AMPLIACIÓN CONVOCATORIA PARA LA ELABORACIÓN DEL ESTUDIO DE MERCADO

El Servicio de Rentas Internas (SRI) a través de la Dirección Nacional de Tecnología, convoca a proveedores nacionales e internacionales a participar en el proceso de elaboración del Estudio de Mercado para la **"ADQUISICIÓN DE SISTEMA DE PREVENCIÓN DE INTRUSOS".**

Este estudio de mercado será utilizado para la definición del presupuesto referencial previo a la publicación del proceso de adquisición.

El precio referencial de los bienes deberá considerar los siguientes aspectos:

- Las especificaciones técnicas detalladas adelante;
- Los precios cotizados deben estar en valor DDP Delivered Duty Paid/ Entregado con derechos pagados, incluyendo todos los derechos de aduanas e impuestos;
- La vigencia de la cotización no debe ser menor a 120 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 1184 días calendario contados a partir del día siguiente hábil de la notificación del administrador del contrato.

Las cotizaciones deben ser remitidas en formato digital (firmadas), al correo institucional programaintax@sri.gob.ec hasta el día 30 de enero de 2024, 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 120 días)
Firma de responsabilidad.

Datos del contratante:

A nombre de: Servicio de Rentas Internas
RUC: 1760013210001

Formato Presentación Cotización:

Propuesta Económica:

Presupuesto total del proyecto:				
DESGLOSE DE COMPONENTES				
Tipo de recurso	**Descripción producto / servicio**	**Cantidad**	**Costo unitario**	**Total**
Hardware	Equipo - Sistema de Prevención de Intrusos - Centro de Datos Principal (Quito), incluye software y garantía de fábrica por 3 años. Instalación. Consola de administración centralizada			

Hardware	Equipo - Sistema de Prevención de Intrusos - Centro de Datos Alternol (Guayaquil), incluye software y garantía de fábrica por 3 años. Instalación.			
Servicios	Migración, Implementación y Transferencia de conocimientos	1		
Servicios	Mantenimiento Preventivo anual	3		
			Subtotal	$ 0,00
			IVA (12 %)	$ 0,00
			Total	**$ 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.

Servicio de Rentas Internas

ESPECIFICACIONES TECNICAS

1. INFRAESTRUCTURA ACTUAL

La solución del Sistema de Prevención de Intrusos (nueva generación / NGIPS) actualmente implementada en el ambiente de Producción del SRI, se compone de 1 equipo físico tipo appliance modelo *TippingPoint 8200TX* que incluye software propietario del fabricante; y 1 equipo virtual modelo *SMS vSMS Enterprise* correspondiente a la consola de gestión.

Los puertos que se disponen a nivel de los equipos de networking Nexus 9300 permiten conexiones de 1 ó 10 GB autonegociables.

Equipamiento y licenciamiento actual de la solución del Sistema de Prevención de Intrusos (nueva generación):

Producto	Marca / Modelo	Licencia	Vigencia Licenciamiento	Throughput
IPS	TippingPoint / 8200TX-0100-1423	TP-9HKY-L32DL-K35MB-WEXHD-B5TK7-U9Z7E	27/12/2024	Hardware, 3Gbps Feature Throughput, Threat DV

La infraestructura de ambientes virtualizados del Sistema de Prevención de Intrusos que dispone el SRI, se encuentra implementada con la plataforma VMWARE ESXi versión 7.0.3.

2. BIENES REQUERIDOS

2.1 ELEMENTOS DE HARDWARE

- La infraestructura del Sistema de Prevención de Intrusos (nueva generación / NGIPS) debe:
  - Estar integrada por hardware para el Centro de Datos Principal en la ciudad de Quito, y para el Centro de Datos Alterno en la ciudad de Guayaquil.
  - Estar conformado por dos equipos físicos, uno para el Centro de Datos Principal en la ciudad de Quito, y uno para el Centro de Datos Alterno en la ciudad de Guayaquil.
  - Incluir el software propio del fabricante, y las suscripciones de software necesarias.
  - Contar con una interfaz web de administración local, que permita la gestión de la configuración del equipo y de las políticas de protección.
  - Tener visibilidad sobre el tráfico cifrado, por medio de componentes de hardware que permitan el descifrado de tráfico en línea.

- Los equipos del Sistema de Prevención de Intrusos (nueva generación / NGIPS) deben:
  - Tener al menos 3 segmentos de protección.
  - Fuente de poder redundante.
  - Poder ser monitoreados por SNMP.
  - Soportar al menos SNMP V2, V3.
  - Contar con una protección frontal que impida la manipulación no autorizada de los componentes del servidor
  - Ser servidores de bastidor (“rack-mounted servers”) y deben poderse montar en bastidores (“racks”) de 19¨.
  - Contar con los rieles, sujetadores y demás accesorios necesarios para un montaje seguro y organizado en los centros de datos del Servicio de Rentas Internas (SRI).
  - Soportar al menos 3.3 Gbps de throughput de tráfico total con todas las protecciones activadas, incluyendo el descifrado de tráfico en línea. Los equipos deben tener la capacidad de crecimiento

para soportar al menos hasta 4 Gbps de throughput a futuro.
- El equipo para Quito debe tener cuatro (4) interfaces Ethernet 1Gbps de fibra
- El equipo para Guayaquil debe tener dos (2) interfaces Ethernet 10Gbps de fibra.
- Las interfaces deben tener mecanismo de bypass interno en el equipo, con la opción de configurarlo en fail-open o fail-close.
- Incluir las suscripciones de software necesarias del Fabricante.
- Se deberá tener derecho de uso de nuevas versiones de software, hotfix, parches, durante la vigencia de las suscripciones del Sistema de Prevención de Intrusos (Nueva generación / NGIPS).
- Se tendrá derecho a actualizaciones de nuevas versiones del software para el Sistema de Prevención de Intrusos (nueva generación / NGIPS) sin costo adicional para el SRI durante la vigencia de las suscripciones. El contratista será quien realice las actualizaciones, migraciones bajo la coordinación del Administrador de Contrato.
- La suscripción del software será provista con soporte ilimitado del fabricante por 3 años (1095 días) calendario, a partir de la fecha de activación.

