equipo	**Ubicación**	**Función**	**Estado actual**
1	DDOS Hybrid Defender - BIG IP I5800	Centro de datos GYE, **ambiente alterno**, DMZ internet	Equipo para mitigación de ataques de Denegación de Servicio Distribuido (DDoS)	Regular, con soporte y garantía de fábrica hasta 26 de diciembre del 2026
2	DDOS Hybrid Defender - BIG IP I5800	Centro de datos UIO, **ambiente productivo**, DMZ internet	Equipo para mitigación de ataques de Denegación de Servicio Distribuido (DDoS)	Regular, con soporte y garantía de fábrica hasta 26 de diciembre del 2026
3	F5 ASM BIG-IP 15.1.7 Build (i7800) 0.0.6 , integrado en 2 LTM	Centro de datos UIO, **ambiente productivo**, DMZ externa	Módulo integrado de seguridad para aplicaciones. Web Application Firewall (WAF)	Regular, con soporte hasta 26 de diciembre del 2026, este módulo WAF forma parte del equipo balanceador de carga.
4	F5 ASM BIG-IP 15.1.7 Build (i7800) 0.0.6 , integrado en 2 LTM	Centro de datos UIO, **ambiente alterno**, DMZ externa	Módulo integrado de seguridad para aplicaciones. Web Application Firewall (WAF)	Regular, con soporte hasta 26 de diciembre del 2026, este módulo WAF forma parte del equipo balanceador de carga.

5	Trend Micro IPS Tipping Point 8200TX	Centro de datos UIO, **ambiente productivo**, DMZ internet	Equipo para detectar y bloquear ataques dirigidos y malware. Sistema de Prevención de Intrusiones (IPS)	Soporte y garantía vencidos el 27 de diciembre del 2024

Tabla 1. Detalle de equipo que conforman el sistema de seguridad perimetral del SRI.

4.2 CONECTIVIDAD Y PUNTOS DE PROTECCIÓN

El SRI cuenta con dos centros de datos; CD Principal en Quito y CD Alterno en Guayaquil este último en instalaciones de CNT bajo modalidad de housing. Estos centros de datos están interconectados mediante enlaces redundantes. Los servicios institucionales expuestos a Internet incluyen portales de declaración tributaria, consulta de obligaciones, facturación electrónica y servicios de interoperabilidad con entidades del Estado.

El SRI cuenta con tomas eléctricas con las siguientes especificaciones para la alimentación de los equipos de seguridad actuales:

COMPONENTE	SITIO	SOCKET	VOLTAJE
DDoS	CD Alterno GYE	IEC-320 C13/14	110 V-AC
DDoS	CD Principal UIO	IEC-320 C13/14	110 V-AC
WAF	CD Alterno GYE	IEC-320 C13/14	110 V-AC
WAF	CD Principal UIO	IEC-320 C13/14	110 V-AC

El SRI cuenta con bastidores (“racks”) con las siguientes dimensiones para el montaje de los equipos:

COMPONENTE	SITIO	ANCHO	PROFUNDIDAD
DDoS	CD Alterno GYE	19”	22”
DDoS	CD Principal UIO	19”	22”
WAF	CD Alterno GYE	19”	22”
WAF	CD Principal UIO	19”	22”

3. METODOLOGÍA DE TRABAJO

5.1 CONDICIONES GENERALES

- Los horarios de trabajo se acordarán con el administrador del contrato, sin incluir costos adicionales por trabajar en fines de semana, feriados, o fuera del horario laboral.
- Todas las actividades que impliquen cambios en la configuración, en la operación, o en el nivel de seguridad informática de los sistemas o componentes instalados o desplegados deberán ser informados al administrador del contrato, y deberán ser aplicados de manera controlada en coordinación con el personal del SRI.
- El personal técnico del contratista deberá contar con todos los medios y recursos necesarios para la ejecución ágil y oportuna de todos los trabajos que son parte del objeto del presente contrato; incluyendo, pero no limitado a:

equipo portátil, módem de acceso a Internet, medios removibles de almacenamiento (ej. USB Flash Drives, USB External Hard Drives, etc.), cables de conexión a puertos de consola, "patch cords", etc.

- Si de acuerdo con los procedimientos institucionales alguna actividad del contrato (por su impacto) requiere ser gestionada mediante cambio tecnológico, el contratista deberá entregar un documento que detalle las actividades técnicas de su parte o del fabricante para la ejecución del cambio, las actividades de contingencia y las de reverso, por cada componente involucrado.
- Toda la información contenida en el apartado de Infraestructura actual ha sido levantada a la fecha del presente documento y puede variar en función de la operación y las necesidades institucionales.
- Es responsabilidad del contratista realizar las validaciones correspondientes oportunamente. Para el presente proceso, el **Centro de Datos Alterno se encuentra en Guayaquil corresponde a las instalaciones de CNT bajo modalidad de housing**; por lo tanto, el contratista deberá tomar en consideración cualquier requisito particular de CNT; por ejemplo: requisitos de ingreso, cableado, montaje de equipos y etiquetado.

5.2 COMPONENTES DE HARDWARE

Esta etapa comprende el suministro, ingreso, montaje, instalación física, interconexión, actualización, activación y verificación operativa de todos los componentes de hardware de la solución, incluyendo los appliances Anti-DDoS, los appliances WAF y la plataforma de gestión centralizada, de conformidad con las especificaciones técnicas, las recomendaciones del fabricante y las condiciones operativas del SRI.

Los appliances principales operarán en el Centro de Datos Principal del SRI, ubicado en Quito, y los appliances alternos operarán en el Centro de Datos Alterno, ubicado en Guayaquil (CNT, modalidad housing), conforme a la distribución definida para la solución.

Todos los gastos asociados al suministro, transporte, ingreso, montaje, instalación, interconexión y puesta en operación del hardware estarán a cargo del contratista. Los oficios, entregables y el acta de entrega-recepción correspondientes a esta etapa se detallan al final de la presente sección.

La activación del componente de licenciamiento deberá ejecutarse como parte de la instalación del hardware, en concordancia con lo establecido en el numeral 5.3 LICENCIAMIENTO Y SOPORTE DE FÁBRICA, ajustándose a los mismos plazos y constituyendo parte de las condiciones para la entrega-recepción de esta etapa.

- El servicio de instalación debe cubrir todos los componentes de hardware: appliances Anti-DDoS y WAF (centro de datos principal y alterno) y plataforma de gestión centralizada (centro de datos principal).
- El contratista debe proveer e instalar todos los rieles, sujetadores y accesorios necesarios para un montaje seguro en los racks de 19 pulgadas del Centro de Datos Principal (Quito) y del Centro de Datos Alterno (Guayaquil), según corresponda.
- El contratista deberá proveer todos los elementos necesarios para la interconexión de los appliances DDoS y WAF con la infraestructura de red del SRI, incluyendo interfaces, transceptores, cableado y demás componentes requeridos, garantizando la compatibilidad técnica y la correcta operación de los enlaces.
- El contratista debe proveer los cables patch cord de fibra óptica OM4 LC-LC para conexiones de 10 GbE/25 GbE y OM3 LC-LC para conexiones de 1 GbE. Los cables deben ser certificados.
- El contratista debe realizar la actualización de firmware y sistema operativo de los equipos a las últimas versiones liberadas por el fabricante previo a la puesta en producción.

Garantía técnica del hardware

- La garantía técnica del fabricante debe cubrir todos los equipos que conforman el componente de hardware del objeto de contrato: appliances Anti-DDoS, appliances WAF y plataforma de gestión centralizada.

