CONVOCATORIA PARA LA ELABORACIÓN DEL ESTUDIO DE MERCADO

El Servicio de Rentas Internas (SRI), convoca a proveedores nacionales e internacionales a participar en el proceso de elaboración del Estudio de Mercado para la **"ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD DE BASE DE DATOS".**

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 hasta mil doscientos cincuenta y cinco (1255) días calendario contados a partir del día siguiente laborable de la suscripción del contrato.

Las cotizaciones deben ser remitidas en formato digital (firmadas), al correo institucional programaintax@sri.gob.ec hasta el día 26 de abril 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: (se solicita incluir CPC 452800041 en la cotización)

DESGLOSE DE COMPONENTES					
Ítem	Tipo de recurso	Descripción	Cantidad	Precio unitario (USD)	Precio Total (USD)

1	Hardware / Software	Solución de seguridad de base de datos	Definida por el oferente.		
2	Hardware / Software	Consola de administración	Definida por el oferente.		
3	Garantía Técnica	GARANTÍA TÉCNICA (INCLUYE MANTENIMIENTO CORRECTIVO POR DEFECTOS DE FÁBRICA) Garantía técnica de todos los bienes ofertados por 3 años	1		
SERVICIOS CONEXOS					
4	Servicios	Implementación/Migración y Transferencia de Conocimientos	1		
5	Servicios	Mantenimiento preventivo	6		
				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 TÉCNICAS

1. INFRAESTRUCTURA ACTUAL

La solución de seguridad de base de datos (sistema de firewall de base de datos – DBF) actualmente implementada en los ambientes de: producción, contingencia, preproducción y testing, se compone de tres (3) equipos físicos tipo appliance marca *IMPERVA* modelo X4500, que incluye software propietario del fabricante; y un (1) equipo físico marca *IMPERVA* modelo *M150* correspondiente a la consola de gestión.

La tabla a continuación detalla los equipos informáticos que componen la infraestructura de hardware del actual sistema de firewalls de base de datos (DBF):

Ítem Nro.	Equipo	Marca	Modelo	Interfaces de red	Throughput	Ubicación física
1	Consola	IMPERVA	M150			Centro de Datos Principal – Quito.
2	Gateway	IMPERVA	X4500	Tiene dos (2) interfaces Ethernet 1Gbps para administración y cuatro (4) interfaces de 10Gbps para tráfico de base de datos	1 GB 9.600 TPS	Centro de Datos Principal – Quito.
3	Gateway	IMPERVA	X4500	Tiene dos (2) interfaces Ethernet 1Gbps para administración y cuatro (4) interfaces de 10Gbps para tráfico de base de datos	1 GB 9.600 TPS	Centro de Datos Principal – Quito.
4	Gateway	IMPERVA	X4500	Tiene dos (2) interfaces Ethernet 1Gbps para administración y ocho (8) interfaces 1Gbps para tráfico de base de datos.	1 GB 9.600 TPS	Centro de Datos Alterno – Guayaquil.

Tabla 1. Detalle de los equipos servidores que conforman el actual sistema de firewalls de base de datos (DBF) del SRI.

La garantía técnica de fábrica de este hardware estuvo vigente hasta el 15 de abril de 2020; los equipos a la fecha están obsoletos.

Cada firewall de base de datos (DBF) protege diferentes bases de datos en ambientes productivo, contingencia, preproducción y testing, por lo tanto, tiene distintos roles de seguridad. La tabla a continuación describe las funciones de cada componente del actual sistema de firewall de base de datos (DBF) del SRI:

Ambientes	Cant. Equipos	Base de Datos protegidas	Ubicación física
Producción Intranet.	1 GATEWAY	• Transaccional. • Componentes de Infraestructura. • Analítica.	Centro de Datos Principal – Quito.
Producción Internet.	1 GATEWAY	• Facturación Electrónica. • Transaccional • Frontera.	Centro de Datos Principal – Quito.
Contingencia. Preproducción y Testing.	1 GATEWAY	• Contingencia. • Preproducción. • Test.	Centro de Datos Alterno – Guayaquil.

Tabla 2. Gateways físicos que conforman el sistema firewall de base de datos (DBF) del SRI.

Con corte a marzo del 2024, la situación actual de capacidad de los servidores físicos de la infraestructura de base de datos es la siguiente:

Centro de Datos Principal

MARCA	MODELO	RACK	CORES INSTALADOS	CORES ACTIVADOS
ORACLE	SPARC M12-2S	Fujistsu Rack 1	24	24
ORACLE	SPARC M12-2S		24	24
ORACLE	SPARC M12-2S	Fujistsu Rack 2	24	24
ORACLE	SPARC M12-2S		24	24
TOTAL			**96**	**96**

Tabla 3. Información capacidad de bases de datos institucionales actual Centro de Datos Principal

Centro de Datos Alterno

MARCA	MODELO	RACK	CORES INSTALADOS	CORES ACTIVADOS
ORACLE	SPARC M12-2S	Fujistsu Rack 1	24	24
ORACLE	SPARC M12-2S		24	24
			48	48

Tabla 4. Información capacidad de bases de datos institucionales actual Centro de Datos Alterno

Las bases de datos de producción, contingencia y preproducción se encuentran instaladas en servidores SPARC M12-2S, con sistema operativo Oracle Solaris; y con hipervisor Solaris 11.4.60.151.2.

El motor de las bases de datos es Oracle con las siguientes versiones:

Ambientes	Ambiente Bases de Datos	11 G	12 C	19 C	Total servidores virtuales
Producción Internet	Base de datos externa	2	2	4	8
Producción Intranet	Base de datos interna	5	4	4	13
Contingencia Preproducción y Testing	Contingencia	4	2	3	9
	Preproducción	4	3	7	14
	Testing	3	2	1	6
Total servidores		**17**	**13**	**20**	**50**

Tabla 5. Motor de Base de Datos.

En las siguientes tablas se presentan los controles (políticas de seguridad, políticas de auditoría y reportería) creados en la actual solución de seguridad de bases de datos (sistema de firewall de base de datos – database firewall DBF):

Ambiente Bases de Datos	Política de Seguridad	Política de Auditoría	Reportería
Base de datos externa	66	17	10
Base de datos interna	26	35	86
Preproducción	20	24	14
Total general	112	76	110

Tabla 6. Cantidad de reglas de la política de seguridad y auditoría de la solución de seguridad de base de datos, a marzo 2024

Objetos	Objetos Totales

Grupos de correo destinatarios de reportería	35
IP group	15
IP group administradores	13
Sensitive Data Dictionary Group	13
Objetos Totales	**76**

Tablas 7. Cantidad de objetos definidos en la solución actual de seguridad de base de datos, a marzo 2024.

De acuerdo con la documentación del Plan de capacidad 2023-2027 del SRI, se estima que la solución de seguridad de base de datos estará alineada al crecimiento de cores de base de datos proyectada para el año 2027, como se indica a continuación:

Ambiente	Cores - 2025	Cores - 2026	Cores - 2027
CONTINGENCIA	12	12	12
PREPRODUCCIÓN	21	21	21
PRODUCCIÓN	88	96	105
Total general	**121**	**129**	**138**

Tablas 8. Proyección de cores al 2027

2. BIENES REQUERIDOS

Los siguientes puntos detallan las características que debe cumplir la solución ofertada tanto para el Centro de Datos Principal en la ciudad de Quito, así como para el Centro de Datos Alterno en la ciudad de Guayaquil:

2.1 COMPONENTES DE INFRAESTRUCTURA

	1. CARACTERÍSTICAS GENERALES
1.1	La infraestructura de la solución de seguridad de base de datos (sistema de firewall de base de datos –DBF) debe estar conformado para la instalación en equipamiento de hardware o en máquinas virtuales para el Centro de Datos Principal en la ciudad de Quito y para el Centro de Datos Alterno en la ciudad de Guayaquil.
1.2	Si la solución ofertada es virtual, el oferente deberá proveer los recursos de infraestructura necesarios para desplegar la solución en infraestructura del SRI.
1.3	La solución ofertada debe ser fabricada al menos en el año 2023. El período de vigencia tecnológica debe ser de al menos 3 años, con la posibilidad de ampliar su garantía técnica del fabricante por al menos 2 años adicionales.
1.4	El oferente debe garantizar que los equipos del sistema de firewall de base de datos (DBF) ofertado no entre en EOST (“End-of-Support”) o en EOL (“End-of-Life”) durante los 5 años posteriores a la suscripción del contrato.
1.5	Contar con el hardware y software compatible y necesario para el correcto funcionamiento de la solución ofertada.
1.6	Los sistemas de firewall de base de datos (DBF) en ambientes productivos en el Centro de Datos Principal (Quito), y contingencia, preproducción y testing en el Centro de Datos Alterno (Guayaquil), deben tener visibilidad sobre el tráfico de base de datos, por medio de componentes de hardware o virtuales que permitan analizar el tráfico en línea.
1.7	Los sistemas de firewall de base de datos (DBF) (Centro de Datos Principal Quito, Centro de Datos Alterno Guayaquil) deben incluir el software propio del fabricante, y el licenciamiento necesario.
1.8	El sistema de firewall de base de datos (DBF) no debe ser intrusiva a nivel de base de datos, evitando así la afectación en el desempeño de las bases de datos monitoreadas por la solución, para ello se