- Los equipos del Sistema de Prevención de Intrusos (nueva generación / NGIPS) deben cumplir con las siguientes funcionalidades:
  - Tener visibilidad sobre el tráfico cifrado, por medio de componentes de hardware que permitan el descifrado de tráfico en línea.
  - Ser accesible a través de SSH y de interfaz Web usando SSL.
  - Soportar al menos los siguientes modos de protección:
    - En línea: Bloquea y reporta ataques
    - Monitoreo: Reporta ataques, pero no los bloquea
  - Contar con protección por firmas de ataques conocidos, que a su vez deben ser categorizadas al menos a nivel de criticidad y tipos de amenaza.
  - Permitir configurar excepciones de análisis de tráfico por firma o por categoría.
  - Permitir crear firmas personalizadas por el usuario.
  - Contar con la funcionalidad de geolocalización de tráfico, es decir, detectar el país de dónde proviene o hacia qué país es destinado el tráfico; con el objetivo de poder configurar reglas de protección basadas en dicho criterio.
  - Detectar y bloquear ataques dirigidos a explotar vulnerabilidades de día cero.
  - Detectar y bloquear tráfico que provenga de fuentes conocidas con mala reputación.
  - Operar y proteger ambientes en los cuales exista tráfico asimétrico sin necesidad de realizar cambios a la topología de la red.
  - Actualizar las firmas, fuentes de mala reputación, listado de malware conocido y otros insumos que las diferentes tecnologías de protección necesiten, de manera automática, desde una red de inteligencia global propia del Fabricante de la solución ofertada.
  - Proteger ante vulnerabilidades conocidas, donde se proteja el tráfico cuyo patrón obedezca al menos a vulnerabilidades conocidas tipo CVE.
  - Contar con protección contra malware al menos de tipo phishing, botnets, troyanos, spyware y gusanos de red.
  - Inspeccionar el tráfico encapsulado en túneles.
  - Soportar sincronización de tiempo a través de NTP.
  - Permitir la aplicación de políticas de protección, la cual debe ser al menos por, dispositivo NGIPS, segmento físico, vlan, direcciones IP, rangos de direcciones IP CIDR (Classless Inter-Domain Routing).
  - Integrarse con Active Directory al menos versión 2019, para reconocer usuarios del dominio para el acceso a los equipos que conforman la solución ofertada.
  - Notificar mediante alertas visuales o correo electrónico cuando existan nuevas versiones o releases de cualquier componente que conforma la solución.
  - Soportar clave pública de curva elíptica para la descripción e inspección de tráfico SSL.
  - El equipo del sistema de Prevención de Intrusos de Nueva Generación NGIPS debe incluir las suscripciones de software propietario del Fabricante.
  - Se deberá suministrar un acceso vía web al portal del fabricante para revisar el estado de las suscripciones de software, información de nuevas versiones, actualizaciones, ingresos y

seguimiento de casos de soporte.
- Las políticas de protección para todas las tecnologías que disponga los equipos del Sistema de Prevención de Intrusos (nueva generación / NGIPS) deben ser configurables mediante la consola de administración.
- El oferente debe garantizar que los equipos del Sistema de Prevención de Intrusos (nueva generación / NGIPS) ofertados no entre en EOS ("End-of-Support") o en EOL ("End-of-Life") durante los 5 años posteriores a la suscripción del contrato.

CONSOLA DE ADMINISTRACIÓN

La solución del Sistema de Prevención de Intrusos (nueva generación / NGIPS) debe contar con una consola de administración centralizada para el Centro de Datos Principal en la ciudad de Quito, la cual tendrá las siguientes características o funcionalidades:

- La consola de administración de la solución puede ser físico o virtualizado.
- Debe incluir el software propio del fabricante y las suscripciones necesarias.
- En caso de que la consola de administración sea virtualizada, el SRI proveerá los recursos virtuales dentro de la plataforma VmWare de la institución, para lo cual el proveedor deberá suministrar al administrador del contrato en la etapa de instalación las características de memoria, procesamiento y almacenamiento requeridas.
- Debe tener la capacidad para configurar todos los tipos de políticas de protección aplicables para los dispositivos del Sistema de Prevención de Intrusos (nueva generación / NGIPS) administrados, para el Centro de Datos Principal en la ciudad de Quito, y para el Centro de Datos Alterno en la ciudad de Guayaquil.
- Debe tener capacidad para crear respaldos completos de configuración, eventos, logs y poder enviarlos a un servidor FTP o SCP externo del SRI.
- Debe tener capacidad para gestionar las actualizaciones de todos los componentes de los dispositivos del Sistema de Prevención de Intrusos (nueva generación / NGIPS) administrados, para el Centro de Datos Principal en la ciudad de Quito, y para el Centro de Datos Alterno en la ciudad de Guayaquil.
- Debe ser accesible a través interfaz Web usando SSL o mediante un cliente local.
- Debe soportar sincronización de tiempo a través de NTP.
- Debe ser accesible por SNMP para tareas de monitoreo.
- Debe soportar al menos SNMP V2, V3.
- La interfaz gráfica de la consola de administración del Sistema de Prevención de Intrusos (nueva generación / NGIPS) debe permitir varios niveles de acceso incluyendo al menos los niveles de administrador y operador.
- La interfaz gráfica de la consola de administración del Sistema de Prevención de Intrusos (nueva generación / NGIPS) debe incluir registros de auditoría de los cambios realizados en configuraciones y políticas, mostrando al menos la fecha y hora de cambio, así como el usuario que lo realizó.
- Debe contar con un módulo de reportes incluido. Los reportes deberán mostrar datos de eventos de seguridad de al menos 18 meses atrás.
- El fabricante debe disponer de un portal donde se detalle todas las firmas liberadas, que al menos incluya: Nombre, descripción, fecha en la que fue liberada, severidad, relación con vulnerabilidades conocidas CVE, umbrales de detección.
- Debe soportar al menos los siguientes exploradores: EDGE, Mozilla Firefox y Google Chrome.
- Debe integrarse con Active Directory al menos versión 2019 para la autenticación.
- Debe incluir un mecanismo de integración para permitir reenviar los eventos de seguridad a un correlacionador de eventos externo.