- La garantía técnica debe incluir el servicio de reemplazo de partes, piezas e inclusive del componente completo en caso de fallo de hardware por defecto de fabricación.
- Todos los equipos deben ser nuevos y no deben entrar en EOST (End-of-Support) ni EOL (End-of-Life) durante los 5 años posteriores a la fecha de suscripción del contrato.
- Si se evidencia que los appliances Anti-DDoS y/o appliances WAF experimentan un consumo de capacidad de cómputo (CPU o RAM) superior al 90% mientras procesan un volumen de tráfico ("throughput") inferior al 90% de lo establecido en la Capacidad efectiva DDoS tráfico limpio (throughput) y Capacidad de mitigación WAF (throughput L7) HTTP/S respectivamente, se determinará que los equipos en cuestión no cumplen con este requerimiento y deberán ser fortalecidos o reemplazados por el Contratista. Esta acción se aplicará tantas veces como corresponda hasta que se evidencie que los equipos estén operando dentro de los parámetros esperados por el SRI, sin que esto represente un costo adicional para el SRI.
- Los casos en los que se requiera aplicar la garantía técnica serán gestionados como incidentes del servicio de mantenimiento correctivo y deberá cumplir el contratista con el ACUERDO DE NIVEL DE SERVICIO.
- El servicio de soporte del fabricante del hardware debe estar disponible 24 horas al día los 7 días de la semana durante la vigencia del contrato y debe cubrir tanto el hardware como las licencias de firmware incluidas en los equipos.
- En los casos en los que se requiera hacer un remplazo completo de alguno de los equipos cubiertos por la garantía, el contratista podrá entregar un equipo temporal, con las mismas o mayores características técnicas y las mismas o mayores funcionalidades, con un licenciamiento de firmware y software equivalente o superior, durante el tiempo de espera por el equipo definitivo, en función del ACUERDO DE NIVEL DE SERVICIO.
- Los equipos temporales deberán contar con etiquetas que los identifiquen como propiedad del contratista y deberá presentarse la documentación que así lo sustente para autorizar su salida.
- Los equipos que requieran reemplazo completo y los equipos temporales deberán pasar por la sanitización de sus medios de almacenamiento antes de su salida de los centros de datos institucionales y deberá presentarse la documentación que así lo sustente para autorizar su salida.
- El servicio de soporte de fábrica debe ser de tipo directo, permitiendo al personal del SRI abrir casos de soporte directamente con el fabricante.

El contratista deberá entregar los siguientes oficios para esta etapa:

- **Oficio de ingreso de equipos**, que incluya como mínimo: fecha de ingreso, detalle de equipos por sitio (fabricante, modelo, número de serie), características técnicas, rol de cada componente dentro de la solución, ubicación prevista y evidencias de ingreso, desembalaje y montaje inicial.
- **Oficio de culminación de la instalación del hardware**, que incluya como mínimo: evidencia del cumplimiento de las especificaciones técnicas, detalle de la instalación ejecutada por sitio, evidencia de actualización de firmware y sistema operativo, evidencia de activación y vigencia del licenciamiento y soporte de fábrica, y evidencia de operación del hardware en la red del SRI.

Una vez cumplido lo establecido en esta etapa, y previa validación a satisfacción del SRI, se suscribirá el **Acta de entrega-recepción del hardware y licenciamiento**, la cual deberá estar respaldada por la siguiente documentación:

- Certificado de garantía técnica del hardware emitido por el fabricante o su representante autorizado, que incluya la vigencia, alcance de cobertura, modalidad de reemplazo y tipo de soporte de fábrica de todos los equipos instalados.
- oficio de ingreso de equipos y del oficio de culminación de la instalación del hardware, debidamente suscritos.
- Inventario técnico final de los equipos instalados, que incluya por cada componente fabricante, modelo, número de serie, ubicación física, rol dentro de la solución, interfaces habilitadas y versión de firmware o sistema operativo instalada.
- Documento o certificado de activación del licenciamiento y del soporte de fábrica de todos los componentes instalados, que evidencie la habilitación de las funcionalidades contratadas, la vigencia correspondiente y el acceso del SRI a los mecanismos de soporte directo del fabricante.

- Detalle de cobertura de garantía por equipo, que incluya fabricante, modelo, número de serie, fecha de inicio y fin de garantía, cobertura aplicable, modalidad de reemplazo y canal de escalamiento o atención.
- Certificación del fabricante o de su representante autorizado que acredite que los equipos entregados son nuevos y que los modelos ofertados no se encuentran en estado EOST (End-of-Support) ni EOL (End-of-Life), ni entrarán en tales estados durante los cinco (5) años posteriores a la suscripción del contrato.

5.3 LICENCIAMIENTO Y SOPORTE DE FÁBRICA

- El contratista debe realizar la habilitación del licenciamiento y del soporte de fábrica asociado a los equipos DDoS, WAF y consola de administración, conforme a la vigencia establecida en el alcance.
- La contratista deberá realizar la entrega del licenciamiento y soporte de fábrica para todos los componentes de acuerdo a lo definido en el alcance.
- La vigencia del licenciamiento y soporte de fábrica debe cubrir el mismo periodo de vigencia de los componentes hardware.
- El contratista deberá realizar la verificación del acceso a funcionalidades completas de seguridad, incluida la verificación de la activación y operación de los servicios de inteligencia, reputación, protección de APIs y Bots
- La vigencia del licenciamiento de todos los elementos del componente de software será de 1.095 días calendario contados a partir de la culminación de la instalación del hardware.
- El licenciamiento debe incluir la actualización continua de firmas Anti-DDoS y WAF desde las redes de inteligencia de amenazas propias del fabricante, sin costo adicional durante la vigencia del contrato.
- El servicio de soporte de fábrica del software debe estar disponible 24x7 y debe cubrir la gestión de incidentes de software, recomendación de versiones, revisión de estado y acceso a la base de conocimientos del fabricante.
- El servicio de soporte de fábrica debe ser de tipo directo, permitiendo al personal del SRI abrir casos de soporte directamente con el fabricante.

Nota: La instalación del componente de licenciamiento debe realizarse como parte de la instalación del hardware, ajustándose a los mismos plazos e incluyéndose como parte de las condiciones para su entrega-recepción.

5.4 IMPLEMENTACIÓN Y TRANSFERENICA DE CONOCIMEINTOS

- Toda actividad de implementación deberá ejecutarse de forma coordinada con el personal del SRI, en las ventanas de mantenimiento acordadas, minimizando el impacto a los servicios institucionales.
- Es responsabilidad del contratista y del fabricante generar evidencias de toda actividad realizada, de manera que se pueda demostrar el cumplimiento de la implementación.
- La transferencia de conocimiento se realizará de forma presencial en instalaciones provistas por el contratista o fabricante.
- El calendario y horario se acordará con el administrador del contrato en función de la disponibilidad del personal del SRI.
- Toda la logística asociada (aulas, equipos, acceso a internet, materiales, laboratorios) corre por cuenta del contratista.
- La transferencia deberá impartirse en al menos dos grupos, en función de la disponibilidad del personal institucional.
- Al finalizar la implementación, el contratista deberá entregar la documentación técnica de respaldo conforme a los entregables definidos para la recepción del servicio.

El contratista deberá entregar los siguientes oficios para esta etapa:

- **Oficio de culminación de la implementación**, que incluya: arquitectura de seguridad final (HLD/LLD) aprobada, memoria técnica completa de implementación para ambos centros de datos, evidencias de migración de configuraciones y políticas, e informe de pruebas, funiconales , alta disponibilidad y seguridad, evidencia de acceso a funcionalidades completas de seguridad, incluyendo verificación de activación de servicios de inteligencia, reputación, protección de APIs y Bots.

- **Informe de transferencia de conocimiento**, que incluya: material de capacitación en formato digital, registro de asistencia de los participantes, contenido temático impartido, evidencias de ejecución de las sesiones, y certificaciones profesionales del fabricante para los participantes.

Una vez cumplido con lo establecido en este ámbito a satisfacción del SRI, se suscribirá el **Acta de entrega-recepción de implementación y transferencia de conocimientos**, que incluirá la siguiente documentación:

- Arquitectura de seguridad final aprobada (HLD/LLD) para ambos centros de datos;
- Memoria técnica completa de la implementación e integración;
- Evidencias de migración de configuraciones, políticas y reglas;
- Informe de pruebas funcionales, de alta disponibilidad y de seguridad;
- Estándares de configuración y guías de operación;
- Reportes operativos habilitados y validados por el SRI.
- Material de capacitación en formato digital (presentaciones, guías, manuales y documentación técnica);
- Registro de asistencia de los participantes (acta de asistencia con lista de asistentes, temario, fechas de sesiones y duración);
- Contenido temático impartido durante la transferencia de conocimiento;
- Evidencias de ejecución de las sesiones (actas, grabaciones o reportes);
- Certificaciones profesionales del fabricante obtenidas por los participantes.

5.5 SOPORTE LOCAL Y MANTENIMIENTO

- El servicio de soporte local estará disponible 24 horas al día, 7 días a la semana durante toda la vigencia del contrato.
- Las actividades de atención podrán realizarse remota o presencialmente según lo requiera el SRI, sin costo adicional por atención fuera de horario laboral.
- Toda intervención sobre los componentes de la solución durante el período de soporte deberá ser coordinada previamente con el administrador del contrato y ejecutada en las ventanas de mantenimiento acordadas.
- El contratista deberá mantener actualizado el registro de casos atendidos y ponerlo a disposición del SRI cuando sea requerido.