1. CARACTERÍSTICAS GENERALES	
	define los siguientes casos: ○ Configurar la solución en modo que la transaccionalidad ingrese directa al sistema de firewall de base de datos antes de ingresar a las bases de datos institucionales, o, ○ Configurar la solución con instalación de agentes en los servidores de bases de datos. En este caso, se considerará el umbral de consumo de procesamiento definido por la institución de hasta un 5%, y para evitar que se supere el umbral, será obligatorio configurar que el servicio de la solución de firewall de base de datos (agente) sea deshabilitado automáticamente al superar el umbral definido por la entidad.
1.9	El sistema de firewall de base de datos (DBF) debe trabajar de forma independiente a la activación de la auditoría nativa de la base de datos, es decir, no requiere la activación de logs de auditoría propios de la base de datos que monitorea, así como evitar degradación o afectación en el desempeño de las bases de datos monitoreadas por la solución.
1.10	El sistema de firewall de base de datos (DBF) debe incluir mecanismos de protección automática en caso de falla diseñada para soportar un esquema de alta disponibilidad, permitiendo de esta manera la continuidad del servicio, sin afectar las transacciones hacia y desde las bases de datos de producción, contingencia, preproducción y testing.
1.11	El sistema de firewall de base de datos (DBF) debe ser compatible al menos con los sistemas que dispone la institución: ○ Vmware versión 6.5.0 o superior (máquinas virtuales) ○ Windows Server 2016 o superior ○ Oracle Solaris 11.4 o superior ○ Exchange Server 2019 o superior (para alertas de la solución de seguridad de base de datos). ○ Motor de base de datos Oracle, versiones 11g, 12c, 19c o superior.
1.12	El sistema de firewall de base de datos (DBF) debe soportar la gestión de seguridades sobre las principales bases de datos institucionales con las versiones y sistema operativo que dispone la institución.
1.13	El sistema de firewall de base de datos (DBF) debe trabajar de forma transparente a las actividades en las bases de datos y/o aplicaciones que accedan a ella, sin requerir la implementación de cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
1.14	La información capturada por el sistema de firewall de base datos (DBF) debe estar cifrada.
1.15	El sistema de firewall de base de datos (DBF) debe incluir esquemas y política de respaldo para toda la información que se administra dentro de dicha solución (base de datos de la información originada en el monitoreo y control, así como del software de funcionamiento).
1.16	El sistema de firewall de base de datos (DBF) debe permitir implementar auditoría de control sobre sí misma, manteniendo un control de cambios sobre las políticas y configuraciones ejecutadas en la solución.
1.17	Notificar mediante alertas visuales o correo electrónico cuando existan nuevas versiones o releases de cualquier componente que conforma la solución.
1.18	Se deberá suministrar un acceso vía web al portal del fabricante para revisar el estado del licenciamiento, información de nuevas versiones, actualizaciones, ingresos y seguimiento de casos de soporte.
1.19	Se deberá tener derecho de uso de nuevas versiones de software, hotfix, parches, durante la vigencia del licenciamiento del sistema de firewall de base de datos (DBF).
1.20	Se tendrá derecho a actualizaciones de nuevas versiones del software para el sistema de firewall de base de datos (DBF) sin costo adicional para el SRI durante la vigencia del licenciamiento. El contratista será quien realice las actualizaciones, migraciones bajo la coordinación del Administrador de Contrato.
1.21	El licenciamiento será provisto con soporte ilimitado del fabricante por tres (3) años (1095 días)

1. CARACTERÍSTICAS GENERALES	
	calendario, contados a partir de la fecha de activación.
	MONTAJE DE LOS EQUIPOS
1.22	Los elementos de hardware deben ser servidores de bastidor (“rack-mounted servers”) y deben poderse montar en bastidores (“racks”) de diecinueve pulgadas - 19” y ocupar un espacio que no supere dos (2) RU (Rack Unit).
1.23	Los elementos de hardware deben contar con los rieles, sujetadores y demás accesorios necesarios para un montaje seguro y organizado en los centros de datos Principal (Quito) y Alterno (Guayaquil) del Servicio de Rentas Internas (SRI).

2. CARACTERÍSTICAS DE LA SOLUCIÓN DE SEGURIDAD DE BASE DE DATOS (SISTEMA FIREWALL DE BASE DE DATOS - DBF)	
2.1	Los equipos del sistema de firewall de base de datos (DBF) para el Centro de Datos Principal en la ciudad de Quito y para el Centro de Datos Alterno en la ciudad de Guayaquil deben tener, al menos: ○ Dos (2) interfaces Ethernet 1Gbps para administración. ○ Se deben incluir todos los componentes de conectividad para que el sistema de firewall de base de datos quede conectado de forma redundante a la red LAN Ethernet del SRI al menos a 25 Gbps. Incluir los transceivers para conectarse a los switches Ethernet del SRI. ○ En caso de falla total de (los) equipo(s) que soporta(n) la solución de seguridad de base de datos, se debe prever un mecanismo alterno que permita el tráfico hacia las bases de datos y no genere bloqueo mientras se reestablece la solución de seguridad de base de datos (sistema de firewall de base d datos – DBF). ○ La solución debe permitir la configuración de bypass lógico, con la opción de suspender el bloqueo y/o auditoría en el momento que se requiera, sin afectar el tráfico sql de las bases de datos que se están monitoreando. ○ Fuente de poder y discos duro redundante. ○ Almacenamiento interno para alojar la solución y/o capacidad de soportar auditoría en línea de al menos tres (3) meses.
2.2	El sistema firewall de base de datos (DBF) deberá tener suficiente capacidad instalada para poder monitorear, auditar y asegurar las bases de datos actuales y futuros crecimientos de la plataforma del SRI, en tal sentido como mínimo el sistema de firewall de base de datos (DBF) suministrado deberá cumplir con las siguientes características de desempeño y activadas desde el momento cero en que entren a producción: **Centro de Datos Principal Quito:** Capacidad de procesar tráfico de dos (2) Gbps (21.600 tps), o la auditoría que producen ciento cinco (105) cores de base de datos. **Centro de Datos Alterno Guayaquil:** Capacidad de procesar tráfico de dos (2) Gbps (21.600 tps), o la auditoría que producen treinta y tres (33) cores de base de datos. En caso de que se active los Planes de Continuidad del Servicio de Rentas Internas, el proveedor deberá garantizar que el ambiente de contingencia de la solución de seguridad de base de datos debe permitir configurarse en modo by pass, para evitar degradación o afectación en el desempeño de las bases de datos de contingencia monitoreadas.
2.3	Los equipos del sistema de firewall de base de datos (DBF) deben poder ser monitoreados por SNMP.
2.4	Los equipos del sistema de firewall de base de datos (DBF) deben cumplir con las siguientes funcionalidades: ○ Tener visibilidad sobre el tráfico SQL, 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.

2. CARACTERÍSTICAS DE LA SOLUCIÓN DE SEGURIDAD DE BASE DE DATOS (SISTEMA FIREWALL DE BASE DE DATOS - DBF)
○ Soportar sincronización de tiempo a través de NTP. ○ Integrarse con Active Directory al menos versión Windows Server 2019, para reconocer usuarios del dominio para el acceso a los equipos que conforman la solución ofertada. ○ 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. ○ Proteger ante vulnerabilidades conocidas, donde se proteja el tráfico cuyo patrón obedezca al menos a vulnerabilidades conocidas tipo CVE.