2.2 INSTALACIÓN

La instalación deberá incluir:

- Planificación y coordinación de los trabajos de instalación e implementación.

- Instalación del software y hardware del nuevo Sistema de Prevención de Intrusos (nueva generación / NGIPS), para el Centro de Datos Principal en la ciudad de Quito, y para el Centro de Datos Alterno en la ciudad de Guayaquil.
- El contratista deberá solicitar al SRI la información o colaboración que necesite para la consecución de la implementación con la debida antelación, para garantizar el cumplimiento de los plazos de ejecución.
- El contratista deberá instalar el hardware del nuevo Sistema de Prevención de Intrusos (nueva generación / NGIPS) siguiendo las mejores prácticas de ensamblaje, montaje, configuración de parámetros y de conexión recomendadas por el fabricante del mismo.
- Para el despliegue de los componentes de hardware se debe contar con:
  - Cables ("patchcords"), transceptores ("transceivers"), rieles, bandejas, sujetadores y demás accesorios para para su montaje e interconexión se realicen de forma segura y organizada en los centros de cómputo del SRI.
  - Transceptores ("transceivers") de modelo CISCO SFP-10G-SR que sean necesarios para las conexiones tanto de 10Gbps como de 1Gbps.
  - Todos los cables (“patchcords”) de par trenzado y de fibra óptica deben ser certificados.
  - Todos los cables (“patchcords”) de par trenzado deben ser de categoría 6 o superior, y deben ser blindados (“shielded”).
  - Demás accesorios que sean necesarios para una interconexión segura y organizada con la infraestructura tecnológica del SRI.
- El contratista deberá configurar el firmware de todos los componentes (ej. BIOS, lights–out management, controladoras, tolerancia a fallos de RAM, etc.) de todos los servidores del nuevo sistema, de modo que se garantice su operación en alto desempeño (“high performance”), del nuevo Sistema de Prevención de Intrusos (nueva generación / NGIPS).
- Personal técnico especializado del fabricante del Sistema de Prevención de Intrusos (nueva generación / NGIPS) deberá definir los valores recomendados para los parámetros de configuración de firmware y software de cada uno de los servidores del sistema, en base a su rol.
- El contratista deberá instalar el software de Sistema de Prevención de Intrusos (nueva generación / NGIPS), en la última versión estable liberada, en todos los equipos del nuevo sistema, tanto de Producción como de Contingencia.
- El contratista deberá realizar pruebas de aceptación de acuerdo con las Características Técnicas del Hardware solicitadas.
- El contratista deberá entregar la memoria técnica de instalación

2.3 GARANTÍA TÉCNICA

- El contratista 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 donde debe constar la marca, modelo, numero de serie y ubicación de los bienes.
- Si durante la vigencia de la garantía técnica se identifica que el dimensionamiento de alguno de los bienes no abastece la “Capacidad de Tráfico” solicitada, el contratista deberá incrementar o reemplazar los elementos de hardware y software sin cargo alguno, hasta obtener el rendimiento del equipo de acuerdo con la capacidad de desempeño solicitada, incluyendo de ser necesario la mano de obra, atención en sitio en horario 24x7.
- En caso de falla de alguno de los elementos de hardware o alguno de sus componentes, o de degradación del desempeño de alguno de los elementos de hardware o alguno de sus componentes, o de observarse comportamientos no esperados durante la operación de alguno de los elementos de hardware o alguno de sus componentes internos, el contratista deberá proceder con el reemplazo de las partes o las piezas comprometidas, o de los elementos de hardware completos de ser necesario; nuevos y sin costo adicional para el SRI, cumpliendo con el Acuerdo de Nivel de Servicio establecidos.
- Durante el periodo de vigencia de la garantía técnica, el contratista deberá aplicar las nuevas versiones de firmware estables, los parches (“hotfix”) de firmware, y los cambios de configuración, que sean recomendados el fabricante del hardware; sin costo adicional para el SRI.
- La garantía técnica debe incluir, pero no debe estar limitado a, las prestaciones que se indican a

continuación:

- Gestión de incidentes causados por el hardware
- Recomendación de versiones de firmware para los servidores del sistema
- Revisión del estado de los servidores del sistema
- Acceso a la Base de Conocimientos del fabricante
- Acceso a la Mesa de Ayuda del fabricante
- Notificaciones proactivas de nuevas versiones y parches liberados

- Todos los puntos anteriores deben estar disponible las 24 horas del día, los 7 días de la semana, durante la vigencia del contrato Cubre la operación integral del Sistema de Prevención de Intrusos (nueva generación / NGIPS), incluyendo tanto los elementos de hardware como el software de este, y tanto aspectos de operación como de seguridad informática.

