TERMINOS DE REFERENCIAS PARA LA CONTRATACIÓN DEL SERVICIO DE SUSCRIPCION DE LICENCIAS DE SOFTWARE ANTIVIRUS.

1. ÁREA QUE REALIZA EL REQUERIMIENTO.

Oficina de Tecnología de Información (OTI).

2. OBJETO DE LA CONTRATACIÓN.

Contratación del servicio de suscripción del Software de Antivirus para garantizar la adecuada protección de la información almacenada en los equipos y sistemas informáticos dentro de SUTRAN.

3. ACTIVIDAD VINCULADA AL POI

La presente contratación está orientada a cumplir la siguiente actividad vinculada al POI.

CENTRO DE COSTO	:	02.03 - Oficina de Tecnología de Información
OBJETIVO ESTRATEGICO INSTITUCIONAL	:	OEI.02 - Modernizar la Gestión Institucional de la SUTRAN.
ACCIÓN ESTRATEGICA INSTITUCIONAL	:	AEI.02.04 - Gestión de Gobierno Digital Implementado en la SUTRAN
ACTIVIDAD OPERATIVA	:	AOI00134600442 - Atención y Soporte a los Servicios Informáticos y Seguridad de la Entidad

4. FINALIDAD PÚBLICA

El presente proceso permitirá continuar las condiciones de seguridad de los usuarios que usan los equipos de cómputo de la entidad, a fin de cumplir con las funciones asignadas de conformidad con lo regulado en el Reglamento de la Organización y Funciones - ROF de la Entidad, aprobado mediante el Decreto Supremo N° 006-2015-MTC, en su artículo 34°, señala las funciones de la Oficina de Tecnología de Información.

5. OBJETIVOS DE LA CONTRATACIÓN.

Objetivo General

Proteger la infraestructura informática de la entidad ante ataques informáticos que pudieran causar perdida de información.

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:35:52 -05:00

Objetivo Especifico:
Adquisición de suscripción de software de antivirus para equipamiento personal de cómputo perteneciente a la entidad, a fin de contar con un sistema de protección eficiente ante ataques informáticos.

6. DESCRIPCION DEL SERVICIO A ADQUIRIR.

La entidad solicita la contratación del servicio de suscripción de un software antivirus de un solo fabricante (consola y agente) que cubra con los requerimientos técnicos mínimos requeridos.

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:31:31 -05:00

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANTIDAD
01	Suscripción anual de software de antivirus para mil trescientos (1300) equipos de cómputo de la entidad.	Servicio	01

6.1. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO.

El contratista deberá de considerar los siguientes lineamientos para la ejecución del servicio.

6.1.1. INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO:

El contratista deberá de realizar la implementación, configuración y funcionamiento del software antivirus, considerando por ello lo siguiente:

- Los trabajos programados serán supervisados por el personal de la Oficina de Tecnología de Información.
- Instalación de la herramienta para la sede principal de la SUTRAN.
- Instalación de la consola principal, *además de subconsolas de ser el caso*, las cuales serán determinadas por la Oficina de Tecnología de la Información.
- Instalación y configuración del software de antivirus en las **estaciones** de trabajo de la entidad, ubicados en la Sede Principal y Sub Sedes de SUTRAN.
- Toda la solución debe estar basada únicamente en software, la solución no deberá incluir la adquisición de ningún tipo de equipamiento adicional como complemento de este.
- El software no debe afectar lentitud en los equipos de cómputo conectados a la Red de la SUTRAN.

Asimismo, el software antivirus a adquirir deberá contar como mínimo las siguientes características técnicas.

6.1.2. COMPATIBILIDAD:

El Software antivirus debe ser compatible con los siguientes sistemas operativos:

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:36:07 -05:00

Sistemas operativos de estaciones de trabajo (en versiones de 32/64 bits)

a) Microsoft Windows 11.
b) Microsoft Windows 10.
c) Microsoft Windows 7 SP 1
d) Microsoft Windows 8 (8.1).
e) Mac OS 10.14 o superior

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:31:51 -05:00

Sistemas operativos de servidores de red (en versiones de 32/64 bits)

a) Microsoft Windows 2003 Server
b) Microsoft Windows 2008 Server
c) Microsoft Windows 2012 Server
d) Microsoft Windows 2016 Server
e) Microsoft Windows 2019 Server
f) Microsoft Windows Small Business Server 2008.
g) Microsoft Windows Small Business Server 2011.

h) Citrix XenDesktop.
i) Citrix XenApp.
j) Red Hat Enterprise.
k) SUSE Enterprise Linux.
l) Oracle Linux.
m) Centos Linux.
n) Ubuntu LTS Server.

Smartphones y tablets

a) Apple iOS 10.0 o superior.
b) Android, 5.0 o superior.

