TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE SERVICIO ANTIVIRUS CORPORATIVO

I. DENOMINACION DE LA CONTRATACION
SERVICIO DE ANTIVIRUS CORPORATIVO

II. AREA USUARIA
OFICINA DE TECNOLOGÍAS Y SISTEMAS INFORMÁTICOS

III. OBJETIVO DE LA CONTRATACIÓN
El presente servicio tiene objetivo contratar el servicio de antivirus corporativo, porque la función principal de los antivirus es la de velar porque el software de los ordenadores, y su sistema operativo, este libre de cualquier intrusión, se ejecute correctamente y no sea el objetivo de virus informáticos, y si es necesario, se encargará también de desinfectar los archivos ya dañados para devolver el sistema a su estado natural.

IV. ACTIVIDAD POI
SERVICIO DE ANTIVIRUS CORPORATIVO

V. FINALIDAD PÚBLICA
Los servicios para contratar nos ayudaran a proteger los equipos informáticos y servidores de las diferentes amenazas existentes, la utilización de un antivirus es fundamental hoy en día para que podamos recorrer la web, leer correos y abrir los documentos que recibimos, sin la preocupación de que podamos ser alcanzados por un ataque que nos destruya nuestros datos, los de terceros y en este caso información de la institución Municipal.

VI. ALCANCES Y DESCRIPCIÓN DEL SERVICIO Y/O CONSULTORÍA

ALCANCE DEL PRODUCTO

ITEM	SERVICIO DE:	TIEMPO	ALCANCE
01	• Protección para Desktops: ENDPOINT ANTIVIRUS Windows / Linux / OS X • Protección para Servidores: SECURITY SERVER Windows /Linux • Consola de Administración: CONSOLA PROTECT WEB Windows / Linux	01 año	350 EQUIPOS INFORMÁTICOS

6.1 Característica y requisitos del Postor:

6.1.1 Características mínimas (última generación):

a. Módulo de exploración UEFI
Comprueba y aplica las medidas seguridad del entorno previo al inicio en cumplimiento con la especificación UEFI. Se diseñó para monitorear la integridad del firmware y, en caso de que se detecte una modificación, se le notifica al usuario.

b. Detecciones de ADN
Son capaces de identificar muestras ya conocidas de malware, nuevas variantes de una familia de malware conocida o incluso el malware aún desconocido que contenga genes que indiquen la presencia de un comportamiento malicioso.

c. Detección de comportamiento malicioso y bloqueo: HIPS
Supervisa la actividad del sistema y emplea un conjunto predefinido de reglas para reconocer el comportamiento sospechoso del sistema.

d. Bloqueo de exploits

Monitorea las aplicaciones que suelen ser atacadas por exploits con mayor frecuencia (navegadores, lectores de documentos, clientes de correo electrónico, Flash, Java, etc.) y, en lugar de enfocarse solamente en algunos identificadores de CVE (Vulnerabilidades y Exposiciones Comunes) en particular, se centra en técnicas de explotación.

e. Ransomware Shield

Es una capa adicional que protege a los usuarios ante el ransomware. Esta tecnología monitorea y evalúa todas las aplicaciones ejecutadas en función de su comportamiento y reputación. Se diseñó para detectar y bloquear procesos cuya conducta es similar a la del ransomware.

f. Protección ante botnets

Detecta las comunicaciones maliciosas que utilizan las botnets y al mismo tiempo identifica los procesos ofensivos. Bloquea todas las comunicaciones maliciosas detectadas y le informa al usuario.

6.1.2 Gestión de Seguridad (Consola de Protección)

Garantiza la visibilidad en tiempo real para todas las endpoints, así como informes completos y administración de seguridad para todos los sistemas operativos y debe cumplir con los siguientes puntos como minimo:

- Consola local con posibilidad de upgrade a cloud (opcional).
- Visibilidad en tiempo real de equipos de escritorio, servidores, máquinas virtuales y hasta dispositivos móviles administrados.
- Informes completos para las soluciones de seguridad.
- Control sobre las capas de prevención y detección.
- Conexión a cualquier navegador web

6.1.3 Servicio de Protección endpoint Antivirus:

Debe darse a nivel de diferentes tecnologías que constamente buscan equilibrar el rendimiento, la detección y falsos positivos, debe permitir a las organizaciones lo siguiente:

- Protegerse contra el ransomware
- Bloquear ataques dirigidos
- Prevenir filtración de datos
- Bloquear ataques sin archivo
- Control
- Control de dispositivos

6.1.4 Seguridad para servidores de archivo (server security):

La Protección debe ser avanzada para servidores contra cargas maliciosas y archivos no deseados. Garantiza un entorno estable y sin conflictos.