3. SERVICIOS CONEXOS REQUERIDOS

3.1 MIGRACIÓN E IMPLEMENTACIÓN

3.1.1 MIGRACIÓN NGIPS / CENTRO DE DATOS PRINCIPAL EN LA CIUDAD DE QUITO

- El Plan de Migración del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Principal en la ciudad de Quito, contendrá al menos lo indicado a continuación:
  - Cronograma de trabajo.
  - Diseño detallado propuesto.
  - Arquitectura detallada propuesta.
  - Personal asignado como técnicos especialistas de soporte y mantenimiento de Sistemas de Prevención de Intrusos de Nueva Generación
- El Plan de Migración podrá ser modificado por acuerdo entre el Administrador del contrato y contratista.
- Los trabajos de migración deberán cubrir todos los módulos y funciones del Sistema de Prevención de Intrusos (nueva generación / NGIPS).
- Se deberán validar, depurar y optimizar las configuraciones de operación del software del Sistema de Prevención de Intrusos (nueva generación / NGIPS) de manera que se garantice el mayor desempeño posible del nuevo sistema.
- Se deberán validar, depurar y optimizar las configuraciones y políticas de seguridad del software del Sistema de Prevención de Intrusos (nueva generación / NGIPS) de manera que se garantice el mayor nivel de seguridad posible para los servicios tecnológicos del SRI protegidos por el nuevo sistema.
- El contratista deberá configurar el módulo de reportería de manera que la información de los registros de eventos contenga el mayor detalle posible para que esté disponible para la generación de reportes; en función de la capacidad disponible del hardware del Sistema de Prevención de Intrusos (nueva generación / NGIPS).
- El contratista deberá configurar y probar los mecanismos de emisión de alertas (ej. Vía email) del Sistema de Prevención de Intrusos (nueva generación / NGIPS).
- El contratista deberá ofrecer acompañamiento en sitio durante el tiempo que se determine necesario para la estabilización del Sistema de Prevención de Intrusos (nueva generación / NGIPS).
- Se deberán migrar la configuración y las políticas de seguridad desde el sistema actual al nuevo Sistema de Prevención de Intrusos (nueva generación / NGIPS).
- Personal técnico especializado del fabricante del software del Sistema de Prevención de Intrusos (nueva generación / NGIPS), deberá asistir al Proveedor en todos los procesos de la migración, validación, depuración, optimización y afinamiento de las configuraciones, arquitectura y políticas de seguridad del sistema nuevo.
- Personal técnico especializado del fabricante del software del Sistema de Prevención de Intrusos (nueva generación / NGIPS), deberá asistir al Proveedor en la verificación de que problemas o errores de configuración, de desempeño, o de seguridad del sistema actual no se hereden al nuevo sistema.
- Por al menos dos días laborales personal técnico especializado del fabricante del software del Sistema de Prevención de Intrusos (nueva generación / NGIPS) deberá participar en sitio en la migración hacia el nuevo sistema, asistiendo al personal del proveedor a cargo de la migración y, en

coordinación con el personal de Seguridad Informática. Esta actividad no representará costos adicionales para el SRI.

- Se deberá ejecutar un diagnóstico del fabricante del software del Sistema de Prevención de Intrusos (nueva generación / NGIPS), y se deberán aplicar las correcciones o remediaciones respectivas previamente a la puesta en producción. Esta ejecución corre por cuenta del contratista.
- Se deberá realizar el afinamiento del Sistema de Prevención de Intrusos (nueva generación / NGIPS) de todos los elementos de hardware que componen la solución ofertada a conformidad del SRI, incluyendo:
    - Análisis y definición del mejor diseño que se adapte a la topología actual de la infraestructura tecnológica del SRI.
    - Acompañamiento en sitio durante el tiempo que se determine necesario para la estabilización de los elementos de hardware.
- Los horarios de migración del Sistema de Prevención de Intrusos (nueva generación / NGIPS) se acordarán con el administrador del contrato, quien será designado por el Servicio de Rentas Internas.
- El equipo de trabajo que participará en la migración del Sistema de Prevención de Intrusos (nueva generación / NGIPS) deberá disponer de todo el material de trabajo que se requiera.
- La migración del Sistema de Prevención de Intrusos (nueva generación / NGIPS) serán supervisados por personal técnico del Servicio de Rentas Internas.
- Todos los gastos incurridos en la migración del Sistema de Prevención de Intrusos (nueva generación / NGIPS), como lo son traslados, viáticos, hospedaje, etc., estarán a cargo del proveedor, el SRI no incurrirá en ningún gasto adicional.
- Se suscribirá un oficio de finalización de la etapa de migración
- El proveedor deberá entregar la memoria técnica de migración que contendrá al menos lo indicado a continuación:
    - Inventario y descripción detallada de los elementos de hardware.
    - Diseño detallado final.
    - Esquemático de conexión física final.
    - Umbrales saludables de operación (ej. CPU, RAM) referenciales.
    - Mecanismos de respaldo y de restauración de configuración.
    - Mecanismos de recuperación y de cambio de contraseñas de gestión.
    - Mecanismo de depuración de registros de eventos (logs).
    - Métodos básicos de detección y resolución de problemas (Base de Conocimientos Básica).
    - Manual de instalación del Fabricante de todos los elementos de hardware del sistema de Prevención de Intrusos de Nueva Generación NGIPS.

3.1.2 IMPLEMENTACIÓN IPS / CENTRO DE DATOS ALTERNO EN LA CIUDAD DE GUAYAQUIL

- La implementación del IPS en el Centros de Datos Alterno en la ciudad de Guayaquil deberá contar con un Plan de Implementación del Sistema de Prevención de Intrusos (nueva generación / NGIPS), contendrá al menos lo indicado a continuación:
    - Cronograma de trabajo.
    - Diseño detallado propuesto de la implementación del IPS en el Centro de Datos Alterno en la ciudad de Guayaquil.
    - Arquitectura detallada propuesta de la implementación del IPS en el Centro de Datos Alterno en la ciudad de Guayaquil.
    - Personal asignado como técnicos especialistas de soporte y mantenimiento de Sistemas de Prevención de Intrusos de Nueva Generación
- El Plan de Implementación podrá ser modificado por acuerdo entre el Administrador del contrato y contratista.
- Los trabajos de implementación en el IPS en el Centro de Datos Alterno en la ciudad de Guayaquil deberán replicar las configuraciones del IPS en el Centro de Datos Principal de la ciudad de Quito, cubrir todos los módulos y funciones del Sistema de Prevención de Intrusos (nueva generación / NGIPS).
- Se deberán migrar la configuración y las políticas de seguridad desde el sistema IPS del Centros de Datos Principal en la ciudad de Quito al Sistema de Prevención de Intrusos (nueva generación /

NGIPS) del Centro de Datos Alterno en la ciudad de Guayaquil.