El contratista deberá entregar los siguientes oficios para esta etapa:

- **Reporte mensual de casos de soporte**, que incluya: número de casos atendidos por prioridad, tiempos de respuesta vs. SLA, causas raíz identificadas y acciones ejecutadas.
- **Informe de mantenimiento preventivo** (por cada visita anual por centro de datos), que incluya: diagnóstico por alarmas y revisión física, reporte de actualización de firmware (versión anterior vs. actual), conclusiones y acciones correctivas recomendadas.
- **Notificación de vulnerabilidades críticas**: el contratista notificará al SRI en un plazo máximo de 48 horas desde su publicación oficial cualquier vulnerabilidad crítica (CVSS ≥ 9.0) que afecte los componentes de la solución.
- **Reporte consolidado anual de soporte**, que incluya: detalle de todos los casos del período, análisis de tendencias, recomendaciones de mejora y estado general de la solución.

Una vez cumplido con lo establecido en este ámbito a satisfacción del SRI, se suscribirá el **Acta de entrega-recepción del Soporte Local Y Mantenimiento,** que incluirá la siguiente documentación:

Entregables periódicos:

- **Reporte mensual de soporte**, que incluya: casos atendidos, tiempos de respuesta y resolución vs. SLA, causas raíz identificadas y acciones ejecutadas.
- **Reporte consolidado anual de soporte**, al final de cada período anual, que incluya:
    - Detalle de todos los casos atendidos durante el período;
    - Análisis de tendencias e incidencias recurrentes;
    - Cumplimiento de SLA durante el período;
    - Recomendaciones de mejora y optimización de la solución;
    - Registro de actualizaciones, parches y cambios aplicados.

Entregables para recepción de cada período anual:

Al final de cada período anual de soporte, previa presentación del reporte consolidado anual y a satisfacción del SRI, se suscribirá el **Acta de conformidad anual del servicio de soporte local**, que habilitará el pago correspondiente al período. Para el último período, esta acta constituirá el **Acta de entrega-recepción definitiva del servicio de soporte local**.

4. BIENES REQUERIDOS

6.1 ARQUITECTURA GENERAL DE LA SOLUCIÓN

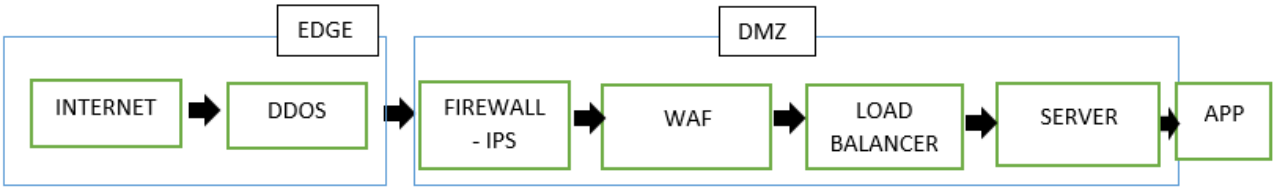
Toda la solución de seguridad perimetral solicitada deberá ser de un mismo fabricante y operar bajo una arquitectura on-premises, desplegada en el Centro de Datos Principal (Quito) y en el Centro de Datos Alterno (Guayaquil, instalaciones de CNT bajo modalidad de housing).

El Centro de Datos Alterno opera con un esquema de protección unitaria (un appliance DDoS y un appliance WAF), sin configuración de Alta Disponibilidad local, en concordancia con su rol de respaldo. La continuidad operativa ante falla de hardware en el sitio alterno se gestiona mediante el SLA de reemplazo Next Business Day (NBD) establecido en la Sección 8.

En cuanto a la distribución de los componentes en los dos centros de datos del SRI, la solución se implementará en un esquema multisitio que contempla:

1.1. Tres (3) appliances WAF, con dos (2) unidades instaladas en el Centro de Datos Principal en Quito y una (1) unidad en el Centro de Datos Alterno (Guayaquil – CNT, modalidad housing).
1.2. Tres (3) appliances dedicados para mitigación de ataques DDoS, con dos (2) unidades en Quito y una (1) unidad en el Centro de Datos Alterno (Guayaquil – CNT, modalidad housing).
1.3. Una (1) consola de administración centralizada para el Centro de Datos Principal en Quito.

La siguiente figura muestra a alto nivel la arquitectura de la solución



6.2 COMPONENTES DE HARDWARE

6.2.1 APPLIANCE DE PROTECCIÓN DDoS

Requerimientos generales
1.Solución Appliance El equipo ofertado deberá ser un dispositivo de hardware dedicado (appliance), diseñado y fabricado específicamente para funciones de seguridad y/o protección contra ataques de denegación de servicio distribuidos (DDoS). No se aceptarán soluciones basadas en software instalado sobre servidores de propósito general, ni hardware de cómputo genérico con funcionalidad habilitada mediante software de terceros. La solución deberá ofrecer el hardware y el software como una solución integrada del mismo fabricante.
2. Capacidad efectiva DDoS tráfico limpio (throughput) El sistema deberá mitigar ataques DDoS volumétricos y de capa de aplicación, con todas las funciones de protección habilitadas soportando como mínimo **9.70 Gbps** de tráfico legítimo bajo mitigación activa.
3. Capacidad de mitigación DDoS El sistema deberá demostrar capacidad efectiva de mitigación frente a ataques DDoS de alta tasa de paquetes, que incluyan ataques volumétricos, protocolarios y multivector, con los mecanismos de mitigación activos y sin degradación significativa del tráfico legítimo.
4. Conexiones concurrentes El sistema deberá soportar un mínimo de **3'881.779 conexiones concurrentes**, manteniendo estabilidad operativa y capacidad de inspección y mitigación incluso bajo condiciones de ataque.
5. Patrones de comportamiento La solución Anti-DDoS deberá ser capaz de detectar y mitigar ataques dirigidos contra tráfico HTTPS sin requerir obligatoriamente el descifrado del contenido.
6. Mecanismos de identificación La solución deberá aplicar mecanismos dinámicos de identificación y limitación del tráfico malicioso durante eventos de ataque, ajustándose de forma automática a las condiciones del tráfico y evitando la fuga de tráfico o la afectación del tráfico legítimo.
7. Arquitectura del sistema DDoS La solución deberá integrarse en la arquitectura de red de la institución operando en línea (inline) como parte del flujo productivo del tráfico y deberá contar con alternativas de despliegue que permitan aprendizaje, detección y mitigación de ataques sin impacto en la topología existente o requerir modificaciones estructurales de la red.
8. Interfaces de red (por equipo) Mínimo 4 interfaces de 10 GbE SFP para tráfico + 1 interface de 1 GbE para gestión. Para los equipos que funcionan en alta disponibilidad se deben incluir las interfaces adicionales que recomiende el fabricante para este modo de operación
9. Fuentes de alimentación Doble fuente redundante hot-swap con rango de entrada 100-240 VAC.
10. Factor de forma Rack-mounted (1U o 2U), compatible con racks de 19 pulgadas.
11. Vigencia tecnológica Modelo fabricado desde el año 2026 en adelante, sin EOST (End of Support) ni EOL (End of Life) durante los 5 años posteriores a la suscripción del contrato.
12. Detección automática de ataques El sistema deberá detectar ataques DDoS mediante análisis conductual continuo y aprendizaje automático, sin dependencia exclusiva de umbrales estáticos manuales.
13. Perfilamiento dinámico de tráfico El sistema deberá establecer y mantener perfiles dinámicos de tráfico legítimo por dirección IP, servicio, protocolo y aplicación, ajustándose a variaciones normales de carga.
14. Mitigación en tiempo real