3. CARACTERÍSTICAS CONSOLA DE ADMINISTRACIÓN
La solución de seguridad de base de datos (sistema de firewall de base de datos –DBF) debe contar con una consola de administración centralizada para el Centro de Datos Principal Quito, la cual tendrá las siguientes características o funcionalidades: 3.1 La consola de administración de la solución puede ser física o virtualizada. 3.2 Debe incluir el software propio del fabricante y el licenciamiento necesario. 3.3 En caso de que la consola de administración sea un equipo físico de hardware, el oferente debe garantizar que el equipo ofertado no entre en EOST (“End-of-Support”) o en EOL (“End-of-Life”) durante los cinco (5) años posteriores a la suscripción del contrato. 3.4 Debe tener la capacidad para configurar todos los tipos de políticas de protección aplicables para los dispositivos del sistema de firewall de base de datos administrada para los Centros de Datos Principal y Alterno (Quito y Guayaquil). 3.5 Las políticas de protección para todas las bases de datos productivas, contingencia, preproducción y testing que proteja los equipos del sistema de firewall de base de datos (DBF) deben ser configurables mediante la consola de administración. 3.6 Debe tener capacidad para crear respaldos completos de configuración, eventos, logs y poder enviarlos a un servidor FTP o SCP externo del SRI. 3.7 Debe tener capacidad para gestionar las actualizaciones de todos los componentes de los dispositivos del sistema de firewalls de base de datos administrados en los centros de datos Principal y Alterno (Quito y Guayaquil). 3.8 Debe ser accesible a través de interfaz Web usando SSL y bajo línea de comando. 3.9 Debe soportar sincronización de tiempo a través de NTP. 3.10 Debe ser accesible por SNMP para tareas de monitoreo. 3.11 Debe soportar al menos SNMP v3. 3.12 La interfaz gráfica de la consola de administración del sistema de firewall de base de datos (DBF) debe permitir varios niveles de acceso incluyendo los niveles de administrador, creador de políticas, operador y auditor. 3.13 La interfaz gráfica de la consola de administración del sistema de firewall de base de datos (DBF) 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 y dirección IP desde donde lo realizó. 3.14 El repositorio del sistema de firewall de base de datos (DBF) que guarda el registro de la actividad monitoreada, no deberá ser accesible por ningún otro mecanismo que no sea la interacción mediante la interfaz gráfica (GUI) proporcionada por el fabricante o por medios administrativos debidamente asegurados. 3.15 Debe contar con un módulo de reportes incluido. Los reportes deberán mostrar datos de eventos de seguridad de al menos doce (12) meses atrás.

3. CARACTERÍSTICAS CONSOLA DE ADMINISTRACIÓN	
3.16	El fabricante debe disponer de un portal web 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.
3.17	Debe soportar al menos los siguientes exploradores: Microsoft Edge, Mozilla Firefox y Google Chrome.
3.18	Debe integrarse con Active Directory al menos versión Windows Server 2019 para la autenticación.
3.19	Debe incluir un mecanismo de integración para permitir reenviar los eventos de seguridad a un correlacionador de eventos externo.

4. CONTROLES Y GESTIÓN DE LA SEGURIDAD	
4.1	El sistema de firewall de base de datos (DBF) debe permitir la creación y actualización de reglas y políticas de seguridad de base de datos de forma manual o automática, sin modificar la configuración de las bases de datos protegidas.
4.2	El sistema de firewall de base de datos (DBF) debe permitir actualizar las políticas de seguridad de base de datos a partir de los reportes de alertas para dinamizar el proceso de toma de decisiones de seguridad.
4.3	El sistema de firewall de base de datos (DBF) debe permitir la definición de reglas y políticas de seguridad de base de datos a todo nivel, es decir, tan amplias o granulares como sea necesario.
4.4	El sistema de firewall de base de datos (DBF) debe permitir la definición de reglas y políticas de seguridad de base de datos de forma dinámica, basada en combinaciones de diversos criterios; para el efecto la solución debe incluir al menos los siguientes criterios: ○ Cantidad de registros que devuelve una consulta. ○ Cantidad de registros procesados o modificados. ○ Cantidad de Login fallidos. ○ Tipo de datos accedidos, en base a una clasificación establecida. ○ Datos definidos como sensibles y/o confidenciales. ○ Base de datos, esquema, tabla, columna. ○ Estado de autenticación de la sesión. ○ Tipo de usuario y/o grupo de usuarios que se conectaron. ○ Usuario conectado a nivel de aplicativo o sistema operativo. ○ Usuario conectado a nivel de base de datos. ○ Login y Logouts. ○ Consultas (querys) realizados. ○ IP origen e IP destino. ○ Objeto accedido. ○ Aplicación usada para el proceso de conexión a la base de datos. ○ Tiempo de respuesta o de procesamiento de la sentencia o query. ○ Errores de SQL en el manejador de base de datos. Operaciones básicas, al menos DML's (como: select, insert, update, delete, call, explain plan, lock, merge). Operaciones privilegiadas, al menos DDL (como: create, alter, drop, comment, truncate, rename) y DCL (como: grant, revoke). Registro entendible de la variable de entrada (condición where de la sentencia enviada) ○ Registro de la fecha del día y hora, minutos y segundos del evento. ○ Acción tomada. Las combinaciones a implementar con los criterios arriba detallados no están sujetas a restricción alguna.

4. CONTROLES Y GESTIÓN DE LA SEGURIDAD	
4.5	Separación de funciones para el acceso a cada una de las opciones/módulos del sistema mediante roles.
4.6	El sistema de firewall de base de datos (DBF) no debe depender de usuarios/passwords determinados por 'defecto'.
4.7	La plataforma del sistema de firewall de base de datos (DBF) debe ser endurecida (Hardening).
4.8	El sistema de firewall de base de datos (DBF) debe permitir descubrimiento de nuevas bases de datos o existentes y generación de inventarios.
4.9	Deberá contener un set de políticas y controles predefinidos para el monitoreo de actividades y estado del sistema de firewall de base de datos (DBF).
4.10	Las políticas de control predefinidas deberán tener soporte para varios estándares, entre ellos SOX, CIS, PCI, COBIT, ISO 27000, o sus equivalentes.
4.11	Permitir análisis en tiempo real para toma de acciones proactivas para determinadas transacciones definidas como no permitidas a nivel de políticas.
4.12	El sistema de firewall de base de datos (DBF) debe tener la capacidad de realizar el bloqueo de conexiones para evitar que la transacción SQL finalice exitosamente en caso de no estar autorizada.
4.13	El sistema de firewall de base de datos (DBF) debe permitir crear, borrar o modificar las reglas y políticas de seguridades de base de datos sin la necesidad de cambios en el Kernel, ni reinicio de equipos, ni reinicio de bases de datos involucradas en el cambio.
4.14	El sistema de firewall de base de datos (DBF) debe permitir la configuración de campos de tablas seleccionadas, para que sean visualizados de forma enmascarada al desplegar los resultados de consultas SQL que incluyan dichos campos, es decir se deberá enmascarar la visualización en el resultado de la consulta SQL al usuario final.
4.15	El sistema de firewall de base de datos (DBF) debe permitir monitorear y controlar la información mediante expresiones regulares y patrones.
4.16	El sistema de firewall de base de datos (DBF) debe monitorear y bloquear las transacciones de los usuarios que estén ingresados directamente en el servidor de base de datos, ya sea desde el mismo centro de procesamiento de datos mediante consola o a través de conexiones tipo terminal como ssh, o escritorio remoto.
4.17	El sistema de firewall de base de datos (DBF) debe permitir poner en cuarentena a usuarios privilegiados incluyendo a administradores de bases de datos cuando estos infrinjan una regla o política de seguridad.
4.18	El sistema de firewall de base de datos (DBF) debe permitir capturar el 100% del tamaño del script que ha afectado a la base de datos.

5. MONITOREO Y GESTIÓN DE VULNERABILIDADES	
5.1	El sistema de firewall de base de datos (DBF) debe permitir el monitoreo, análisis y auditoria, en tiempo real de las actividades realizadas por usuarios remotos, locales, aplicaciones, usuarios de aplicaciones, sobre el sistema operativo, procedimientos almacenados u otras actividades/consultas en las bases de datos definidas por el Servicio de Rentas Internas.
5.2	El sistema de firewall de base de datos (DBF) debe permitir activar bloqueos en tiempo real, a partir de alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o maliciosa de cualquier naturaleza sobre la base de datos.
5.3	El sistema de firewall de base de datos (DBF) debe permitir monitorear y auditar el tráfico encriptado hacia las Bases de Datos.
5.4	El sistema de firewall de base de datos (DBF) debe permitir identificar individualmente a los usuarios finales que interactúan con la base de datos desde las aplicaciones; incluso cuando utilizan mecanismos distintos a dichas aplicaciones para comunicarse con la base de datos. Esta capacidad no debe implicar la modificación de la aplicación y/o de la base de datos.
5.5	El sistema de firewall de base de datos (DBF) debe permitir ejecutar trabajos de análisis y auditoria