- Se deberán validar, y optimizar las configuraciones de operación del software del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Alterno en la ciudad de Guayaquil, de manera que se garantice el mayor desempeño posible del nuevo sistema.
- Se deberá ejecutar un diagnóstico del fabricante del software del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Alterno en la ciudad de Guayaquil, y se deberán aplicar las correcciones o remediaciones respectivas previamente a la implementación en el Centro de Datos Alterno en la ciudad de Guayaquil.
- El contratista deberá configurar el módulo de reportería de manera que la información de los registros de eventos contenga el mayor detalle posible para que esté disponible para la generación de reportes; en función de la capacidad disponible del hardware del Sistema de Prevención de Intrusos (nueva Generación / NGIPS) en el Centros de Datos Alterno en la ciudad de Guayaquil.
- El contratista deberá configurar y probar los mecanismos de emisión de alertas (ej. Vía email) del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centros de Datos Alterno en la ciudad de Guayaquil.
- El contratista deberá ofrecer acompañamiento en sitio durante el tiempo que se determine necesario para la estabilización del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Alterno en la ciudad de Guayaquil.
- Personal técnico especializado del fabricante del software del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Alterno en la ciudad de Guayaquil, deberá asistir al Proveedor en todos los procesos de implementación, migración de configuración, validación, depuración, optimización y afinamiento de las configuraciones, arquitectura y políticas de seguridad del sistema nuevo.
- Personal técnico especializado del fabricante del software del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Alterno en la ciudad de Guayaquil, deberá asistir al Proveedor en la verificación de que problemas o errores de configuración, de desempeño, o de seguridad del sistema actual no se hereden al nuevo sistema.
- Por al menos dos días laborables personal técnico especializado del fabricante del software del Sistema de Prevención de Intrusos (nueva generación / NGIPS), deberá participar en el Centro de Datos Alterno en la ciudad de Guayaquil en la implementación, migración de configuraciones, validación, depuración, y afinamiento de las configuraciones, arquitectura asistiendo al personal del proveedor a cargo y, en coordinación con el personal de Seguridad Informática. Esta actividad no representará costos adicionales para el SRI.
- Se deberá realizar el afinamiento del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Alterno en la ciudad de Guayaquil de todos los elementos de hardware que componen la solución ofertada a conformidad del SRI, incluyendo:
    - Análisis y definición del mejor diseño que se adapte a la topología y direccionamiento de la infraestructura tecnológica del SRI de Guayaquil.
    - Acompañamiento en sitio durante el tiempo que se determine necesario para la estabilización de los elementos de hardware.
    - Los horarios de implementación del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Alterno en la ciudad de Guayaquil, se acordarán con el administrador del contrato, quien será designado por el Servicio de Rentas Internas.
    - El equipo de trabajo que participará en la implementación del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Alterno en la ciudad de Guayaquil, deberá disponer de todo el material de trabajo que se requiera.
    - La implementación del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Alterno en la ciudad de Guayaquil, serán prestados de acuerdo a lo definido por el administrador del contrato y supervisados por personal técnico del Servicio de Rentas Internas.
    - Todos los gastos incurridos en la implementación del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Alterno en la ciudad de Guayaquil, como traslados, viáticos, hospedaje, etc., estarán a cargo del proveedor, el SRI no incurrirá en ningún gasto adicional.
- El proveedor deberá entregar la memoria técnica de implementación del Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Alterno de la ciudad de Guayaquil, que

contendrá al menos lo indicado a continuación:

- Inventario y descripción detallada de los elementos de hardware.
- Diseño detallado final.
- Esquemático de conexión física final.
- Umbrales saludables de operación (ej. CPU, RAM) referenciales.
- Mecanismos de respaldo y de restauración de configuración.
- Mecanismos de recuperación y de cambio de contraseñas de gestión.
- Mecanismo de depuración de registros de eventos (logs).
- Métodos básicos de detección y resolución de problemas (Base de Conocimientos Básica).
- Manual de instalación del Fabricante de todos los elementos de hardware del sistema de Prevención de Intrusos de Nueva Generación NGIPS - GYE.

El nuevo Sistema de Prevención de Intrusos (nueva generación / NGIPS) en el Centro de Datos Alterno en la ciudad de Guayaquil deberá quedar completamente operativo a satisfacción del SRI.

Finalizada la etapa de migración e implementación se suscribirá un oficio de constancia de fechas de finalización de las actividades tanto de MIGRACIÓN NGIPS / CENTRO DE DATOS PRINCIPAL EN LA CIUDAD DE QUITO como de IMPLEMENTACIÓN IPS / CENTRO DE DATOS ALTERNO EN LA CIUDAD DE GUAYAQUIL

3.2 TRANSFERENCIA DE CONOCIMIENTOS

La transferencia de conocimiento sobre temas relacionados al sistema a ser implementado deberá incluir:

- La transferencia de conocimientos del Sistema de Prevención de Intrusos (nueva generación / NGIPS) debe ser de al menos 20 horas, y para al menos 8 personas, e incluir al menos los siguientes temas generales:
  - Arquitectura de la solución de prevención de intrusos de nueva generación
  - Administración de la solución de prevención de intrusos de nueva generación
  - Gestión de Políticas de seguridad
  - Mejores Prácticas
  - Respaldos de configuración
  - Detección y Resolución de problemas y afinamiento de la solución.
  - Generación y personalización de reportes, que el SRI indique que son necesarios en su gestión de la solución de prevención de intrusos de nueva generación NGIPS.

- La transferencia de conocimiento deberá incluir los materiales, laboratorios virtuales con tecnología similar al sistema instalado, equipos, enlace de internet dedicado y talleres necesarios para la correcta asimilación del contenido y la generación de las destrezas necesarias en los asistentes. Deberá estar desarrollada sobre la última versión disponible del Fabricante del Sistema de Prevención de Intrusos (nueva generación / NGIPS).
- La transferencia de conocimiento se deberá realizar de forma presencial en las instalaciones provistas por el contratista o el fabricante.