El sistema deberá detectar y comenzar la mitigación de ataques DDoS en tiempo real, activando contramedidas adaptativas de forma automática e inmediata tras la identificación del comportamiento anómalo, mediante análisis conductual, generación de firmas dinámicas y análisis heurístico, sin requerir intervención manual.
15. Análisis conductual El sistema deberá detectar ataques de Denegación de Servicio Distribuido mediante análisis conductual continuo y aprendizaje automático, sin dependencia exclusiva de umbrales estáticos definidos manualmente.
16. Medidas adaptativas La mitigación deberá ejecutarse en tiempo real mediante medidas adaptativas basadas en comportamiento, análisis heurístico y reglas dinámicas, sin requerir intervención manual.
17. Continuidad del tráfico legítimo Durante procesos de mitigación, el sistema deberá identificar, priorizar y preservar el tráfico legítimo, evitando bloqueos indiscriminados o degradación del servicio.
18. Inspección profunda de paquetes El sistema deberá realizar inspección profunda de paquetes sin degradación, incluso durante ataques de alta tasa de paquetes por segundo.
19. Operación autónoma El sistema deberá operar de forma autónoma durante eventos de ataque, sin requerir intervención manual obligatoria.
20. Aprendizaje continuo El sistema deberá realizar aprendizaje automático antes, durante y después de los ataques, ajustando los perfiles de comportamiento sin interrupción del servicio.
21. Alta disponibilidad El sistema de protección DDoS deberá configurarse en Alta Disponibilidad para el Centro de Datos de Quito.
22. Visibilidad de ataques El sistema deberá proporcionar visibilidad detallada y en tiempo real de los ataques DDoS, incluyendo como mínimo el tipo de ataque, los vectores y protocolos involucrados, la intensidad y evolución temporal del ataque, la diferenciación entre tráfico legítimo y malicioso, así como las acciones de mitigación aplicadas, permitiendo el análisis operativo y forense de eventos de seguridad.
23. Registro de eventos El sistema deberá registrar de forma detallada y persistente los eventos y métricas asociados a ataques DDoS, incluyendo como mínimo eventos de detección, activación de mecanismos de mitigación, métricas de tráfico (paquetes por segundo, ancho de banda, conexiones), clasificación de tráfico legítimo y malicioso, así como acciones automáticas ejecutadas, permitiendo su uso para auditoría, análisis forense y revisión post-incidente.
Ataques volumétricos
24. Mitigación de UDP Flood El sistema deberá detectar y mitigar ataques volumétricos basados en UDP Flood mediante análisis conductual y control adaptativo de tráfico.
25. Mitigación de ICMP Flood El sistema deberá detectar y mitigar ataques ICMP Flood sin afectar el tráfico legítimo de control de red.
26. Mitigación de ataques de amplificación El sistema deberá mitigar ataques de amplificación, incluyendo DNS Amplification y NTP Amplification.
27. Mitigación de ataques de reflexión El sistema deberá detectar y mitigar ataques de reflexión, incluyendo aquellos basados en SSDP (Simple Service Discovery Protocol).
Ataques protocolarios
28. Mitigación de TCP SYN Flood El sistema deberá detectar y mitigar ataques TCP SYN Flood.
29. Mitigación de TCP ACK Flood

El sistema deberá mitigar ataques TCP ACK Flood orientados a agotar recursos de sesión.
30. Mitigación de TCP RST Flood
El sistema deberá mitigar ataques TCP RST Flood diseñados para interrumpir conexiones legítimas.
31. Mitigación de agotamiento de conexiones
El sistema deberá detectar y mitigar ataques orientados al agotamiento de tablas de conexión.
Ataques de capa aplicación
32. Mitigación de HTTP GET Flood
El sistema deberá mitigar ataques HTTP GET Flood mediante análisis de comportamiento.
33. Mitigación de HTTP POST Flood
El sistema deberá mitigar ataques HTTP POST Flood diseñados para agotar recursos de backend.
34. Mitigación de ataques HTTPS Flood
El sistema deberá mitigar ataques HTTPS Flood sin necesidad obligatoria de descifrado SSL/TLS.
35. Mitigación de agotamiento a nivel aplicación
El sistema deberá detectar ataques diseñados para agotar recursos de aplicación.
Ataques lentos y evasivos
36. Mitigación de Slow POST
El sistema deberá mitigar ataques Slow POST.
37. Mitigación de micro-floods
El sistema deberá mitigar micro-floods de bajo volumen.
38. Mitigación de ataques burst
El sistema deberá detectar y mitigar ataques tipo burst.
39. Mitigación de evasión de umbrales
El sistema deberá detectar evasión de umbrales estáticos.
40. Mitigación de ataques de fragmentación
El sistema deberá detectar y mitigar ataques de fragmentación.
41. Mitigación de carpet bombing
El sistema deberá mitigar ataques de tipo carpet bombing.

6.2.2 SISTEMA DE PROTECCIÓN DE APLICACIONES WEB (WAF)

Requerimiento general
1. Solución Appliance El equipo ofertado deberá ser un dispositivo de hardware dedicado (appliance), diseñado y fabricado específicamente para funciones de seguridad y/o seguridad de aplicaciones web (WAF). No se aceptarán soluciones basadas en software instalado sobre servidores de propósito general, ni hardware de cómputo genérico con funcionalidad habilitada mediante software de terceros. La solución deberá ofrecer el hardware y el software como una solución integrada del mismo fabricante.
2. Capacidad de mitigación WAF (throughput L7) HTTP/S El sistema WAF deberá soportar un throughput efectivo de **6.11 Gbps** de tráfico HTTP/S, con todas las funciones de inspección, detección y mitigación habilitadas, incluyendo protección OWASP Top 10, APIs y Bots, para un mínimo de 8 sitios web de producción. Los valores de capacidad deben corresponder a condiciones reales de operación en capa 7. Es decir, no son valores tomados en condiciones específicas de tráfico como, por ejemplo, tamaños de paquetes controlados, tráfico de forwarding o correspondientes a funcionalidades de balanceo de carga sin inspección detallada de capa de aplicación. En caso de que el throughput efectivo en capa 7 (L7) con todas las funcionalidades de seguridad habilitadas no se encuentre en documentación pública, podrá sustentarse mediante documentación oficial del fabricante (reporte de laboratorio), que certifique y garantice el cumplimiento bajo condiciones reales de inspección.

Este mecanismo aplicará exclusivamente para este requerimiento y no será válido para otros requisitos técnicos.
3. Conexiones concurrentes HTTP/S El sistema WAF deberá soportar un mínimo de **132.918 conexiones concurrentes** a nivel de capa de aplicación, manteniendo inspección stateful y operación en línea, sin degradación del servicio de las aplicaciones protegidas, incluso bajo condiciones de carga sostenida y con las funciones de seguridad habilitadas.
4. Transacciones por segundo (TPS HTTP/S) El sistema WAF deberá soportar un mínimo de **35.018 transacciones** HTTP/S por segundo, considerando tráfico legítimo sostenido, picos de carga y escenarios de ataque a la capa de aplicación.
5. Inspección SSL/TLS El sistema WAF deberá soportar inspección SSL/TLS en línea para tráfico HTTP/S, con capacidad suficiente para procesar el tráfico cifrado de las aplicaciones protegidas, manteniendo habilitadas las funciones de inspección, detección y mitigación de amenazas propias de la solución, sin degradación del servicio ni afectación a la disponibilidad de las aplicaciones.
6. Interfaces de red Mínimo 4 interfaces 25 GbE SFP para datos y 1 GbE BASE-T para gestión. Para los equipos que funcionan en alta disponibilidad se deben incluir las interfaces adicionales que recomiende el fabricante para este modo de operación
7. Fuentes de alimentación Doble fuente redundante hot-swap con rango de entrada 100-240 VAC.
8. Factor de forma Rack mounted (1U o 2U), compatible con racks de 19 pulgadas.
Arquitectura y operación del WAF
9. Arquitectura del sistema WAF La solución WAF deberá integrarse a la arquitectura de red institucional operando en línea, en tiempo real y bajo un esquema on premises, como parte del flujo productivo del tráfico protegido. Todas las aplicaciones deberán ser protegidas y soportadas por el equipo físico instalado en la infraestructura del SRI (al menos 8 aplicaciones de producción). Se permite el uso complementario de servicios del fabricante exclusivamente para funciones avanzadas de análisis, inteligencia, perfilamiento o clasificación relacionadas con la protección de APIs y Bots, siempre que dichos servicios no impliquen desvío, redireccionamiento (proxy reverso), encaminamiento ni terminación del tráfico productivo fuera de la infraestructura institucional.
10. Inspección L7 Realizar inspección profunda de tráfico HTTP y HTTPS en capas L7
11. Capacidades equivalentes El sistema de Firewall de Aplicaciones Web (WAF) deberá cumplir íntegramente con todas las especificaciones funcionales, de rendimiento, detección y mitigación definidas en el presente documento, independientemente de si se implementa como appliance dedicado o como módulo de seguridad integrado en una plataforma de procesamiento y entrega de aplicaciones, sin reducción de capacidades.
12. Impacto en latencia El sistema de Firewall de Aplicaciones Web (WAF) deberá operar en línea (inline) y en tiempo real, permitiendo la medición y visualización desde su consola de administración de métricas de desempeño tales como tiempo de respuesta de las aplicaciones, transacciones por segundo (TPS), throughput HTTP/HTTPS y utilización de recursos del sistema, con el fin de verificar que la habilitación de las funciones de seguridad no genera degradación significativa del servicio ni afecta la operación normal de las aplicaciones protegidas, aun con todas las políticas de seguridad activas.
13. Modo de operación Soporte de operación en modo detección, bloqueo y modo híbrido, permitiendo transición controlada entre modos sin interrupciones del servicio.
14. Aprendizaje automático Incorporar mecanismos de aprendizaje automático supervisado y no supervisado para establecer perfiles normales de tráfico por aplicación y API.
15. Modelos de seguridad