5. MONITOREO Y GESTIÓN DE VULNERABILIDADES	
	basados en eventos o alertas históricas, estos trabajos se pueden ejecutar bajo demanda y sin la necesidad de correr procesos en batch para el efecto.
5.6	El sistema de firewall de base de datos (DBF) debe contar con alarmas y notificaciones en tiempo real de la actividad de las bases de datos a fin de detectar fugas desconocidas de información, transacciones SQL no autorizadas, y ataques a los protocolos y a los sistemas en caso de producirse inyecciones SQL o ataques de DoS o DDoS.
5.7	El sistema de firewall de base de datos (DBF) debe disponer una lógica propia para el monitoreo de actividades en tiempo real, notificando al menos las siguientes situaciones: o Altos volúmenes de acceso a datos transaccionales. o Altos volúmenes de acceso a datos sensibles y/o confidenciales. o Acceso a datos inusual para cierta hora del día. o Acceso a datos desde un origen desconocido. o Acceso a datos utilizando aplicaciones o herramientas no autorizadas.
5.8	El sistema de firewall de base de datos (DBF) debe contar con análisis de vulnerabilidades sobre el software de manejo de la base de datos, protocolo de comunicación, y configuración de seguridad de los servidores que contienen bases de datos.
5.9	El análisis de vulnerabilidades debe contar con checks de verificación de: o Auditoria (comparing settings to benchmark). o Descubrimiento de puertas traseras. (opcional) o Configuración (descubrimiento de configuración no segura). o Descubrimiento de datos. o Descubrimiento de passwords por defecto. o Monitoreo de integridad (Verificación de cambios en las bases de datos). o Pruebas a nivel del OS. o Pruebas a nivel de parches. o Vulnerabilidades conocidas (sql injections, buffer overflows…). o Código vulnerable (PL/SQL, TSQL). o Detección de passwords débiles.
5.10	El sistema de firewall de base de datos (DBF) debe incluir análisis de vulnerabilidades de la infraestructura relacionada con la base de datos.
5.11	El sistema de firewall de base de datos (DBF) debe incluir la presentación y análisis periódico de inteligencia de vulnerabilidades de la tecnología relacionada a las bases de datos.
5.12	Identificar anomalías, riesgos o incidentes de usuarios y los comandos ejecutados en las bases de datos, generando un tablero de control de una Interfaz gráfica (GUI), con el detalle de cada anomalía y la razón por la que fue generada.
5.13	Identificar si un usuario de la base de datos está en riesgo de acuerdo con su criticidad y desplegado en un tablero de control dentro de una Interfaz gráfica (GUI).

6. REPORTES Y GESTIÓN DE AUDITORÍA	
6.1	El sistema de firewall de base de datos (DBF) debe permitir generar reportes y descubrir tendencias en base a la actividad y comportamiento de la base de datos, la información obtenida la entrega en tiempo real y/o programables para entrega vía correo electrónico.
6.2	El sistema de firewall de base de datos (DBF) debe incluir un completo set de reportes de auditoría listos para ser usados.
6.3	El sistema de firewall de base de datos (DBF) debe permitir la personalización de los reportes que exporte a formatos compatibles como pdf, csv, xml, html, entre otros, es decir, no habrá restricciones de uso de la información para poder generar o customizar un reporte.
6.4	El sistema de firewall de base de datos (DBF) debe contar con una herramienta para editar los

6. REPORTES Y GESTIÓN DE AUDITORÍA
reportes de forma ágil, esto es, sin la necesidad de programar código alguno. 6.5 El sistema de firewall de base de datos (DBF) debe contar con una interfaz de tipo gráfico y basada en ambiente web para el manejo y gestión de la información procesada. Para el efecto la solución debe contar con tablero de control o dashboard que permitan navegar de forma gráfica sobre la información procesada. 6.6 La interfaz del sistema de firewall de base de datos (DBF) debe permitir visualizar distintas alertas al menos del tipo falsos positivos y del tipo negativos, o incidentes de seguridad detectados. 6.7 El sistema de firewall de base de datos (DBF) debe permitir definir grupos y roles de administración para restringir la información de eventos y alertas que pueden ser visualizados por los usuarios que tienen asignados dichos roles. 6.8 El sistema de firewall de base de datos (DBF) debe permitir archivar la información histórica y de auditoría generada, para el efecto soporta distintos sistemas de almacenamiento que son cargados a través de varios medios (al menos: FTP, NFS y SCP). 6.9 El sistema de firewall de base de datos (DBF) debe incluir un informe periódico de superficie de ataque de los activos relacionados con las bases de datos. 6.10 El sistema de firewall de base de datos (DBF) debe permitir analizar los eventos detectados en las bases de datos monitoreadas teniendo en cuenta los siguientes criterios mínimos, a la hora de generar los reportes de auditoría: o Cantidad de eventos ocurridos, número de usuarios sospechosos y/o sistemas comprometidos. o Visibilidad del origen del ataque; es decir, determinar de forma clara si un ataque proviene de una dirección IP interna o externa a la organización. o Visibilidad correlacionada de los eventos detectados y su relación con las vulnerabilidades encontradas en las bases de datos monitoreadas. o Visibilidad correlacionada de los eventos detectados y asociados a todas las actividades realizadas sobre la base de datos, sin importar su origen, es decir; si el origen es a través de una aplicación, de un usuario final o de un usuario administrador con privilegios remoto o local. Para el efecto la solución no requiere modificar o alterar el código de las aplicaciones, tampoco requiere la instalación de API´s. o Visibilidad de errores en la ejecución de sentencias SQL de carácter inusual o excepcional o Visibilidad de intentos de acceso o login fallidos. o Visibilidad de actividad sobre los elementos de la base de datos catalogados como sensibles, sin importar el tipo de elemento, pudiendo ser de tipo tabla, campo, procedimiento almacenado, entre otros. o Visibilidad en tiempo real de alarmas y notificaciones.

2.2 ENTREGA E INSTALACIÓN DE LOS COMPONENTES DE INFRAESTRUCTURA

La entrega e instalación de los componentes de infraestructura deberá incluir:

- Planificación y coordinación de los trabajos de instalación e implementación;
- El contratista deberá entregar un plan de instalación de los componentes de infraestructura, en el plazo de hasta setenta y cinco (75) días calendario contados a partir del siguiente día de la firma del contrato, el mismo que deberá ser aprobado por el Administrador del Contrato designado por el SRI, en un plazo de hasta siete (7) días calendario.
- En caso de que se requiera correcciones al Plan de instalación de los componentes de infraestructura, el contratista dispondrá de hasta siete (7) días calendario posteriores a la notificación del Administrador del contrato, para enviar el Plan de instalación de los componentes de infraestructura actualizado.

- El Plan de instalación de los componentes de infraestructura deberá contener al menos:
    - Estrategia de instalación del sistema firewall de base de datos (DBF) en el Centro de Datos Principal en la ciudad de Quito y en el Centro de Datos Alternos en la ciudad de Guayaquil. Si se considera necesario el traslado físico de los componentes de infraestructura, el contratista deberá incluir todos los recursos y logística necesaria para su ejecución, sin costo adicional para el SRI.
    - Cronograma referencial para las actividades de instalación.
    - Número de horas que invertirá el técnico asignado para la instalación y número de horas requeridas del personal del SRI para la participación de los trabajos.
- Instalación de la solución de seguridad de bases de datos (sistema de firewall de base de datos – DBF) en sitio (Centro de Datos Principal Quito y Centro de Datos Alterno 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.
- Todos los equipos deben ser entregados en el lugar de entrega establecido.
- El contratista deberá instalar el hardware y/o software del nuevo sistema de firewall de base de datos (DBF) 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 que su montaje e interconexión se realicen de forma segura y organizada en los centros de cómputo del SRI.
- Cada equipo debe contar con los transceptores (“transceivers”) propios de fábrica necesarios para la operación de las interfaces de tráfico de datos
    - 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”).
    - Transceptores ("transceivers") interfaces óptico para tráfico de base de datos.
    - Demás accesorios que sean necesarios para una interconexión segura y organizada con la infraestructura tecnológica del SRI.
- El contratista deberá instalar la última versión del firmware de todos los componentes (ej. BIOS, lights–out management, controladoras, etc.) de todos los servidores del nuevo sistema.
- 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 firewall de base de datos (DBF), de modo que se garantice su operación en alto desempeño (“high performance”), del nuevo sistema de firewall de base de datos (DBF).
- El contratista gestionará que personal técnico especializado del fabricante del software del sistema de firewall de base de datos (DBF) defina los valores recomendados para los parámetros de configuración de firmware y software de cada uno de los servidores del nuevo sistema, en base a su rol.
- El contratista deberá instalar el software del sistema de firewall de base de datos (DBF), en la última versión estable liberada, en todos los equipos del nuevo sistema, tanto de producción, contingencia, preproducción y testing.
- El contratista deberá realizar pruebas de aceptación de acuerdo con las características técnicas del hardware solicitadas.
- El contratista deberá entregar la Memoria técnica de la instalación de los componentes de infraestructura, en un plazo de hasta quince (15) días hábiles desde el día siguiente hábil a la instalación de los bienes, el mismo que deberá ser aprobado por el Administrador del contrato designado por el SRI, en un plazo de hasta siete (7) días hábiles.