3.3 MANTENIMIENTO CORRECTIVO

- El mantenimiento correctivo debe tener una disponibilidad de 7x24 de lunes a domingo, las 24 horas del día.
- Los trabajos generados por un requerimiento podrán llevarse a cabo en horario normal, fuera de horario laboral, fines de semana, feriados; sin costo adicional para a el SRI.
- Los trabajos generados por un requerimiento podrán ser en sitio o remoto según sea el requerimiento expreso del SRI.
- El servicio de mantenimiento correctivo cubre la operación integral del Sistema de Prevención de Intrusos (nueva generación / NGIPS), incluyendo tanto el hardware como el software del mismo, y

tanto aspectos de operación como de seguridad informática.

- Se trabajará en base a requerimientos de atención (o casos de soporte), los cuales serán registrados con el contratista local, para su resolución cumpliendo con el Acuerdo de Nivel de Servicio establecidos. El administrador del contrato informará el listado del personal del SRI que podrá solicitar soporte
- En caso de controversia sobre la prioridad de un requerimiento de soporte técnico, prevalecerá el criterio del SRI.
- El contratista deberá entregar el procedimiento al Administrador del Contrato (designado por el contratante), mediante oficio o correo electrónico, del detalle de los canales de comunicación disponibles y el procedimiento para la apertura de casos y el ingreso de requerimientos tanto con el fabricante como con el proveedor, siendo obligatorios el medio telefónico, el correo electrónico y un portal de gestión de requerimientos tecnológicos (ITSM).
- La atención de los casos deberá ser llevada a cabo en sitio o en forma remota, donde el personal del SRI indique.
- Una vez iniciados los trabajos en sitio, el contratista deberá garantizar la permanencia del equipo técnico necesario durante el tiempo que sea requerido para que se solucione el incidente y el sistema regrese a un estado de operación normal o aceptable para el SRI, 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.
- Se aceptará el cierre de un caso únicamente cuando se haya determinado y se haya aplicado una solución definitiva al evento reportado.
- Si para el análisis de un caso 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 contratista es el único responsable de realizar todas las acciones que sean necesarias, para obtener esta información.
- Si para el análisis se requiere abrir un caso de soporte con el fabricante, es responsabilidad del contratista 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. Sin perjuicio de este punto, el SRI debe tener contar con el acceso para poder abrir casos de soporte con del fabricante.
- En los casos 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 nuevo, según corresponda.
- La información que el contratista provea durante la gestión de los casos de soporte debe demostrar el respectivo y adecuado análisis por parte del personal técnico designado.
- En el caso de realizar trabajos de manera ininterrumpida, será responsabilidad del contratista considerar la rotación del personal con los perfiles presentados en la oferta para descanso, con el objetivo de no afectar los avances en la atención del caso de acuerdo con su severidad.
- En los casos que las actividades de remediación tomen más de dos semanas, se deberá adjuntar un plan de actividades, mismo que deberá estar aprobado por parte del Administrador del Contrato.
- Al concluir la atención de cada caso, el contratista 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.

3.4 MANTENIMIENTO PREVENTIVO

- El contratista deberá realizar tres (3) visitas programadas de revisión del Sistema de Prevención de

Intrusos (nueva generación / NGIPS), una por año.

- El cronograma de mantenimientos preventivos programados a realizarse será notificado al proveedor mediante oficio firmado digitalmente por parte del administrador del contrato.
- El mantenimiento preventivo podrá llevarse a cabo en horario normal, fuera de horario laboral, fines de semana, feriados; sin costo adicional para a el SRI.
- El mantenimiento preventivo incluirá las siguientes actividades:
    - Limpieza externa de los elementos de hardware.
    - La limpieza interna debe ser incluida siempre y cuando no se pierda la garantía de los equipos con fábrica, se deben utilizar las herramientas adecuadas para evitar daños en los equipos.
    - Revisión de alertas visuales.
    - Inspección física del sitio de instalación del equipo, incluyendo sus cables y conectores.
    - Etiquetado y ordenamiento del cableado que llega a los elementos de hardware.
    - Revisar el estado de salud y el desempeño del Sistema de Prevención de Intrusos (nueva generación / NGIPS).
    - Verificar que el mecanismo de respaldos esté operando correctamente.
    - Validar la necesidad de la instalación de parches de software y hardware.
    - Instalar los parches de software y hardware recomendados por el fabricante.
    - Instalar la última versión estable recomendada por el fabricante del software y hardware.
    - Validar la necesidad de cambios en la configuración del Sistema de Prevención de Intrusos (nueva generación / NIPS).
    - Aplicar configuraciones de afinamiento de seguridad y de operación recomendadas por el fabricante de software, en caso de ser necesario.
    - Aplicar rectificaciones o mejoras.
- 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 contratista, genere la falla, o error, o degradación, o comportamiento no esperado de algún equipo que compone el Sistema de Prevención de Intrusos (nueva generación / NGIPS) o alguno de sus componentes, el contratista deberá aplicar la remediación/garantía correspondiente; sin costo adicional para el SRI, cumpliendo con el Acuerdo de Nivel de Servicio establecido.
- Al concluir cada visita y sus actividades, el contratista deberá entregar al Administrador del Contrato un informe 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 de Prevención de Intrusos (nueva generación / NGIPS);
    - Las recomendaciones de mejora en configuración, o de incremento de capacidad o mejora de diseño, en caso de ser necesario;
- Cada vez que sea requerido por el SRI, el contratista deberá elaborar y entregar la documentación correspondiente a los cambios tecnológicos que se planeen llevar a cabo en el Sistema de Prevención de Intrusos (nueva generación / NGIPS), en el formato que defina el administrador del contrato.