Soportar modelos de seguridad positivos y negativos, combinados con análisis de comportamiento para reducir falsos positivos.
16. Protección multiaplicación Permitir la protección simultánea de múltiples aplicaciones web y APIs (Application Programming Interface), con políticas independientes por aplicación.
17. Operación continua Mantener capacidades de inspección y protección bajo carga sostenida de tráfico legítimo, sin degradación del servicio.
18. Alta disponibilidad El sistema WAF deberá configurarse en Alta Disponibilidad para el Centro de Datos Principal (Quito).
19. Registro y trazabilidad Generar registros detallados de eventos de seguridad, acciones aplicadas y cambios de configuración, para fines de auditoría y análisis forense.
Protección de aplicaciones web (OWASP Top 10)
20. Protección OWASP Top 10 Detectar y mitigar todos los ataques contemplados en el OWASP Top 10 mediante inspección profunda de solicitudes HTTP/S.
Protección de APIs
21. Protección OWASP API Top 10 Proteger APIs conforme al OWASP API Security Top 10 mediante validación estructural y análisis conductual.
22. Descubrimiento automático de APIs La solución deberá contar con capacidades de descubrimiento y visibilidad de APIs, permitiendo identificar endpoints, métodos, atributos relevantes de las solicitudes y respuestas, así como facilitar el inventario de APIs conocidas, observadas y no documentadas para un mínimo de 5 aplicaciones con las funcionalidades de API Discovery.
23. Validación de esquemas Validar que las solicitudes y respuestas de APIs cumplan con esquemas definidos o aprendidos dinámicamente.
24. Protección por endpoint Permitir aplicar políticas diferenciadas por API, endpoint y método HTTP.
25. Protección contra abuso de APIs Detectar y mitigar abusos de APIs, incluyendo uso excesivo, manipulación de parámetros y secuencias anómalas.
26. Análisis de lógica de negocio Identificar patrones anómalos de uso de APIs que indiquen abuso de lógica de negocio.
27. Risk Score La solución deberá proporcionar capacidades de análisis y priorización de riesgos sobre APIs, apoyándose en los hallazgos de descubrimiento, exposición, uso, sensibilidad de datos y comportamiento observado, con el fin de facilitar la gestión de riesgos y la aplicación de controles de mitigación.
Protección contra automatización y Bots
28. Detección de Bots La solución deberá detectar y clasificar tráfico automatizado mediante mecanismos de análisis de comportamiento, telemetría, reputación, firmas, huella de cliente u otras técnicas equivalentes, diferenciando entre tráfico humano, bots legítimos y bots maliciosos.
29. Clasificación de tráfico La solución deberá clasificar el tráfico en: tráfico generado por humanos, Bots legítimos y Bots maliciosos, al igual que debe existir la capacidad de identificar si un Bot legitimo realiza demasiadas solicitudes, permitiendo configurar umbrales.
30. Acciones de mitigación Permitir configurar acciones como página de bloqueo, captcha o permitir acceso.
31. Permitir / Denegar La solución deberá permitir agregar usuarios a una lista de usuarios confiables, así como bloqueo de usuarios no deseados.
32. Telemetría de usuarios La plataforma deberá utilizar recolección de telemetría de usuarios, para la detección de automatización
33.Tráfico automatizado

La solución deberá permitir aplicar acciones de mitigación frente a tráfico automatizado malicioso o abusivo, incluyendo mecanismos configurables de desafío, limitación, bloqueo o tratamiento diferenciado, sin requerir cambios manuales sobre las aplicaciones protegidas y deberá utilizar un modelo de ML/IA para la detección de automatización.

34. Lista de orígenes confiables

La solución deberá permitir agregar orígenes a una lista de usuarios confiables, así como bloqueo de orígenes no deseados.

35. Bots maliciosos

La solución debe detectar al menos los siguientes tipos de bots maliciosos:

a. Bots de Tipo Scripts.
b. Bots avanzados que utilicen headless browsers.
c. Bots que utilicen Browser completo y que emulen comportamiento humano.
d. Bots avanzados que emulen comportamiento humano y que modifiquen aleatoriamente su dirección y IP y/o identificador de dispositivo.

36. Mecanismos de detección

La solución de mitigación de BOTs, debe contar con al menos los siguientes mecanismos de detección y mitigación:

- Inteligencia de bots maliciosos compartida entre usuarios del servicio.
- Reputación de IP para seguimiento de tráfico que provenga de proxys y redes TOR
- Machine Learning semi-supervisado para identificar patrones de bots emergentes.
- Análisis de comportamiento de los usuarios para detección de anomalías.
- Test de turing reversos y dinámicos para descubrir la identidad del bot.
- Creación del fingerprinting único por cada conexión.

Inteligencia de Amenazas

37. Detalle de inteligencia de amenazas

La solución debe contar con un servicio de inteligencia reputacional local que permita a los administradores de la solución visualizar el nivel de riesgo de una dirección IP consultada.

Inspección SSL/TLS y rendimiento

38. Inspección SSL/TLS

Soportar descifrado SSL/TLS para inspección de seguridad según políticas definidas.

39. Inspección concurrente

Soportar inspección simultánea de múltiples aplicaciones cifradas manteniendo estabilidad bajo carga.

40. Continuidad operativa

Mantener la disponibilidad de las aplicaciones protegidas durante procesos de inspección profunda.

Operación y visibilidad

41. Visibilidad en tiempo real

Proporcionar visibilidad en tiempo real de ataques, eventos y acciones de mitigación.

42. Análisis forense

Permitir análisis detallado de solicitudes HTTP/S y eventos asociados a ataques.

43. Reportes de seguridad

Generar reportes de seguridad personalizables para operación y auditoría.

6.2.3 PLATAFORMA DE GESTIÓN CENTRALIZADA

Requerimientos generales de la plataforma de gestión

1. Plataforma de gestión centralizada

La solución deberá contar con una plataforma de gestión centralizada implementada íntegramente en sitio (on-premises), que unifique la administración de todos los componentes de seguridad perimetral, Anti-DDoS y WAF, así como

las capacidades de protección, análisis, correlación de eventos, protección de APIs, protección contra Bots e inteligencia de amenazas, sin dependencia de portales o consolas fuera de la infraestructura del SRI.
2. Modalidad de implementación de la plataforma La plataforma de gestión centralizada podrá implementarse como appliance físico dedicado o como máquina virtual. En caso de que la consola de administración sea provista en modalidad virtual, el oferente deberá incluir, sin costo adicional para el SRI: - El hipervisor requerido para su operación (VMware, Hyper-V u otro equivalente), - Todo el hardware necesario para la implementación de la consola de gestión, - El licenciamiento correspondiente al hipervisor y/o Sistema Operativo - Cualquier componente de software/hardware adicional necesario para su correcta operación y retención/exportación de información.
3. Integración con plataformas de monitoreo La consola de administración deberá estar diseñada para operación con sistemas de gestión centralizada, facilitando el monitoreo, la respuesta y el análisis de eventos de seguridad en tiempo real.
4. Arquitectura centralizada y resiliencia La plataforma de gestión deberá operar como sistema central de control y coordinación.
Integración y coordinación entre controles de seguridad
5. Integración con el sistema DDoS La plataforma deberá integrar la información de detección y mitigación del sistema DDoS, permitiendo la correlación de eventos y la ejecución de acciones conjuntas.
6. Integración con el sistema WAF La plataforma deberá integrar la información proveniente del WAF, incluyendo eventos asociados a aplicaciones web y APIs.
7. Correlación de eventos La plataforma deberá correlacionar eventos de seguridad permitiendo un análisis integral de ataques.
8. Comunicación bidireccional en tiempo real Los componentes de seguridad deberán intercambiar telemetría y eventos con la plataforma de gestión de forma bidireccional y en tiempo real.
9. Contexto unificado de ataques La plataforma deberá presentar el contexto completo de los ataques, correlacionando origen, vector, impacto y acciones aplicadas entre los distintos controles de seguridad.
Orquestación y respuesta coordinada
10. Orquestación de mitigaciones La plataforma deberá permitir la activación coordinada de mitigaciones entre el sistema DDoS y el WAF, sin requerir intervención manual por cada componente.
11. Propagación controlada de políticas Las políticas de seguridad definidas desde la plataforma central deberán propagarse de forma controlada y consistente a los distintos componentes de la solución.
12. Automatización de respuesta La plataforma deberá soportar la automatización de respuestas ante eventos de seguridad, en función de reglas, umbrales y correlación de eventos.
13. Coordinación ante ataques complejos La plataforma deberá permitir la gestión centralizada de ataques combinados o multivector, coordinando acciones entre capas de red y de aplicación.
Visibilidad, monitoreo y análisis
14. Dashboards en tiempo real La plataforma deberá proporcionar dashboards en tiempo real con visibilidad del estado de los sistemas, ataques activos y acciones de mitigación.
15. Línea de tiempo de ataques La plataforma deberá presentar una línea de tiempo completa de los ataques, desde la detección hasta la mitigación y recuperación.
16. Análisis forense