2.3 GARANTÍA TÉCNICA (INCLUYE MANTENIMIENTO CORRECTIVO POR DEFECTOS DE FÁBRICA)

La garantía técnica contemplará lo siguiente:

- Mantenimientos correctivos ilimitados durante el plazo contractual.
- Cobertura de repuestos, accesorios, partes y piezas de los bienes, para lo cual el contratista deberá garantizar que sean nuevos y su disponibilidad durante el tiempo de vigencia de la garantía técnica.
- La garantía técnica del fabricante para el sistema de firewall de base de datos (DBF) será en partes, piezas, mano de obra con horario de atención 24x7 (24 horas al día, sietes a la semana), reemplazo de partes dañadas o con fallas o incluso el equipo completo sin cargo alguno, hasta obtener la operación normal del servicio.
- 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, número de serie y ubicación de los bienes.
- La garantía técnica debe incluir la atención de consultas bajo demanda sobre cambios en la arquitectura implementada, diseño, funcionamiento y personalización de la infraestructura existente y de ser necesario la reinstalación y/o reconfiguración de los equipos objeto de la presente contratación.
- 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.
- El mantenimiento correctivo se trabajará en base a casos, los cuales serán registrados con el contratista y/o fabricante para su resolución con la correspondiente prioridad de atención basada en la severidad del problema.
- El mantenimiento correctivo comprende atención y resolución de casos abiertos, los cuales pueden ser relacionados a hardware y/o software, así como también problemas con la configuración, rendimiento y procesamiento de los diferentes componentes de la infraestructura definida en el alcance de esta adquisición.
- 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.
- El contratista deberá entregar el Procedimiento y mecanismos de apertura, categorización, seguimiento y escalamiento de casos con el proveedor y fabricante; el mismo que será aprobado por el Administrador del contrato.
- La atención de los casos de soporte técnico se realizará las veces que la institución lo requiera, de acuerdo con incidentes detectados por cualquiera de las partes, ya sea por el SRI o el contratista.
- De acuerdo con la severidad establecida y a la necesidad del SRI, los servicios de mantenimiento

correctivo podrán ser realizados de forma remota o de manera presencial en las oficinas del SRI o en las instalaciones donde se encuentren los equipos físicamente.

- La garantía técnica deberá incluir la solución a problemas físicos y lógicos, los cuales incluyen problemas de configuraciones, funcionamiento, problemas asociados al diseño, a bugs reportados por el fabricante, entre otros.
- El Administrador del Contrato entregará el listado de usuarios que podrán reportar un problema o aperturar un caso con el fabricante y proveedor en cualquier momento que se presente, quienes deberán tener acceso al portal del fabricante con usuarios personalizados, listado que podrá ser actualizado cuando la contratante así lo estime necesario.
- El tiempo máximo de cambio de partes, empieza a contar desde que el fabricante emite el diagnóstico correspondiente, hasta que la parte con problemas sea restaurada o reemplazada por el técnico asignado y se restablezca el normal funcionamiento del componente. Este tiempo se lo podrá extender siempre y cuando exista una justificación por escrito emitida al Administrador del contrato y aceptada por el mismo.
- El contratista entregará un Informe técnico de los casos categorizados con severidad uno o que involucren el cambio de parte al Administrador del Contrato, en un plazo de hasta cinco (5) días hábiles, contados a partir del día siguiente del cierre del caso. El informe debe contener al menos:
    - Descripción reporte SRI
    - 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 causa raíz identificada;
    - La solución (temporal o definitiva) aplicada;
    - Incidentes previos que estén relacionados;
    - Las conclusiones y recomendaciones.

Severidad

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

- **Severidad uno**
    - Alarma, avería, fallo, o error de uno de los elementos de hardware o software del sistema firewall de base de datos (DBF)que protege las bases de datos de producción.
    - Inhibición completa o parcial de uno de los elementos de hardware o software del sistema firewall de base de datos (DBF) que protege las bases de datos de producción.
    - Indisponibilidad o degradación de las bases de datos producción que están protegidas por el sistema firewall de base de datos (DBF).
    - Incremento del consumo de los recursos de las bases de datos de producción en el caso de superar el umbral definido en las características generales.
    - Corrupción o pérdida de datos del sistema de firewall de base de datos (DBF) (ej. registros de eventos, registros de auditoría, archivos de políticas, archivos de configuración, etc.).
    - Atención de alarmas que indiquen una condición grave del sistema firewall de base de datos (DBF).
    - Caídas del sistema de firewall de base de datos (DBF) y repetición de caídas al reiniciar el sistema.
    - Alarmas del propio equipo que evidencien una posible falla grave del mismo.

- **Severidad dos**
  - Pérdida parcial de capacidad de servicio. La operación continúa en modo restringido.
  - Alarma, avería, fallo, o error de uno de los componentes del sistema de firewall de base datos (DBF) que protege las bases de datos de contingencia, preproducción, testing (GYE).
  - Inhibición completa o parcial de uno de los componentes del sistema de firewalls de base de datos (DBF) que protege las bases de datos de contingencia, preproducción, testing.
  - Incremento del consumo de los recursos de las bases de datos de contingencia, preproducción, testing en el caso de superar el umbral definido en las características generales.
  - Indisponibilidad o degradación de las bases de datos de contingencia, preproducción y testing del SRI que están protegidas por el sistema de firewalls de base de datos (DBF).
  - Si los componentes de hardware del sistema firewall de base de datos (DBF) están operando con funcionalidad reducida o limitada.

- **Severidad tres**
  - No hay pérdida de servicio, no hay impedimentos en el sistema, se solicita una actualización o soporte en algún tipo de configuración.
  - Advertencias ("warnings") del sistema firewall de base de datos (DBF) que no estén causando ninguna indisponibilidad o degradación de la misma, ni de las bases de datos del SRI que están protegidas por éste.
  - Planificación de trabajos relacionados con el sistema.
  - Requerimientos para afinamiento del sistema.
  - Consultas bajo demanda sobre la arquitectura implementada, diseño, funcionamiento y configuración de la infraestructura implementada.
  - Afinamiento de la arquitectura, del diseño, de la topología, personalización, operación del sistema de firewall de base de datos (DBF), 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 firewall de base de datos (DBF).

En caso de que no exista acuerdo en el tipo de severidad, el SRI definirá la prioridad.

Nivel de Servicio

24x7: 24 horas al día, 7 días a la semana, 365 días al año.

Severidad	Tiempo máximo de respuesta del contratista	Tiempo máximo de diagnóstico preliminar del contratista	Tiempo máximo de cambio de partes Centro de Datos Principal	Tiempo máximo de cambio de partes Centro de Datos Alterno
Uno	2 horas	2 horas	4 horas	12 horas
Dos	4 horas	6 horas	8 horas	16 horas
Tres	8 horas	8 horas	No aplica	No aplica

Tabla9. Niveles de severidad

- El tiempo máximo de respuesta a los casos, definido como el tiempo desde que el SRI reporta un problema hasta que el técnico asignado inicia con la atención presencial o remota, dependerá de la severidad establecida al caso y el nivel de soporte.
- El tiempo máximo de diagnóstico, empieza desde que el técnico asignado inicia con la atención presencial o remota hasta que se emite el diagnóstico correspondiente.