- Protección contra ransomware
- Prevención ante violación de datos
- Detección de amenazas 0-day
- Prevención ante ataques de archivo

6.1.5 Implementación:

El servicio de soporte técnico ofrecido por la Empresa Proveedora, debe consistir en brindar una solución integrada a problemas técnicos y comerciales si fuese el caso, esos incluyen los siguientes servicios:

1. Instalación del producto Onsite
2. Capacitación certificada en el uso de los productos ofrecidos

3. Mantenimiento y evaluación de nuestro parque informático
4. Pruebas de confirmación
5. Seguimiento preventivo cada 03 meses
6. Actualizaciones a nuevas versiones

VII. REGLAMENTOS TECNICOS, NORMAS METROLOGICAS Y/O SANITARIAS
NO CORRESPONDE

VIII. SEGUROS
NO CORRESPONDE

IX. PRESTACIONES ACCESORIAS A LA PRESTACION PRINCIPAL
NO CORRESPONDE

X. REQUISITOS MINIMOS DEL PROVEEDOR
El proveedor deberá cumplir con los siguientes requisitos mínimos:

- Ser distribuidor autorizado de la marca.
- Tener RUC activo y habilitado.
- Estar inscrito en el Registro Nacional de Proveedores – RNP.

XI. LUGAR DE PRESTACION DEL SERVICIO
La instalación se realizará en un equipo servidor de la Oficina de Tecnologías y Sistemas Informáticos de la Municipalidad Distrital de San Sebastián.

XII. PLAZO DE INSTALACION, CONFIGURACIÓN, EJECUCIÓN, CAPACITACIÓN y PRESTACION DEL SERVICIO

a) El plazo de entrega para implementación, instalación, configuración y puesta en marcha del servicio será de hasta (15) días calendarios como máximo que se computaran a partir del día siguiente suscrito y firmado el contrato o hecha la notificación de la Orden de Servicio, culminando con el acta de conformidad de la instalación del servicio.
b) El Acta de conformidad de la Instalación del servicio será suscrito por el área usuaria y el contratista en el plazo de 02 días contados a partir del día siguiente de culminada la implementación.
c) El plazo de prestación del servicio deberá ser de (01) año, a partir del día siguiente de suscrita el acta de conformidad de la instalación del servicio por parte del contratista y el área usuaria que es la Oficina de Tecnología de Información.
d) El proveedor del servicio deberá brindar capacitación al personal de la Oficina de Tecnologías y Sistemas Informáticos para el uso correcto de la instalación y configuración en los terminales.

XIII. ENTREGABLES

- Acta de conformidad de instalación del servicio, donde se registre la fecha de inicio y fin del servicio.
- Certificados para el personal capacitado.

XIV. LUGAR DE ENTREGA
El proveedor deberá presentar su carta de cumplimiento en el plazo de 02 días siguientes a la firma del acta de conformidad de instalación del servicio y por mesa de Partes de la MUNICIPALIDAD DISTRITAL DE SAN SEBASTIÁN.

XV. SISTEMA DE CONTRATACIÓN
NO CORRESPONDE

XVI. CONFORMIDAD DE LA PRESTACIÓN
La conformidad será emitida por la Oficina de Tecnologías y Sistemas Informáticos, quien verificará el cumplimiento del servicio.

XVII. FORMA Y CONDICIONES DE PAGO

El pago se realizará de manera única y previa conformidad emitida por la Oficina de Tecnologías y Sistemas Informáticos.

Todo pago será con cuenta de CCI entre la ENTIDAD y el PROVEEDOR Salvo indicación contraria del área de pagos, previa conformidad del área usuaria.