La plataforma deberá permitir análisis forense de eventos, incluyendo detalles de tráfico, vectores de ataque y decisiones de mitigación.
17. Visualización consolidada La plataforma deberá mostrar eventos y métricas consolidadas de todos los componentes de seguridad, evitando silos de información.
Gestión de accesos, auditoría y trazabilidad
18. Control de accesos basado en roles (RBAC) La plataforma deberá soportar control de accesos basado en roles para administración, operación y auditoría.
19. Auditoría de cambios La plataforma deberá registrar todos los cambios realizados sobre políticas, configuraciones y acciones de mitigación.
20. Trazabilidad completa La plataforma deberá permitir trazabilidad completa de eventos, acciones y usuarios para fines de cumplimiento y auditoría.
21. Registro centralizado de eventos La plataforma deberá centralizar los registros de eventos de seguridad generados por todos los componentes integrados y tener una capacidad de retención de al menos 12 meses.
Integración con el ecosistema de seguridad
22. Integración con sistemas SIEM La plataforma deberá permitir integración con sistemas SIEM externos mediante protocolos estándar para correlación y análisis centralizado.
23. Exportación de eventos y reportes La plataforma deberá permitir la exportación de eventos y reportes en formatos estándar para análisis externo.
24. Interfaces de integración La plataforma deberá exponer interfaces programáticas para integración con sistemas externos de gestión y automatización.
Capacidades operativas de la plataforma
25. **Análisis automatizado de eventos** La plataforma de gestión centralizada deberá proporcionar análisis automatizado de eventos y ataques de todos los controles de seguridad (DDoS y WAF)
26. Asistencia operativa durante incidentes La plataforma deberá ofrecer asistencia operativa durante incidentes a través del partner, incluyendo contextualización del ataque, priorización de acciones y recomendaciones de mitigación orientadas a reducir el tiempo medio de respuesta.
27. Análisis post-incidente La plataforma deberá mantener capacidades de análisis post-incidente, preservando trazabilidad completa para auditoría y mejora continua.
28. Apoyo al operador Estas capacidades deberán apoyar al operador, sin sustituir la toma de decisiones humana.
29. Acceso sin dependencia En caso de indisponibilidad o falla de la plataforma de gestión centralizada, los sistemas de seguridad perimetral (Anti DDoS y WAF) deberán permitir el acceso administrativo directo e independiente a cada control, a través de sus interfaces de gestión, garantizando la continuidad de la operación, la visibilidad básica de eventos y la capacidad de administración sin dependencia obligatoria de la consola centralizada.
30. Respaldo de configuración de la plataforma de gestión El contratista deberá implementar un mecanismo de respaldo periódico de la configuración completa de la plataforma de gestión centralizada, con una frecuencia mínima semanal. El contratista deberá documentar y entregar al SRI el procedimiento de restauración de la plataforma a partir de los respaldos generados, como parte de los entregables de la etapa de Documentación definida en la Sección 7.1.

7. SERVICIOS CONEXOS REQUERIDOS

7.1 IMPLEMENTACIÓN Y TRANSFERENICA DE CONOCIMEINTOS

La implementación se planificará y ejecutará en las siguientes etapas

ETAPA	ACTIVIDADES PRINCIPALES	CRITERIO DE ACEPTACIÓN
PREPARACIÓN	Aprobación de la arquitectura HLD/LLD, interconexión e integración con infraestructura SRI, configuración inicial de los appliances, configuración de usuarios y perfiles de administración, validación de actualizaciones automáticas de firmas y alertas, pruebas de alta disponibilidad.	Arquitectura HLD/LLD aprobada por el SRI. Plan de implementación aprobado.
TRANSICIÓN	Configuración y aplicación de políticas de seguridad Anti-DDoS y WAF, periodo de aprendizaje recomendado por el fabricante, afinamiento de baselines y perfiles de aplicación, pruebas de seguridad y operación, elaboración de documentación de cambio (plan de implementación, contingencia y reverso).	Políticas configuradas y validadas. Documentación de cambio aprobada por el SRI.
PUESTA EN PRODUCCIÓN	Reemplazo o incorporación del sistema en la operación productiva de la red del SRI, según cronograma acordado con el administrador del contrato. Ejecución de actividades de contingencia y reverso según plan aprobado.	Sistema operando en producción sin incidentes no planificados.
ESTABILIZACIÓN	Monitoreo post-implementación, atención de incidentes derivados del cambio, corrección y afinamiento de configuraciones, configuración de reportes solicitados por el SRI y acompañamiento del fabricante.	Configuraciones estabilizadas. Reportes operativos habilitados y validados por el SRI.
DOCUMENTACIÓN	Pruebas de aceptación, memoria técnica, arquitectura de seguridad final (HLD/LLD), estándares de configuración, guías de operación y presentación a personal técnico del SRI.	Documentación técnica completa entregada y aceptada por el SRI.

- El contratista deberá elaborar, revisar y someter a aprobación del SRI la arquitectura de la solución (HLD/LLD), así como el plan de implementación, incluyendo actividades, responsables, ventanas de intervención, criterios de validación, contingencia y reverso.
- La implementación deberá ejecutarse de manera integral, coordinada y por etapas, en concordancia con el alcance definido para la solución DDoS, WAF y plataforma de gestión centralizada, así como con la metodología de trabajo y el cronograma aprobados por el SRI.
- El contratista deberá realizar la instalación lógica, configuración inicial, integración, pruebas, afinamiento, puesta en producción y estabilización de los sistemas DDoS y WAF en los centros de datos principal y alterno, incluyendo la consola de administración centralizada, conforme a la arquitectura aprobada por el SRI.
- La implementación deberá contemplar la integración de la solución con la infraestructura tecnológica existente del SRI, considerando topología, conectividad, segmentación, dependencias de red, interoperabilidad con los componentes actuales y requerimientos operativos de los servicios institucionales publicados en Internet.

- El contratista deberá ejecutar la migración de configuraciones, políticas, perfiles, reglas y demás parámetros de protección desde las plataformas actuales hacia la nueva solución, asegurando consistencia funcional, trazabilidad de cambios y continuidad operativa.
- La solución deberá contemplar un período de aprendizaje y afinamiento inicial, conforme a las recomendaciones del fabricante y al cronograma aprobado por el SRI, durante el cual se ajustarán perfiles de comportamiento, líneas base, firmas, políticas y umbrales de detección, sin afectar la disponibilidad ni el desempeño de los servicios institucionales.
- Durante la implementación del sistema Anti-DDoS, el contratista deberá definir, configurar y validar las políticas de protección requeridas para los segmentos de red y servicios críticos identificados por el SRI, incluyendo parámetros de comportamiento, límites de tráfico, mecanismos de mitigación y reglas adaptadas a la operación institucional, minimizando falsos positivos y preservando el tráfico legítimo.
- Durante la implementación del sistema WAF, el contratista deberá configurar y validar las políticas de seguridad para las aplicaciones web y APIs priorizadas por el SRI, incluyendo perfiles positivos y negativos, protecciones contra OWASP Top 10, mecanismos de aprendizaje, firmas, controles de abuso, virtual patching y demás funcionalidades requeridas para la protección de los servicios publicados.
- El contratista deberá verificar la correcta operación de la solución en el centro de datos principal y en el centro de datos alterno, incluyendo los esquemas de alta disponibilidad, la sincronización de políticas y eventos, la visibilidad centralizada y la generación de reportes requeridos por el SRI.
- Como parte del servicio, el contratista deberá ejecutar y documentar pruebas funcionales, de integración, de alta disponibilidad, de seguridad y de operación, con el fin de demostrar que la solución implementada cumple con los requerimientos técnicos, no introduce interrupciones no planificadas y se encuentra apta para su puesta en producción.
- La puesta en producción deberá realizarse conforme al cronograma y ventanas aprobadas por el SRI, con acompañamiento técnico del contratista y del fabricante, y con ejecución controlada de actividades de validación, contingencia, reverso, monitoreo y estabilización posterior al cambio.