6.1.3. CARACTERISTICAS INTERNAS:

a) La solución de seguridad para estaciones y servidores será de tipo integrada; es decir, incluye un único agente que brinda protección frente a virus, spyware, adware, rootkits, comportamientos sospechosos, filtrado de seguridad URL, detección Web de ataques de scripts maliciosos y aplicaciones potencialmente peligrosas en todos los protocolos de la red.
b) La solución debe contar con una herramienta para cuarentena de usuario final que permita controlar y/o autorizar el uso de ciertas aplicaciones no deseadas.
c) La solución contará con versiones para Linux por medio de un módulo de escaneo de archivos de alto rendimiento, estabilidad y eficacia el cual debe permitir el escaneado en acceso, en demanda y programado de unidades locales, extraíbles y compartidas (como NFS y Samba), y otros sistemas de archivos. La versión para Linux debe poder ser configurada y administrada desde la consola central.
d) La solución de seguridad instalada en todas las plataformas requeridas debe notificar los eventos de virus, spyware, adware, antispyware, anti troyano, antimalware, que verifique cualquier archivo creado, accedido o modificado aplicaciones no deseadas, intrusiones, cambios en la configuración del cliente de seguridad a la consola central.
e) El sistema de filtrado URL y el de detección Web de Ataques de Script maliciosos debe denegar el acceso al sitio y deber mostrar una página HTML de bloqueo en el navegador de internet (IE, Mozilla, Chrome, Opera, etc.).
f) La solución deberá incluir un sistema para el Control de acceso web a sitios inapropiados. Este sistema deberá estar integrado al agente antimalware y deben permitir notificar o bloquear el acceso a sitio web en base a categorías.
g) La solución permite la creación de CD, DVD o USB Booteables de emergencia mediante imágenes .ISO u otro formato de grabación de medios para la recuperación y limpieza de archivos infectados. La creación de dichas imágenes no deberá depender de productos de terceros ni requerir licenciamiento de productos adicionales al del propio fabricante.
h) Detectar en tiempo real cualquier archivo infectado que trate de ser ejecutado, leído, copiado hacia/desde el servidor/estación de trabajo. El código malicioso debe ser detenido antes de que pueda propagarse por la red. La tecnología de esta solución le permitirá tomar muestras de posibles archivos maliciosos y enviarlas de forma manual para su análisis.
i) La solución ofertada debe realizar un análisis detallado y a través del mismo reportar un diagnóstico profundo de la estructura del sistema, como librerías, aplicaciones instaladas, entre otras, que puedan tener un comportamiento sospechoso como consecuencia del ataque de algún malware.
j) La solución deberá contar con protección Anti-Ransomware que actué de forma proactiva ante un proceso de cifrado en las carpetas de red compartidas producido por un equipo remoto.
k) El módulo Anti-Ransomware debe permitir la definición granular de las carpetas a proteger los servidores del cliente

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:36:54 -05:00

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:31:59 -05:00

l) Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: "Win32.Trojan.banker") para que cualquier objeto detectado con el resultado elegido sea ignorado.

6.1.4. CONTROL DE DISPOSITIVOS:

a) Para la protección contra el malware en dispositivos externos, la solución deberá incluir un sistema de control de dispositivos que habilite o no el funcionamiento de los siguientes dispositivos externos.
b) El sistema de control de dispositivos estará integrado en el agente antimalware, es decir no requiere la instalación de programas adicionales en los equipos.
c) La solución debe tener la capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un periodo de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamiento central o de intervención local del administrador en la máquina del usuario.
d) La solución deberá tener un módulo que permita la implementación de políticas de seguridad para el control de dispositivos el mismo que deberá tener la capacidad de asignar privilegios de solo lectura a cualquier USB de almacenamiento externo que se conecte al equipo a fin de evitar que cualquier aplicación de peligro se escriba o ejecute desde este medio.
e) La solución deberá tener un módulo que permita la implementación de políticas de seguridad para el control de dispositivos el mismo que deberá permitir que el usuario pueda solicitar permiso de acceso a su dispositivo desde su PC.
f) La solución deberá tener un módulo que permita la implementación de políticas de seguridad para el control de dispositivos el mismo que deberá permitir la creación de listas blancas especificas construidas a partir del reconocimiento del ID del hardware de cada USB de almacenamiento.
g) La solución deberá permitir registrar los eventos de escritura y eliminación en las unidades extraíbles para los tipos de archivos de office, comprimidos, imágenes, audio, gráficos, base de datos, ejecutables y texto.