XVIII. PENALIDADES

Penalidad por mora en la ejecución de la prestación del servicio:
En caso de retraso injustificado en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o, de ser el caso del ítem que debió ejecutarse. Esta penalidad será deducida de los pagos a realizarse.

La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente formula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{Monto vigente}}{F \times \text{Plazo vigente en días}}$$

Donde F tendrá los siguientes valores:

- Para plazos menores o iguales a sesenta (60) días: F = 0.40
- Para plazos mayores a sesenta (60) días: F= 0.25

Tanto el monto como el plazo se refieren, según corresponda al monto vigente del contrato o ítem que debió ejecutarse o, en caso que estos involucran obligaciones de ejecución periódica o entregas parciales, a la presentación individual que fuera materia de retraso.

XIX. OTRAS PENALIDADES

NO APLICA

XX. RESPONSABILIDAD DEL PROVEEDOR Y/O CONSULTOR

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos de los bienes ofertados por un plazo no menor de un (1) año contado a partir de la conformidad otorgada por la Entidad.

XXI. DISPOSICIONES DE CONFIDENCIALIDAD

El contratista se obliga a mantener y guardar estricta reserva y absoluta confidencialidad de todos los documentos e información que tenga acceso o sea proporcionada por la Municipalidad, a los que tenga acceso en la ejecución del servicio.

Se entiende que la obligación asumida por el proveedor está referida no solo a los documentos e informaciones señalados como "confidenciales" si no a todos los documentos e informaciones que en razón del presente servicio o vinculado con la ejecución del mismo, puedan ser conocidos a través del contratista.

XXII. CLAUSULA DE ANTICORRUPCION

EL CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a los impedimentos señalados en El Reglamento, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a los impedimentos señalados en El Reglamento.

Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas,

organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

XXIII. NORMAS ANTISOBORNO

El proveedor, no debe ofrecer, negociar o efectuar cualquier pago, objeto de valor o cualquier dádiva en general, o cualquier beneficio o incentivo ilegal en relación al contrato, que pueden constituir un incumplimiento a la ley, tales como robo, fraude, cohecho o tráfico de influencias, directa o indirectamente, o a través de socios, integrantes órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas, en concordancia a lo establecido en el artículo 11 de Ley de Contrataciones del Estado, Ley N° 30225, sus modificaciones.

Asimismo, el proveedor se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participantes, integrantes órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas en virtud a lo establecido en los artículos antes citados de la Ley de Contrataciones.

De la misma forma, el proveedor se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviere conocimiento; así también, en adoptar medidas técnicas, prácticas, a través de canales dispuestos por la MDSS.

El proveedor es consciente que, de no cumplir con lo anteriormente expuesto, se somete a la resolución del servicio o bien contratado y a las acciones civiles y/o penales que el Programa pueda accionar, constituyendo su declaración, la firma del mismo en la Orden de Servicio de la que estos términos de referencia forman parte integrante.

XXIV. CUMPLIMIENTO DE NORMAS DE EMERGENCIA SANITARIA CONTRA EL COVID- 19

Deberá dar cumplimiento a la directiva Institucional que regula los protocolos COVID - 19.

XXV. RESOLUCIÓN DE CONTRATO

La MDSS puede resolver el contrato, en los siguientes casos:

a) Por el incumplimiento injustificado de las obligaciones contractuales, legales o reglamentarias a su cargo, pese a haber sido requerido para ello.
b) Por la acumulación del monto máximo de la penalidad por mora o por el monto máximo para otras penalidades, en la ejecución de la prestación a su cargo.
c) Por la paralización o reducción injustificada de la ejecución de las prestaciones, pese a haber sido requerido para corregir tal situación.
d) Por caso fortuito o fuerza mayor que imposibilite de manera definitiva la continuidad de la ejecución, amparado en un hecho o evento extraordinario, imprevisible e irresistible; o por un hecho sobreviniente al perfeccionamiento del contrato, orden servicio que no sea imputable a las partes.
e) Asimismo, puede resolver de forma total o parcial la orden de servicio y/o contrato por mutuo acuerdo entre las partes, previa opinión del área usuaria.

XXVI. SOLUCIÓN DE CONTROVERSIAS

Los conflictos que se deriven de la ejecución e interpretación de la presente contratación son resueltos mediante trato directo, conciliación y/o acción judicial.