- El contratista deberá ejecutar y documentar las siguientes pruebas:

  Pruebas funcionales

  - Verificación de operación de todos los componentes (DDoS, WAF, consola) en ambos centros de datos.
  - Validación de políticas de seguridad configuradas.
  - Verificación de integración con la infraestructura existente del SRI.

  Pruebas de alta disponibilidad

  - Simulación de fallo de un nodo en el Centro de Datos Principal y verificación de conmutación automática.
  - Verificación de sincronización de políticas y eventos entre nodos.
  - Validación del tiempo de recuperación (RTO) conforme a lo ofertado.

  Pruebas de seguridad

  - Verificación de detección y mitigación de al menos tres (3) vectores de ataque DDoS representativos.
  - Verificación de detección de al menos cinco (5) categorías del OWASP Top 10 en el WAF.
  - Validación de que el tráfico legítimo no es bloqueado durante las pruebas de mitigación.

  Criterios de aprobación y rechazo

  - Todas las pruebas deberán documentarse con evidencias (capturas, logs, reportes).

- El SRI aprobará o rechazará los resultados en un plazo máximo de cinco (5) días hábiles.
- En caso de rechazo, el contratista tendrá diez (10) días hábiles para corregir y re-ejecutar las pruebas fallidas.

7.2 TRANSFERENCIA DE CONOCIMIENTO

- La transferencia de conocimiento se organizará considerando una asistencia de hasta nueve (9) funcionarios del SRI y una duración de no menos de cuarenta (40) horas.
- La transferencia de conocimiento debe realizarse de forma presencial en instalaciones provistas por el fabricante/contratista, con los materiales, laboratorios prácticos y todos los equipos necesarios.
- Los temas deben cubrir todos los componentes implementados: sistema Anti-DDoS y sistema WAF, incluyendo su plataforma de gestión centralizada, capacidades de monitoreo y análisis de eventos, así como los procedimientos operativos asociados.
- El contenido debe incluir: arquitectura tecnológica y de seguridad del sistema, administración y gestión de políticas, interpretación de eventos y ataques, procedimientos de respuesta ante incidentes, y mantenimiento operativo.
- Se deberán incluir los respectivos cursos y certificaciones del fabricante sobre las herramientas DDoS y WAF para los participantes mencionados.
- Toda la logística asociada con la transferencia de conocimiento correrá por cuenta del contratista.

7.3 SOPORTE LOCAL

El servicio de soporte local estará conformado por: servicio de mantenimiento preventivo, servicio de mantenimiento correctivo y servicio de asistencia técnica, con una vigencia de 1.005 días calendario contados a partir del día siguiente a la culminación de la implementación.

7.3.1 MANTENIMIENTO PREVENTIVO

ESPECIFICACIÓN TÉCNICA

- El servicio de mantenimiento preventivo debe cubrir todos los equipos del componente de hardware: appliances Anti-DDoS, appliances WAF y la plataforma (consola) de gestión centralizada, según corresponda.
- Anualmente el contratista realizará una visita de mantenimiento preventivo por cada centro de datos, revisando alarmas, estado físico de los equipos, limpieza especializada e instalación de los últimos parches de firmware recomendados por el fabricante.
- Las visitas de mantenimiento preventivo deberán coordinarse con el administrador del contrato con un mínimo de 10 días hábiles de anticipación y ejecutarse dentro de las ventanas de mantenimiento aprobadas por el SRI.

Entregables por visita:

Por cada visita realizada, el contratista entregará un **Informe de mantenimiento preventivo** que incluya:

- Diagnóstico por alarmas y revisión física del estado de los equipos;
- Reporte de actualización de firmware (versión anterior vs. versión actual);
- Registro fotográfico del estado físico de los equipos;
- Conclusiones, hallazgos y acciones correctivas recomendadas;
- Firma de conformidad del administrador del contrato del SRI.

7.3.2 ACUERDOS DE NIVEL DE SERVICIO

1. El tiempo de respuesta se define como el lapso entre el momento en que el SRI hace la solicitud de servicio y el momento en que inicia el análisis técnico por parte del ingeniero especialista designado a dicho requerimiento. Aplica a los servicios de mantenimiento correctivo y de asistencia técnica.
2. La notificación de recepción del requerimiento no es aceptada como el inicio del análisis técnico.
3. El tiempo de reemplazo se define como el lapso desde que se diagnostica la falla de hardware hasta el momento en el que se instala el repuesto y se recupera la operación normal del equipo. Aplica exclusivamente a los incidentes de mantenimiento correctivo que requieren que se aplique garantía técnica.

PRIORIDAD	MANTENIMIENTO CORRECTIVO	ASISTENCIA TÉCNICA	REEMPLAZO DE HARDWARE
1	Fallo total o parcial de componentes en CD Principal; indisponibilidad o degradación de servicios productivos del SRI.	Solicitudes asociadas a componentes del CD Principal o servicios productivos protegidos.	Reemplazo en CD Principal.
2	Fallo de componentes en CD Alterno; operación con funcionalidad reducida sin afectar producción.	Solicitudes asociadas a componentes del CD Alterno o servicios no productivos.	Reemplazo en CD Alterno.
3	Advertencias que no causan indisponibilidad ni degradación de servicios.	Planificación, afinamiento, diagnóstico, actualizaciones, reportes e intervenciones del fabricante.	N/A

PRIORIDAD	TIEMPO DE RESPUESTA – CORRECTIVO	TIEMPO DE RESPUESTA – ASISTENCIA	TIEMPO DE REEMPLAZO HARDWARE
1	1 hora	3 horas	8 horas
2	3 horas	6 horas	16 horas laborables
3	24 horas	16 horas laborables	N/A

7.3.3 MANTENIMIENTO CORRECTIVO Y ASISTENCIA TÉCNICA

ESPECIFICACIÓN TÉCNICA

- El servicio de mantenimiento correctivo debe cubrir todos los componentes del objeto de contrato: appliances Anti-DDoS, Appliances WAF, plataforma de gestión centralizada y software asociado.
- El servicio debe estar disponible 24 horas al día, 7 días a la semana durante toda la vigencia del contrato.
- Los servicios de mantenimiento correctivo y asistencia técnica tendrán una duración por todo el periodo de vigencia del contrato.
- Las actividades de atención podrán realizarse remota o presencialmente según lo requiera el personal técnico del SRI, sin costo adicional por atención fuera de horario laboral.
- El contratista será responsable de la gestión integral del servicio: canales de atención, registro y seguimiento de tickets, coordinación, escalamiento, comunicación, evidencias y cierre de casos.

- Los tiempos de respuesta y resolución se regirán por los niveles de servicio (SLA) establecidos en la Sección 7.3.2 del presente documento.

8. GLOSARIO DE TÉRMINOS

1. **DDoS** (Denegación de Servicio Distribuido): Ataque que busca saturar un servicio o sistema con grandes volúmenes de tráfico desde múltiples orígenes para dejarlo indisponible.
2. **WAF** (Web Application Firewall): Firewall especializado en proteger aplicaciones web, inspeccionando y filtrando solicitudes HTTP/HTTPS para bloquear ataques dirigidos a la capa de aplicación.
3. **IPS** (Sistema de Prevención de Intrusiones): Tecnología que detecta y bloquea amenazas o actividades maliciosas en tiempo real dentro del tráfico de red.
4. **OWASP Top 10**: Listado de las diez categorías de riesgos de seguridad más críticas para aplicaciones web, publicado por la organización OWASP.
5. **API** (Application Programming Interface): Conjunto de reglas y mecanismos que permite la comunicación e intercambio de datos entre sistemas o aplicaciones.
6. **SLA** (Acuerdo de Nivel de Servicio): Compromiso formal que define tiempos de respuesta, resolución y niveles mínimos de atención que debe cumplir el proveedor.
7. **HLD/LLD**: Documentos de diseño de alto nivel y de bajo nivel que describen la arquitectura general y el detalle técnico de implementación de la solución.
8. **Alta Disponibilidad (HA):** Esquema de diseño que busca mantener un servicio operativo ante fallas, mediante redundancia y conmutación entre equipos.
9. **EOL (End of Life):** Estado en el que un fabricante declara que un producto ha llegado al fin de su vida útil comercial y deja de evolucionarlo.
10. **EOST (End of Support):** Fecha a partir de la cual un fabricante deja de brindar soporte técnico, actualizaciones o correcciones para un producto.