3.5 ACUERDOS DE NIVEL DE SERVICIO

Severidad

La severidad del caso registrado será establecida entre el SRI y el contratista, categorizando el problema con niveles de prioridad con el siguiente criterio:

PRIORIDAD	MANTENIMIENTO CORRECTIVO	SEGURIDAD INFORMATICA	REEMPLAZO DE HARDWARE
1	• Alarma, avería, fallo, o error de uno de los componentes del Sistema de Prevención de Intrusos (nueva generación / NGIPS) de Producción. • Inhibición completa o parcial de uno de los componentes del Sistema de Prevención de Intrusos (nueva generación / NGIPS) de Producción. • Indisponibilidad o degradación o alguna afectación de los servicios tecnológicos de Producción del SRI que dependen del Sistema de Prevención de Intrusos (nueva generación / NGIPS) • Corrupción o pérdida de datos del sistema (ej. registros de eventos, registros de auditoría, archivos de políticas, archivos de configuración, etc.). • Atención de alarmas que indiquen una condición grave del Sistema de Prevención de Intrusos (nueva generación / NGIPS) de Producción. • Solicitudes de asistencia asociadas a servicios tecnológicos de Producción del SRI protegidos por el Sistema de	• Incidentes de Seguridad Informática que afecten o que estén asociados a los servicios tecnológicos de Producción del SRI protegidos por el Sistema de Prevención de Intrusos (nueva generación / NGIPS). • Alarmas de Seguridad Informática del Sistema de Prevención de Intrusos (nueva generación / NGIPS).	• Aplicación de garantía técnica que requiere el reemplazo de alguna parte, pieza, o el equipo completo del Sistema de Prevención de Intrusos (nueva generación / NGIPS) de Producción.

	Prevención de Intrusos (nueva generación / NGIPS).		
2	• Alarma, avería, fallo, o error de uno de los componentes del Sistema de Prevención de Intrusos (nueva generación / NGIPS) de Contingencia. • Inhibición completa o parcial de uno de los componentes del Sistema de Prevención de Intrusos (nueva generación / NGIPS) de Contingencia. • Indisponibilidad o degradación de los servicios tecnológicos del SRI que no son de Producción y que dependen del Sistema de Prevención de Intrusos (nueva generación / NGIPS). • Si los componentes del Sistema de Prevención de Intrusos (nueva generación / NGIPS) están operando con funcionalidad reducida o limitada, sin afectar a los servicios tecnológicos de Producción del SRI.	• Incidentes de Seguridad Informática que afecten parcialmente a servicios tecnológicos del SRI protegidos por el Sistema de Prevención de Intrusos (nueva generación). • Revisión, monitoreo y afinamiento del Sistema de Prevención de Intrusos (nueva generación / NGIPS) cuando el personal del SRI reporte la existencia de incidentes de seguridad informática o de problemas de seguridad informática asociados al sistema en sí, o a servicios tecnológicos que dependan del mismo.	• Aplicación de garantía técnica que requiere el reemplazo de alguna parte o pieza, o de equipo del Sistema de Prevención de Intrusos (nueva generación / NGIPS) de Contingencia.
3	• Advertencias ("warnings") del Sistema de Prevención de Intrusos (nueva generación / NGIPS) que no estén	• Advertencias ("warnings") de Seguridad Informática del Sistema de Prevención de Intrusos (nueva	• No aplica.

	causando ninguna indisponibilidad o degradación del mismo sistema ni de los servicios tecnológicos del SRI que dependen de éste. • Solicitudes de asistencia asociadas a servicios tecnológicos del SRI que no son de Producción y que están protegidos por el Sistema de Prevención de Intrusos (nueva generación / NGIPS) • Solicitudes de información acerca de nuevas versiones disponibles • Planificación de trabajados relacionados con el sistema • Reportes e informes bajo demanda de diagnóstico del sistema, o de algún evento particular relacionado con el sistema • Requerimientos para afinamiento del sistema • Solicitudes de información de diagnóstico obtenida previamente. • Consultas bajo demanda sobre la arquitectura implementada, diseño, funcionamiento y configuración de la infraestructura implementada • Afinamiento de la	generación / NGIPS).	

	arquitectura, del diseño, de la topología, personalización, operación del Sistema de Prevención de Intrusos (nueva generación / NGIPS), así como la documentación asociada. • Diagnóstico “HEALTH CHECK” del sistema cada vez que el personal del SRI lo solicite, o en las visitas de revisión para verificar el estado de salud de los equipos o software del Sistema de Prevención de Intrusos (nueva generación / NGIPS).		

Descripción de los niveles de prioridad del ACUERDO DE NIVEL DE SERVICIO.

- Tabla de Tiempos de Respuesta y Reemplazo de Partes y Piezas. El tiempo está medido en horas consecutivas:

Prioridad	Mantenimiento Correctivo / Seguridad Informática	Reemplazo de Hardware
1	1 hora	4 horas partes y piezas, 12 horas cambio de equipo
2	2 horas	8 horas laborables
3	4 horas	N/A

- El tiempo de respuesta se define como el lapso entre el momento en que el SRI hace la solicitud y el momento en que se inicia del análisis técnico por parte del ingeniero especialista designado a dicho requerimiento en conjunto con el personal del SRI. La notificación informativa de recepción del requerimiento no es aceptada como el inicio

del análisis técnico.

- El tiempo de reemplazo de Hardware se define como el lapso desde que se diagnostica como causa la falla y la necesidad de reemplazo de partes o piezas hasta el momento en que se presenta el contratista con el ítem nuevo de reemplazo definitivo, y se recupera la operación normal. Aplica al Reemplazo de Partes y Piezas. En caso de reemplazo del equipo, se acepta la instalación de un equipo provisional hasta la llegada del definitivo siempre y cuando el provisional sea de iguales o mejores características que el equipo ofertado. Para los requerimientos o casos de soporte de garantía técnica, mantenimiento correctivo, el personal técnico del contratista debe acercarse a sitio o ejecutarlo de manera remota, donde el personal del SRI indique para proceder con la atención.

4. PLAZO DE EJECUCIÓN

El plazo de ejecución de este contrato será de hasta 1184 días calendario contados a partir del día siguiente hábil de la notificación del administrador del contrato.