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:37:06 -05:00

6.1.5. PROTECCIÓN CONTRA ATAQUES DE DÍA CERO:

a) La solución deberá contar con tecnologías de detección proactiva de amenazas conocidas y basadas en la nube (in the cloud) del mismo fabricante. Vigilia proactiva ante amenazas del día 0, exploits.
b) La solución ofertada deberá ofrecer una rápida y eficaz detección de archivos sospechosos mediante la comprobación instantánea de archivos sospechosos en la nube.
c) El sistema de protección de filtrado URL realizando comprobaciones de direcciones web sospechosos (hackeadas, que albergan malware, etc.) en forma automática hacia la nube (base de datos del fabricante) para una rápida y efectiva protección contra este tipo de amenazas.

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:32:05 -05:00

6.1.6. SEGURIDAD:

a) El firewall será administrado de manera centralizada desde la consola de administración.
b) El firewall permitirá bloquear, autorizar aplicaciones y puertos específicos tanto local como centralizadamente.
c) Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas.
d) La solución incluye una tecnología de detección de intrusos de host (HIPS) incorporado en el agente antimalware que brinde protección en acceso.

e) La solución deberá incluir una tecnología para la detección de intentos de desbordamiento de buffers (BOPS – Buffer Overflow Protection System) incorporado en el agente antimalware.
f) La solución deberá contar con una tecnología de prevención y detección de intrusos que detecta malware antes de su ejecución (pre-execution) y en ejecución (on-execution).
g) El sistema HIPS no requiere ejecutar o instalar agentes o programas adicionales al motor antimalware ni ejecutarse en forma programada para la prevención y/o detección de intrusos de hosts, debe ser parte de la misma solución.
h) La solución debe ser capaz de evitar que sus procesos, servicios, archivos o archivos de registro puedan ser detenidos, deshabilitados, eliminados o modificados para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus.
i) La desinstalación del módulo o cliente y sus componentes debe estar protegido con una clave de seguridad asignada por el administrador de la solución. Esta clave puede ser configurada para un grupo específico o todos los equipos en la red.
j) La seguridad de la solución deberá integrarse al directorio activo de la red y con el sistema de grupos de Microsoft para una mejor y efectiva protección.
k) El usuario no podrá realizar una configuración particular a menos que el administrador de la red le otorgue privilegios ya sea localmente o mediante la integración con el Directorio Activo de Microsoft.
l) La solución deberá contar con un sistema de alertas para parches de (Microsoft) según su importancia.
m) La consola de administración deberá notificar la lista de equipos con vulnerabilidades de malwares o ataques específicos.
n) Cualquier intento de vulneración de las características de seguridad deberá ser reportado a la consola de gestión centralizada.
o) Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL).
p) Capacidad de verificar tráfico de enlaces phishings.
q) Capacidad de verificar enlaces introducidos en correos electrónicos contra phishings.
r) Capacidad de bloquear tráfico SSL en los browsers: Internet Explorer, Firefox y Opera.
s) Capacidad de verificación del cuerpo del correo electrónico y adjuntos usando heurística.
t) Capacidad de verificación de tráfico HTTP y cualquier script de Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas.
u) Debe tener módulo de bloqueo de Phishing, con actualizaciones incluidas en las vacunas, obtenidas por Anti-Phishing Working Group (http://www.antiphishing.org/).
v) Debe tener módulo que analice cada macro de VBA ejecutado, buscando por señales de actividad maliciosa.
w) Debe disponer funcionalidad de prevención ante ataques de BadUSB, el cual solicite o no al usuario validación del nuevo dispositivo.
x) La solución deberá contar con tecnologías de detección proactiva de amenazas basadas en la nube del mismo fabricante.
y) Debe contar con soportes a notificaciones utilizando Growl para sistema operativo MAC.
z) Deberá contar con un sistema de análisis en reposo capaz de escanear en busca de malware sin impactar en el performance de los equipos.

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:37:18 -05:00

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:32:14 -05:00

6.1.7. CONTROL DE APLICACIONES:

a) La solución debe controlar el uso de determinados tipos de aplicaciones en los equipos de la red.
b) El sistema de control de aplicaciones debe permitir la afinación de la configuración para agregar programas y/o aplicaciones que causan un impacto negativo en el trabajo de los usuarios, en el uso del ancho de banda en la red y el incumplimiento de políticas de seguridad de SUTRAN.
c) La entidad puede solicitar al fabricante y/o postor la inclusión de nuevos programas y/o aplicaciones en la configuración del producto que considere que deben bloquearse y que se requiera incluir en dicho sistema limitando la ejecución de aplicativos por hash SHA256, nombre de archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ejemplo, navegadores, gestor de descarga, juegos, aplicación de acceso remoto, etc), además de tener la capacidad de bloquear la ejecución de un aplicativo que este en almacenamiento externo.
d) Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de antivirus.
e) El control de aplicaciones debe disponer de un modo de bloqueo basado en listas blancas el cual debe permitir que solo determinadas aplicaciones se ejecuten.