- El tiempo máximo de cambio de partes o equipo, empieza a contar desde que se emite el diagnóstico correspondiente, hasta que la parte con problemas sea restaurada o reemplazada por el técnico asignado. Este tiempo se lo podrá extender siempre y cuando exista una justificación aceptada por escrito por el Administrador del Contrato.
- En caso de reemplazo del equipo, se acepta la instalación de un equipo provisional siempre y cuando el provisional sea de iguales o mejores características que el equipo ofertado. El reemplazo del equipo definitivo será de hasta sesenta (60) días calendario desde la confirmación del reemplazo definitivo del equipo.
- Los casos permitirán principalmente restablecer la normal operación de la solución implementada, sin embargo, una vez restablecido el servicio, si no se conoce la causa raíz del problema presentado o el workaround aplicado no ha permitido dar una solución que evite futuros incidentes relacionados al caso abierto o posterior al diagnóstico se identifique problemas de rendimiento o capacidad, el Administrador del Contrato tendrá la potestad de solicitar al contratista un Plan de acción correctivo para investigar y solucionar el problema. El contratista tendrá un plazo de hasta diez (10) días calendario para la entrega del Plan de acción correctivo, contados a partir del día siguiente de la solicitud formal por parte del Administrador del contrato.
- Ante problemas de rendimiento o capacidad el contratista debe garantizar el óptimo funcionamiento y los niveles de rendimiento de la infraestructura entregada y sus niveles de procesamiento solicitado mientras dure la vigencia del contrato, para lo cual el contratista debe actualizar y/o cambiar componentes de hardware y/o software sin costo para el SRI, si existiera degradación en el rendimiento o capacidad del sistema de firewall de base de datos (DBF) o que afecte al desempeño de las bases de datos institucionales, como parte de la garantía técnica contratada.
- Se deben considerar eventos relacionados a problemas de rendimiento y capacidad los siguientes:
    - Eventos clasificados como rendimiento directamente por los elementos (hardware o software) del sistema de firewall de base de datos (DBF).
    - El almacenamiento no soporte el tamaño de captura de información, las periodicidades y frecuencias de respaldos configurados.
    - Que el throughput no soporten la transaccionalidad de las bases de datos institucionales.
    - El plan de acción correctivo debe contener al menos:
        - Historial de eventos presentados.
        - Diagnóstico del problema.
        - Workaround.
        - Actividades y recursos para ejecutar.
        - Tiempos de ejecución.
- El plan de acción correctivo asociado a problemas de rendimiento o capacidad, debe considerar todas las acciones y recursos necesarios, incluyendo nuevo equipamiento (agregar equipos no incluidos en el acta de entrega recepción), para garantizar el cumplimiento de los niveles de servicio establecidos.
- El tiempo máximo para la ejecución del Plan de acción correctivo, definido desde que el SRI acepta el Plan de acción correctivo hasta que finalice la ejecución del mismo es de hasta treinta (30) días calendario. Este tiempo se lo podrá extender previa autorización del Administrador del Contrato, en el caso de no llegar a un acuerdo el Administrador del Contrato definirá este plazo. Los recursos identificados en el Plan de acción correctivo deberán ser cubiertos en su totalidad por el contratista.
- En caso de presentarse un incidente de seguridad, especialmente ciberataque que afecte a las bases de datos institucionales o fuga de información de las bases de datos institucionales protegidas, el contratista deberá asignar un equipo humano del oferente con apoyo del fabricante, especializado en respuesta, contención y recuperación que trabaje de manera ininterrumpida y continua hasta solventar el incidente.
- 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.

- 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.
- Todos los puntos anteriores deben estar disponibles las veinticuatro (24) horas del día, los siete (7) días de la semana, durante la vigencia del contrato, cubre la operación integral del sistema de firewall de base de datos (DBF), incluyendo tanto los elementos de hardware como el software de este, y tanto aspectos de operación como de seguridad de la información.

2.3.1 Medio de contacto

El contratista deberá poner a disposición del Administrador del Contrato el Procedimiento y mecanismos de apertura, categorización, seguimiento y escalamiento de casos del proveedor y fabricante, el mismo que deberá ser actualizado por el contratista cada vez que existan cambios y socializado al Administrador del Contrato.

2.3.2 Servicio hasta la conclusión del trabajo

Una vez que el técnico del contratista o fabricante inicia con las labores de atención del caso, este deberá dar servicio hasta que se solucione la falla y/o aplique una solución temporal y la infraestructura se encuentre en operación o hasta que se haya logrado un progreso razonable autorizado por el Administrador del Contrato.

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 razonables en la investigación del caso de acuerdo con su severidad.

El trabajo se puede suspender temporalmente si son necesarios partes o recursos adicionales y se reanudará cuando estos estén disponibles, respetando el tiempo máximo de solución. El tiempo máximo de cambio de partes empieza a contar desde que el SRI reporta el caso.

3. SERVICIOS CONEXOS REQUERIDOS

3.1 IMPLEMENTACIÓN/MIGRACIÓN Y TRANSFERENCIA DE CONOCIMIENTOS

3.1.1 IMPLEMENTACIÓN/MIGRACIÓN DE LA SOLUCIÓN DE SEGURIDAD DE BASE DE DATOS (SISTEMA DE FIREWALL DE BASE DE DATOS – DBF) CENTRO DE DATOS PRINCIPAL QUITO Y CENTRO DE DATOS ALTERNO GUAYAQUIL.

- El Plan de implementación/migración de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF) adquirida y migración de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF) actual instalada en el Centro de Datos Principal de Quito y Centro de Datos Alterno de Guayaquil, contendrá al menos lo indicado a continuación:
    - Cronograma de trabajo.
    - Diseño detallado propuesto.
    - Arquitectura detallada propuesta para el Centro de Datos Principal de Quito y Alterno Guayaquil.
    - Mejores prácticas de la marca ofertada que incluya al menos criterios rendimiento, disponibilidad, ciclo de vida de los respaldos, compatibilidad con la infraestructura del SRI y seguridad.
    - Personal asignado para la prestación de los servicios conexos de implementación/migración.
    - Número de horas que invertirá el técnico asignado para la instalación y número de horas requeridas del personal del SRI para la participación de los trabajos.

- El Plan de implementación/migración podrá ser modificado por acuerdo entre el Administrador del Contrato y contratista.
- El contratista deberá ofrecer acompañamiento en sitio y participar en las reuniones con el personal técnico del SRI durante el tiempo que se determine necesario para la estabilización del sistema de firewall de base de datos (DBF).
- Los trabajos de migración deberán cubrir los controles y reportería implementados actualmente; en función de la definición del Administrador de Contrato.
- Se deberán validar, depurar y optimizar las configuraciones del sistema de firewall de base de datos (DBF) 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 sistema de firewall de base de datos (DBF) de manera que se garantice el mayor nivel de seguridad posible para las bases de datos productivas, contingencia, preproducción y testing del SRI protegidos por el nuevo sistema.
- El contratista deberá implementar un caso de enmascaramiento de información; en función de la definición del Administrador de Contrato.
- 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 sistema de firewall de base de datos (DBF).
- El contratista deberá configurar y probar los mecanismos de emisión de alertas (ej. vía correo electrónico) del sistema de firewall de base de datos (DBF).
- El contratista gestionará que personal técnico especializado del fabricante del software de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF), asista al contratista en todos los procesos de la migración, validación, depuración, optimización y afinamiento de las configuraciones, arquitectura y políticas de seguridad de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF) nuevo.
- El contratista gestionará que personal técnico especializado del fabricante del software del sistema firewall de base de datos (DBF), lo asista en la verificación de problemas o errores para mejorar la configuración, desempeño, o controles implementados.
- El contratista gestionará que el fabricante ejecute un diagnóstico del software del sistema de firewall de base de datos (DBF), 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 firewall de base de datos (DBF) 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 y software.
- Los horarios de implementación/migración de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF) se acordarán con el Administrador del Contrato.
- El equipo de trabajo que participará en la implementación/migración de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF) deberá disponer de todo el material de trabajo que se requiera.
- Todas las actividades que ejecute el contratista relacionadas a la implementación/migración de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF) serán supervisadas por personal técnico del Servicio de Rentas Internas.
- Todos los gastos incurridos en la implementación/migración de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF) (traslados, viáticos, hospedaje, etc.) estarán a cargo del contratista, el SRI no incurrirá en ningún gasto adicional.
- Una vez concluido la implementación/migración, el contratista deberá emitir en un plazo de hasta diez (10) días hábiles, contados a partir del día siguiente hábil a la finalización del servicio de implementación/migración y transferencia de conocimientos, una Memoria técnica del proceso de configuración en español, que incluya al menos los siguientes puntos:

  - Inventario y descripción detallada de los elementos de hardware.
  - Diseño detallado final que incluya diagramas de infraestructura y conectividad
  - 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).
  - Mecanismo de operación del sistema de firewall de base de datos (DBF).
  - Mecanismo de creación de cuentas de usuarios y asignación de permisos de administración.
  - Mecanismos de creación de políticas de seguridad y de auditoría.
  - Mecanismos de enmascaramiento de información.
  - Métodos básicos de detección y resolución de problemas (Base de Conocimientos Básica).
  - Manual de instalación del fabricante de todos los elementos de hardware y software de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF).
  - Manuales de administración y operación de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF).

- La Memoria técnica del proceso de configuración deberá ser aprobada por el Administrador del Contrato en un plazo de hasta diez (10) días hábiles. En caso de que se requiera correcciones a la memoria técnica del proceso de configuración, el contratista deberá enviar la memoria técnica actualizada, en un plazo de hasta siete (7) días hábiles, posterior a la notificación del Administrador del contrato.

Finalizada la etapa de implementación y migración se suscribirá un oficio de constancia de fechas de finalización de las actividades tanto de IMPLEMENTACIÓN/MIGRACIÓN de la solución de seguridad de base de datos (sistema firewall de base de datos – DBF), tanto en el Centro de Datos Principal en la ciudad de Quito como del Centro de Datos Alterno en la ciudad de Guayaquil.