BIENES REQUERIDOS

- El plazo para la entrega e instalación de los bienes en el Centro de Datos Principal de la ciudad de Quito, y en el Centro de Datos Alterno de la ciudad de Guayaquil será de hasta 90 días contados a partir de la notificación del administrador del contrato.
- La Memoria Técnica de instalación deberá ser entregada en un plazo de hasta 15 días calendario desde el día siguiente hábil a la instalación de los bienes.
- El plazo de la vigencia de la garantía técnica y del soporte de fábrica será de 1095 días contados a partir de la instalación de los bienes.

SERVICIOS CONEXOS REQUERIDOS

- El Plan de Migración y el Plan de Implementación deberán ser entregados en un plazo de hasta 30 días calendario contados a partir de la notificación del administrador del contrato.
- El plazo de entrega para el servicio de Migración e Implementación al Sistema de Prevención de Intrusos (nueva generación / NGIPS) será de hasta 45 días calendario contados a partir del día siguiente hábil al plazo de entrega e instalación de los bienes.
- La Transferencia de conocimientos del Sistema de Prevención de Intrusos (nueva generación / NGIPS), deberá ser entregado en un plazo de hasta 15 días calendario desde el siguiente día hábil a la finalización del servicio de Migración e Implementación.
- El plazo de la vigencia del mantenimiento preventivo y correctivo será de 1095 días contados a partir de la instalación de los bienes.
- El plazo de entrega del procedimiento de apertura, seguimiento, escalamiento y cierre de casos con el proveedor y fabricante deberá ser entregado en un plazo de hasta 15 días calendario contados a partir del día siguiente hábil a la entrega e instalación de los bienes.
- El plazo de entrega del informe consolidado de los casos atendidos será de hasta 10 días hábiles después de finalizado cada período de soporte (anual).
- El plazo de entrega de los informes de mantenimiento preventivo será de hasta 10

días hábiles contados a partir del día siguiente de concluido el mantenimiento.

5. FORMA Y CONDICIONES DE PAGO

Elementos de hardware, instalación y garantía técnica: El 100% de este rubro se pagará contra entrega a satisfacción del SRI, previa presentación de la planilla de pago y la suscripción del Acta de Entrega Recepción correspondiente.

Para la suscripción del Acta de Entrega Recepción correspondiente a los elementos de hardware, instalación y garantía técnica, deberá entregar, mediante oficio dirigido al Administrador del Contrato, la siguiente documentación:

- Documento de garantía técnica con vigencia de 1095 días
- La guía de acceso y uso del portal y/o interfaz de gestión
- La guía de escalamiento de casos con el fabricante

Migración, Implementación del Sistema de Prevención de Intrusos y transferencia de conocimientos: El 100% de este rubro se pagará contra entrega a satisfacción del SRI, previa presentación de la planilla de pago, y la suscripción del Acta de Entrega Recepción correspondiente.

Para la suscripción del Acta de Entrega Recepción parcial correspondiente a la Migración, Implementación y transferencia de conocimientos, el contratista deberá entregar, mediante oficio dirigido al Administrador del Contrato, la siguiente documentación:

- Oficio de constancia de finalización de la migración e implementación.
- La memoria técnica de la migración del Sistema de Prevención de Intrusos en el Centro de Datos Principal en la ciudad de Quito, con el detalle de todas las actividades realizadas y el detalle de los productos implementados.
- La memoria técnica de la implementación del Sistema de Prevención de Intrusos en el Centro de Datos Alterno en la ciudad de Guayaquil, con el detalle de todas las actividades realizadas y el detalle de los productos implementados.
- La lista de asistencia a la transferencia de conocimiento debidamente firmada.

Mantenimiento preventivo, mantenimiento correctivo del Sistema de Prevención de Intrusos de Nueva Generación NGIPS: El pago del servicio se realizará anualmente. Para estos pagos se requerirá la presentación de la planilla de pago y la suscripción del Acta de Entrega Recepción correspondiente.

Para la suscripción del Acta de Entrega Recepción Parcial el contratista deberá entregar mediante oficio al Administrador de contrato:

- Los Informes de Mantenimiento Preventivo por cada mantenimiento realizado.
- El Informe Consolidado de los casos de soporte atendidos, que contenga los siguientes campos por cada caso reportado:
  - ✓ La fecha y hora;
  - ✓ Descripción del problema o solicitud (Explicar claramente cuál es el problema

o la solicitud que necesita atención. Proporcionar detalles específicos, como mensajes de error, comportamientos inesperados, etc.).
- ✓ Prioridad y nivel de severidad.
- ✓ Número de ticket o referencia anterior, si corresponde.
- ✓ Los resultados de las actividades de revisión y de diagnóstico llevadas a cabo;
- ✓ Un análisis de salud de la solución basado en la información de diagnóstico obtenida;
- ✓ El listado de actualizaciones de software de punto final instaladas, de ser el caso;
- ✓ Los cambios de configuración y afinamiento aplicados, de ser el caso;
- ✓ Los hallazgos relevantes, en caso de haberlos;
- ✓ Solución aplicada;
- ✓ Las recomendaciones de mejora en configuración, en caso de ser necesario;

6. LUGAR DE ENTREGA

- Los equipos, instalación, implementación /migración, el servicio de mantenimiento y las actividades de garantía técnica deben entregarse en el Centro de Datos de Principal del SRI, ubicado en la ciudad de Quito, calles Páez 657 y Ramírez Dávalos, edificio CODIGEN, segundo piso.
- Los equipos, instalación, implementación, el servicio de mantenimiento y las actividades de garantía técnica deben entregarse en el Centro de Datos de Alterno del SRI, ubicado en la ciudad de Guayaquil, av. Francisco de Orellana y Justino Cornejo, edificio World Trace Center (WTC), Torre C, quinto piso.
- Los servicios de garantía técnica que no requieran intervención directa sobre los equipos deben entregarse en la ciudad de Quito, av. Amazonas entre Unión Nacional de Periodistas y Pereira, Plataforma Gubernamental de Gestión Financiera, Bloque 5 (Azul), piso 1; o donde señale el Administrador del Contrato designado por el Comprador.
- En caso de cambio en la dirección especificada anteriormente, el Administrador del Contrato informará mediante oficio al proveedor la nueva dirección.