9. PLAZO DE EJECUCIÓN

HITO / ENTREGABLE	PLAZO MÁXIMO
Plazo total del contrato	Hasta 1.185 días calendario
Entrega de bienes instalados y puesta en marcha (hardware + software base) instalación física	90 días calendario desde la notificación del administrador del contrato
Vigencia de garantía técnica y soporte de fábrica	1.095 días calendario desde la culminación de la instalación del hardware
Vigencia del licenciamiento del componente de software	1.095 días calendario desde la culminación de la instalación del hardware
Servicio de implementación, integración y transferencia de conocimiento	60 días calendario desde el día siguiente a la culminación de la instalación del hardware
Vigencia del servicio de soporte local	1.005 días calendario desde el día siguiente a la culminación de la implementación

10. FORMA Y CONDICIONES DE PAGO

El Servicio de Rentas Internas (SRI) pagará al contratista conforme a los hitos y entregables establecidos en el presente TDR, previa presentación de la planilla de pago y la suscripción de las actas de entrega–recepción correspondientes, de acuerdo con el siguiente detalle:

- **Componente de hardware, instalación, garantía técnica de hardware y licenciamiento (software y soporte de fábrica):** El cien por ciento (100%) de este rubro se pagará contra entrega, instalación y puesta en funcionamiento de los bienes, previa presentación de la planilla de pago y la suscripción del acta de entrega–recepción correspondiente.
- **Implementación y transferencia de conocimiento:** El cien por ciento (100%) de este rubro se pagará contra entrega de los entregables y evidencias de implementación y de la transferencia de conocimiento establecida en la Sección 7.1 y 7.2, previa presentación de la planilla de pago y la suscripción del acta de entrega–recepción correspondiente.
- **Soporte local (mantenimiento preventivo, correctivo y asistencia técnica):** Este rubro se pagará en partes iguales, al final de cada período establecido en el **plazo de ejecución** y conforme al cronograma aprobado, previa presentación de la planilla de pago y la suscripción del acta de entrega–recepción correspondiente a cada período. Para el último pago, se requerirá adicionalmente la suscripción del acta de entrega–recepción final.

11. PERIODO DE VALIDEZ DE LA/S OFERTA/S

El período de validez de la Oferta será de ***154*** días contados a partir de la fecha de presentación de Ofertas

12. VARIACIÓN DE CANTIDADES AL MOMENTO DE ADJUDICACION

No existirá aumento o disminución de cantidades

13. PLAZO PARA LA PREPARACIÓN DE LA/S OFERTA/S

El plazo para la preparación de la(s) oferta(s) será de 7 semanas (49 días) a partir de la fecha del llamado a licitación.

14. 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 completa en un periodo menor de 18 meses.

15. PENALIDADES

El Servicio de Rentas Internas impondrá al contratista las siguientes penalidades ante incumplimientos:

PENALIDAD	EVENTO DE INCUMPLIMIENTO	UNIDAD DE CÁLCULO
2/1000	Retraso en la instalación de bienes, activación de garantía técnica y soporte de fábrica.	Por día de retraso
2/1000	Retraso en la entrega de la documentación de garantía técnica y soporte de fábrica.	Por día de retraso
2/1000	Retraso en el tiempo máximo de respuesta de los casos de soporte, según SLA	Por hora de retraso

PENALIDAD	EVENTO DE INCUMPLIMIENTO	UNIDAD DE CÁLCULO
2/1000	Retraso en el tiempo máximo establecido para reemplazo de partes y piezas.	Por hora de retraso
1/1000	Retraso en la entrega del servicio de implementación.	Por día de retraso
1/1000	Retraso en la entrega de la transferencia de conocimiento.	Por día de retraso
1/1000	Retraso en la entrega de informes y reportes de soporte local.	Por día de retraso
1/1000	Inasistencia a visitas programadas de mantenimiento preventivo.	Por día de inasistencia

Las penalidades se calcularán sobre el monto de las obligaciones que se encuentren pendientes de ejecutar.

16. PERSONAL TÉCNICO

ROL	**CANT.**	**PERFIL REQUERIDO**	**Certificación vigente Mínimo una obligatoria***	**RESPONSABILIDADES**
Gerente del Proyecto	1	Ing. Sistemas, Telecomunicaciones, Electrónica o equivalente (Tercer Nivel). Maestría en Seguridad Informática o equivalente (Cuarto Nivel).	SCRUM Máster o PMP Mín. 2 años de experiencia en gestión/implementación de proyectos tecnológicos de seguridad perimetral de gran escala.	Gestión, coordinación y documentación del proyecto. Transferencia de conocimiento de la solución en conjunto con el fabricante
Especialista Técnico – Anti-DDoS	2	Ing. Sistemas, Telecomunicaciones, Electrónica o equivalente (Tercer Nivel).	Certificación técnica profesional del fabricante del sistema Anti-DDoS ofertado. Mín. 2 años de experiencia en implementación o soporte de soluciones de seguridad perimetral de gran escala.	Acompañamiento en la Implementación, migración y soporte del sistema Anti-DDoS. Transferencia de conocimiento de la solución en conjunto con el fabricante
Especialista Técnico – WAF	2	Ing. Sistemas, Telecomunicaciones, Electrónica o equivalente (Tercer Nivel).	Certificación técnica profesional del fabricante del sistema WAF ofertado, vigente. Mín. 2 años de experiencia en	Acompañamiento en la Implementación, migración y soporte del sistema WAF.

ROL	CANT.	PERFIL REQUERIDO	Certificación vigente Mínimo una obligatoria*	RESPONSABILIDADES
			implementación o soporte de soluciones de seguridad perimetral de gran escala.	Transferencia de conocimiento de la solución en conjunto con el fabricante

La implementación de la solución deberá ser ejecutada con la participación directa del fabricante de la tecnología ofertada, en coordinación con el contratista (canal) y su equipo técnico.

El contratista será responsable de garantizar que el personal asignado cuente con el respaldo, validación o certificación vigente del fabricante, y que la implementación se realice conforme a las mejores prácticas, metodologías y lineamientos oficiales establecidos por este.

El fabricante deberá participar al menos en las fases de validación o diseño (HLD/LLD), implementación, pruebas de la solución y transferencia de conocimiento.

Para efectos de este contrato, el personal detallado en la tabla de la presente sección corresponde al mínimo técnico requerido. Considerando que el alcance incluye soporte en modalidad 24x7 y el cumplimiento de los SLA establecidos, la atención de incidentes y requerimientos técnicos asociados a la solución (DDoS y WAF) se realizará principalmente mediante el soporte de fábrica (fabricante) 24x7, de tipo directo, permitiendo al personal del SRI la apertura de casos con el fabricante.

El contratista será responsable de la gestión integral del servicio (canales de atención, registro y seguimiento de tickets, coordinación, manos remotas, escalamiento, comunicación, evidencias y cierre), así como de garantizar el cumplimiento de los niveles de servicio y las obligaciones contractuales.

17. OTROS PARÁMETROS REQUERIDOS

No.	DESCRIPCIÓN	OBSERVACIONES
1	El oferente debe ser distribuidor autorizado de fábrica de los siguientes componentes: Sistema Anti-DDoS, Sistema WAF, soluciones de seguridad perimetral.	Certificado emitido por el fabricante durante el año en curso.
2	El oferente debe proveer toda la documentación técnica necesaria para validar el cumplimiento de las especificaciones técnicas: fichas técnicas, hojas de especificación, catálogos, manuales, certificados de fábrica.	Indicar ubicación exacta donde consta la información. Entregar copias en formatos editables (MS Word, MS Excel, PDF que permita la búsqueda y copia de texto).

18. LUGAR DE ENTREGA

- Los appliances Anti-DDoS y WAF principales, y la consola de administración, deberán entregarse e instalarse en el Centro de Datos Principal del SRI, ubicado en la ciudad de Quito.

- Los appliances Anti-DDoS y WAF alternos deberán entregarse e instalarse en el Centro de Datos Alterno en Guayaquil, en instalaciones de CNT bajo modalidad de housing (Sector Casas Viejas, según se indica en la Nota General).

- Las actividades que no requieran intervención directa sobre equipos se atenderán en las instalaciones del SRI en Quito: Av. Río Amazonas entre Unión Nacional de Periodistas y Alfonso Pereira, Plataforma Gubernamental de Gestión Financiera, Bloque 5 (Azul), piso 1.

- Toda documentación deberá entregarse principalmente en formato digital, suscrita electrónicamente, dirigida al administrador del contrato.