3.1.2 TRANSFERENCIA DE CONOCIMIENTOS

La transferencia de conocimiento sobre temas relacionados al sistema de firewall de base de datos (DBF) a ser implementado deberá incluir:

- El contratista debe presentar al Administrador del Contrato el Plan de transferencia de conocimientos en un plazo de hasta treinta (30) días calendario contados a partir del día siguiente hábil al plazo de entrega de instalación de los bienes.
- El Administrador del Contrato deberá aprobar el Plan de transferencia de conocimientos presentado en un plazo de hasta siete (7) días calendario a partir de la entrega por parte del contratista, en el caso de generarse alguna observación o cambio el contratista tendrá hasta siete (7) días calendario para entregar el Plan transferencia de conocimiento actualizado.
- La transferencia de conocimientos de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF) serán prestados por parte del contratista. Todos los gastos incurridos (traslados, viáticos, hospedaje, etc.) estarán a cargo del contratista, el SRI no incurrirá en ningún gasto adicional.
- Debe basarse en cursos oficiales del fabricante, sobre arquitectura, configuración, administración y troubleshooting de la solución adquirida.
- La transferencia de conocimientos de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF) debe ser de al menos cuarenta (40) horas y para al menos diez (10) personas del SRI, e incluir al menos los siguientes temas generales:

    - Arquitectura de solución de seguridad de base de datos (sistema de firewall de base de datos - DBF).
    - Administración de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF).
    - Gestión de Políticas de seguridad y de auditoría.
    - Configuración de obtención de datos sensibles.
    - Configuración de enmascaramiento de datos
    - Análisis de vulnerabilidades.
    - Análisis e identificación de anomalías, riesgos o incidentes de usuarios.
    - 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 seguridad de base de datos (sistema de firewall de base de datos - DBF).

- La transferencia de conocimientos 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 de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF).
- La transferencia de conocimientos se deberá realizar de forma presencial en instalaciones provistas por el contratista.

3.2 MANTENIMIENTO PREVENTIVO

- Se deberá contar con mantenimiento preventivo de la solución ofertada por 3 años contados a partir del día siguiente hábil a la fecha de finalización del servicio conexo requerido de Implementación/Migración y trasferencia de conocimientos de la solución de seguridad de base de

datos (sistema de firewall de base de datos – DBF) Centro de Datos Principal Quito y Centro de Datos Alterno Guayaquil.

- El contratista deberá presentar el Plan de mantenimiento preventivo anual dentro del primer mes del periodo del servicio para aprobación del Administrador del contrato. Este plan deberá ser presentado anualmente durante la vigencia del contrato.
- El plan de mantenimiento preventivo anual debe incluir el tiempo estimado de actividades de mantenimiento y/o indisponibilidad de los equipos.
- El contratista deberá realizar seis (6) visitas programadas de revisión de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF), dos (2) por año.
- El mantenimiento preventivo podrá llevarse a cabo en horario normal o fuera de horario laboral, fines de semana, feriados; sin costo adicional para a el SRI.
- El mantenimiento preventivo se realizará de acuerdo con el Plan de Mantenimiento Preventivo aprobado por el SRI, estará constituido por una visita semestral que deberá ser realizada por el contratista, en la que al menos estarán incluidas las siguientes actividades:

    - Limpieza externa de los elementos de hardware (una por año).
    - 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 (una por año).
    - Revisión de alertas visuales (una por año).
    - Inspección física del sitio de instalación del equipo, incluyendo sus cables y conectores (una por año).
    - Etiquetado y ordenamiento del cableado que llega a los elementos de hardware (una por año).
    - Revisar el estado de salud y el desempeño de la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF) (dos por año).
    - Verificar que el mecanismo de respaldos esté operando correctamente (dos por año);
    - Validar la necesidad de la instalación de parches de software y hardware (dos por año);
    - Instalar los parches de software y hardware recomendados por el fabricante (dos por año);
    - Instalar la última versión estable recomendada por el fabricante del software y hardware (dos por año);
    - Validar la necesidad de cambios en la configuración del sistema (dos por año);
    - Aplicar configuraciones de afinamiento de seguridad y de operación recomendadas por el fabricante de software, en caso de ser necesario (dos por año);
    - Aplicar rectificaciones o mejoras (dos por año);

- 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 falla, o error, o degradación, o comportamiento no esperado de algún equipo que compone la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF) 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.
- Solicitudes de asistencia asociadas a requerimientos de nuevas funcionalidades en las bases de datos de producción del SRI protegidos por la solución de seguridad de base de datos (sistema de firewall – DBF).
- Reportes e informes bajo demanda de diagnóstico del sistema, o de algún evento particular relacionado con el sistema o por caso de posibles incidentes de fuga de información.
- Al concluir cada visita y sus actividades, el contratista deberá entregar al Administrador del Contrato un informe de mantenimiento preventivo 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 firewall de base de datos (DBF);
- Las recomendaciones de mejora en configuración, o de incremento de capacidad o mejora de diseño, en caso de ser necesario;

- Debido a la operación ininterrumpida que deben tener los servicios tecnológicos del SRI, las fechas definitivas de cada mantenimiento serán aprobadas oportunamente por el Administrador del Contrato designado por el SRI, a fin de minimizar la afectación a los usuarios internos y externos. El SRI notificará al contratista con al menos diez (10) días hábiles de anticipación, las fechas y horario definitivos para cada mantenimiento. El mantenimiento preventivo deberá ejecutarse tentativamente de acuerdo con el siguiente detalle:
  - Centro de Datos Principal (Quito): Septiembre - Octubre
  - Centro de Datos Alterno (Guayaquil): Enero – Febrero
- 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 la solución de seguridad de base de datos (sistema de firewall de base de datos - DBF), en el formato que defina el Administrador del Contrato.

4. PLAZO DE EJECUCIÓN

El plazo de ejecución de este contrato será de hasta mil doscientos cincuenta y cinco (1255) días calendario contados a partir del día siguiente laborable de la suscripción del contrato.

BIENES REQUERIDOS

- El plazo para la 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 noventa (90) días calendario contados a partir del siguiente día de la firma del contrato.
- El contratista deberá entregar mediante correo electrónico u oficio al Administrador del Contrato, hasta setenta y cinco (75) días calendario contados a partir del siguiente día de la firma del contrato: el listado de equipos, con la marca, modelo, tipo, descripción, serie y cronograma de entrega de los bienes (día y ubicación).
- El plazo de entrega del Plan de instalación de los componentes de infraestructura será de hasta setenta y cinco (75) días calendario contados a partir del siguiente día de la firma del contrato, el mismo que deberá ser aprobado por el Administrador del Contrato designado por el SRI, en un plazo de hasta siete (7) días calendario.
- En caso de que se requiera correcciones al Plan de instalación de los componentes de infraestructura, el contratista dispondrá de hasta siete (7) días calendario contados a partir del siguiente día de la notificación del Administrador del contrato para enviar el plan actualizado.
- El contratista deberá entregar la Memoria técnica de la instalación de los componentes de infraestructura, en un plazo de hasta quince (15) días hábiles desde el día siguiente hábil a la instalación de los bienes, el mismo que deberá ser aprobado por el Administrador del contrato designado por el SRI, en un plazo de hasta siete (7) días hábiles.
- En caso de que se requiera correcciones a la Memoria técnica de la instalación de los componentes de infraestructura, el contratista dispondrá de hasta siete (7) días hábiles posteriores a la

notificación del Administrador del contrato para enviar la memoria técnica actualizada.

- El plazo de la vigencia de la garantía técnica y del soporte de fábrica será de mil noventa y cinco (1095) días contados a partir siguiente día hábil a la fecha de finalización de la implementación/ migración y trasferencia de conocimientos.
- El plazo de entrega del Plan de acción correctivo es de hasta diez (10) días calendario a partir del siguiente día de la solicitud del Administrador del Contrato, y su ejecución es de máximo de hasta treinta (30) días calendario desde el siguiente día que el SRI acepta el plan de acción correctivo. Este tiempo se lo podrá extender previa autorización del Administrador del Contrato, en el caso de no llegar a un acuerdo el Administrador del Contrato definirá este plazo.

SERVICIOS CONEXOS REQUERIDOS

- El Plan de Implementación/Migración aprobado por el Administrador deberá ser entregado en un plazo de hasta setenta y cinco (75) días calendario contados a partir del siguiente día de la firma del contrato, el mismo que deberá ser aprobado por el Administrador del Contrato designado por el SRI, en un plazo de hasta siete (7) días calendario.
- En caso de que se requiera correcciones al Plan de Implementación/Migración, el contratista dispondrá de hasta siete (7) días calendario posteriores a la notificación del Administrador del Contrato para enviar el plan actualizado.
- El plazo de entrega para el servicio de Implementación/Migración al sistema de firewall de base de datos (DBF) será de hasta cuarenta y cinco (45) días calendario contados a partir del día siguiente hábil de la finalización de la instalación de los bienes.
- El plazo de entrega de la Memoria técnica del proceso de configuración del servicio de Implementación/Migración deberá será de hasta diez (10) días hábiles, contados a partir del día siguiente hábil a la finalización del servicio de implementación/migración y trasferencia de conocimientos, el mismo que deberá ser aprobado por el Administrador del Contrato, en un plazo de hasta diez (10) días hábiles.
- En caso de que se requiera correcciones de la Memoria técnica del proceso de configuración, el contratista dispondrá de hasta siete (7) días hábiles posteriores a la notificación del Administrador del Contrato para enviar la memoria técnica actualizada.
- El plazo de entrega del Plan de transferencia de conocimientos será de hasta treinta (30) días calendario, contados a partir del día siguiente hábil de la finalización de la instalación de los bienes.
- En caso de que se requiera correcciones al Plan de transferencia de conocimientos, el contratista dispondrá de hasta siete (7) días calendario posteriores a la notificación del Administrador del contrato para enviar el plan de transferencia de conocimientos actualizado.
- La transferencia de conocimientos del sistema de firewall de base de datos (DBF), deberá ser entregado en un plazo de hasta sesenta (60) días calendario desde el siguiente día hábil a la finalización de la instalación de los bienes.
- El plazo de la vigencia de los servicios de mantenimiento preventivo y garantía técnica de hardware será de mil noventa y cinco (1095) días calendario (3 años) contados a partir del siguiente día hábil a la fecha de finalización de la implementación/migración y transferencia de conocimientos.
- El plazo de entrega del Plan de mantenimiento preventivo será de hasta siete (7) días calendario, contados a partir del día siguiente de la notificación de las fechas y horario del mantenimiento, por parte del Administrador del Contrato.
- El plazo de entrega del Procedimiento y mecanismos de apertura, categorización, seguimiento y escalamiento de casos con el contratista y fabricante deberá ser entregado en un plazo de hasta setenta y cinco (75) días calendario contados a partir del siguiente día de la firma del contrato.
- El plazo de entrega del informe consolidado de los casos atendidos será de hasta diez (10) días hábiles después de finalizado cada período de soporte (anual).
- El plazo de entrega de los informes de mantenimiento preventivo será de hasta diez (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:

- Entrega del certificado del fabricante de activación de la garantía técnica.
- Oficio con el listado de equipos
- Plan de instalación de los componentes de infraestructura
- Procedimiento y mecanismos de apertura, categorización, seguimiento y escalamiento de casos con el contratista y fabricante que incluye la guía de acceso y uso del portal y/o interfaz de gestión.
- Plan de Implementación/Migración

Implementación/Migración 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 del servicio conexo de Implementación/Migración y transferencia de conocimiento correspondiente.

Para la suscripción del Acta de Entrega Recepción correspondiente a la implementación/migración 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 implementación, migración y trasferencia de conocimientos.
- Memoria técnica de la instalación de los componentes de infraestructura
- Memoria técnica del proceso de configuración efectuado en la Implementación/Migración del sistema de firewall de base de datos (DBF) en el Centro de Datos Principal en la ciudad de Quito y del Centro de Datos Alterno en la ciudad de Guayaquil, con el detalle de todas las actividades realizadas y el detalle de los productos implementados.
- Plan de transferencia de conocimientos
- Listado de asistencia a la transferencia de conocimiento debidamente firmada.

Mantenimiento preventivo del sistema de firewalls de base de datos (DBF): El servicio conexo de mantenimiento preventivo se pagará en tres partes iguales de acuerdo con los periodos definidos en el Plan de mantenimiento preventivo aprobado. 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 correspondiente, el contratista deberá entregar mediante oficio al Administrador de Contrato:

- Plan de mantenimiento preventivo
- Informes de mantenimiento preventivo por cada mantenimiento realizado.
- 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;

Para el último pago se requerirá la suscripción del Acta de Entrega Recepción definitiva.

6. LUGAR DE ENTREGA

- Los equipos, la implementación, el servicio de mantenimiento y las actividades de garantía técnica de los sistemas de Producción deben entregarse en el centro de datos de producción del SRI, ubicado en la ciudad de Quito.
- Los equipos, la implementación, el servicio de mantenimiento y las actividades de garantía técnica de los sistemas de contingencia, preproducción y testing deben entregarse en el centro de datos de contingencia del SRI, ubicado en la ciudad de Guayaquil.
- 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 6 (verde), piso 3; o donde señale el Administrador del Contrato.
- En caso de cambio en la dirección especificada anteriormente, el Administrador del Contrato informará mediante oficio al contratista la nueva dirección.

7. GLOSARIO DE TÉRMINOS TÉCNICOS

ACTIVE DIRECTORY: Es el término que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadoras. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP y Kerberos.

BIOS: El sistema básico de entrada-salida o BIOS es un estándar de facto que define la interfaz de firmware para computadoras compatibles. También es conocido como BIOS del sistema.

CONSOLA DE ADMINISTRACIÓN: Es una interfaz gráfica que le permite gestionar las aplicaciones y realizar tareas de administración para la solución de seguridad de base de datos - DBF.

CORRELACIONADOR DE EVENTOS: También conocido como SIEM (Security Information and Event Management), tiene como objetivo principal el ayudar a las empresas a construir un centro de operaciones de seguridad en donde se tenga centralizada la información de múltiples fuentes.

DDL: Es un lenguaje de definición de datos (Data Definition Language, DDL por sus siglas en inglés) es un lenguaje proporcionado por el sistema de gestión de base de datos que permite a los usuarios de esta

llevar a cabo las tareas de definición de las estructuras que almacenarán los datos, así como de los procedimientos o funciones que permitan consultarlos.

DML: Es un lenguaje proporcionado por el sistema de gestión de base de datos que permite a los usuarios llevar a cabo las tareas de consulta o manipulación de los datos, organizados por el modelo de datos adecuado.

END-OF-LIFE: Un producto al final de su vida útil es un producto al final del ciclo de vida del producto que impide que reciban actualizaciones, lo que indica que el producto está al final de su vida útil.

FIREWALL PARA BASES DE DATOS (DBF): Es una aplicación de software o de hardware que permite filtrar y auditar las peticiones que llegan a las bases de datos, mediante un conjunto de reglas preestablecidas.

FTP: Protocolo de transferencia de archivos es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor.

GARANTÍA TÉCNICA: Comprende la reparación del bien en caso de daño o defecto de funcionamiento, que incluye la provisión e instalación de repuestos, accesorios, piezas o partes, así como la oportunidad de ejecutar todas las acciones necesarias para garantizar su funcionalidad y operatividad.

HEALTH CHECK: Es un diagnóstico completo y profundo de los distintos componentes de la infraestructura de la solución de seguridad de base de datos – DBF.

HOTFIX: Revisión, parche rápido o parche en caliente, es un único paquete que incluye información normalmente en forma de uno o más ficheros que es utilizado para solucionar un problema en una pieza de software.

INTERFACES ETHERNET: Es la tecnología tradicional para conectar dispositivos en una red de área local (LAN) o una red de área amplia (WAN) por cable, lo que les permite comunicarse entre sí a través de un protocolo: un conjunto de reglas o lenguaje de red común.

ITSM: La gestión de servicios de tecnologías de la información es una disciplina basada en procesos, enfocada en alinear los servicios de TI proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final.

LOGS: Se usa el término registro, log o historial de log para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular. De esta forma constituye una evidencia del comportamiento del sistema.

LIGTHS-OUT-MANAGEMENT: Mecanismo para encender, apagar y reiniciar en remoto los dispositivos.

PATCHCORDS: Cable de conexión también llamado cable de red, se usa en redes de computadoras o sistemas informáticos o electrónicos para conectar un dispositivo electrónico con otro.

PL/SQL: Procedural Language/Structured Query Language, es un lenguaje de programación incrustado en Oracle.

PRUEBAS DE ACEPTACIÓN: Las pruebas de aceptación pertenecen a las últimas etapas previas a la liberación en firme de versiones nuevas a fin de determinar si cumplen con las necesidades y/o requerimientos de las empresas y sus usuarios.

SNMP: Protocolo simple de administración de red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

THROUGHPUT: La tasa de transferencia efectiva es el volumen de trabajo o de información neto que fluye a través de un sistema, como puede ser una red de computadoras.

TRANSCEIVERS: Un transceptor es un dispositivo que cuenta con un transmisor y un receptor que comparten parte de la circuitería o se encuentran dentro de la misma caja.

T-SQL: Expande el estándar de SQL para incluir programación procedimental, variables locales, varias funciones de soporte para procesamiento de string, procesamiento de fechas, matemáticas, etc, y cambios a las sentencias DELETE y UPDATE.