6.1.8. MITIGACIÓN Y CONTINGENCIA DE AMENAZAS DE DÍA CERO:

a) La solución debe contar con un módulo de análisis de vulnerabilidades y gestión de parches capaz de reconocer desde la consola todas las vulnerabilidades que derivan del sistema operativo y programas instalados en PCs y servidores.
b) El módulo de análisis de vulnerabilidades y gestión de parches deberá ser capaz de clasificar los parches que necesitan aplicarse en las estaciones de trabajo y servidores a fin de cerrar los huecos de seguridad encontrados, así como lanzar pruebas de aplicabilidad de los mismos a fin de asegurarse de que estos no ocasionen problemas de compatibilidad.

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:37:54 -05:00

6.1.9. ACTUALIZACIÓN DE BASE FIRMAS Y COMPONENTES DEL PRODUCTO

a) Las actualizaciones del fichero de firmas de virus y del motor de escaneado de malware en los servidores y estaciones de trabajo se realizan automáticamente (programadas) y manualmente desde internet.
b) La actualización de firmas automáticas deberá realizarse cada 30 minutos o según periodo programado.
c) El tamaño de las actualizaciones de firmas de virus es pequeño de tal modo que no tenga un impacto negativo en el tráfico de la red.
d) La actualización de nuevas versiones del producto se puede realizar automáticamente y no requiere la desinstalación y/o reinstalación de algún componente previo, estas actualizaciones son incrementales.
e) La solución permite programar la comprobación de nuevas versiones de la solución al menos 12 horas y programar la instalación automática de ellas en horas de menos tráfico de red. Para este fin, la solución debe contar con opciones para la programación del horario por día y hora especificada.
f) Debido a que el cliente no cuenta con servidores dedicados en alguna sede remota, la solución debe permitir distribuir actualizaciones a hosts cliente de grupos de administración, no solo a través del servidor de Administración, sino a través de agentes de actualización de estos grupos. Un Agente de actualización debe ser un equipo dentro de la red del servidor de Administración dedicado a almacenar y

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:37:41 -05:00

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:32:23 -05:00

distribuir actualizaciones de bases de datos, paquetes de instalación, tareas de grupo y directivas. Es un centro para almacenamiento provisional de bases de datos, paquetes de instalación, tareas de grupo y directivas. Puede asignar un Agente de actualización en cualquier grupo de administración. La función principal de un Agente de actualización es la distribución (actualización) de bases de datos y paquetes de instalación en todos los equipos cliente en ese grupo, así como la ejecución de tareas de grupo y directivas del servidor de Administración.

g) La funcionalidad de agentes de actualización debe poder solucionar el problema de distribución de firmas, directivas y tareas a una organización con muchas oficinas remotas logrando ahorro del tráfico VPN y la no dependencia de equipos adicionales para que hagan la función de servidores de administración esclavos.
h) La implementación de la función de agentes de actualización no debe demandar recursos adicionales a los ya dispuestos para la protección de estaciones de trabajo (PCs).
i) Ningún software instalado en los equipos de cómputo de los usuarios del cliente debe bloquear la instalación del antivirus, La actualización del producto debe ser transparente.

6.1.10. CONSOLA DE ADMINISTRACIÓN

a) La solución deberá contar con una consola de administración centralizada desde donde se pueda administrar y controlar todos los componentes de la solución ofertada en forma centralizada y distribuida. Debe disponer de Compatibilidad con Windows Failover Clustering u otra solución de alta disponibilidad.
b) La solución debe disponer de una interfaz de administración MMC y Web (HTTPS) y/o MMC.
c) La herramienta deberá tener incluido la capacidad de gestión de las políticas de control de acceso a la red sin requerir instalar productos adicionales, y con capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación;
d) El servidor de la consola de administración debe poder instalarse en sistemas operativos Windows.
e) La consola debe permitir la administración simultáneamente de equipos y servidores Windows, Linux (Mac opcional).
f) La herramienta deberá ser escalable y debe permitir la administración de complejas redes, permitiendo la administración centralizada y distribuida de más de 4000 a más equipos desde una sola consola, interconectando varias consolas para optimizar el ancho de banda y para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes.
g) La consola debe sincronizarse con el Directorio Activo para la instalación automática de la solución de seguridad en los equipos, debe tener la capacidad de instalar remotamente la solución de seguridad de endpoint en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory.
h) La administración deberá estar basada en políticas para Actualización, Opciones Antimalware, HIPS, Control de Aplicaciones, Control de Dispositivos y Firewall.
i) Capacidad de monitorear diferentes subnets de red con el objetivo que cuando se detecten máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente se importe la máquina para la estructura de protección de la consola y se verifique si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente.
j) Cualquier cambio en las políticas deberán desplegarse automáticamente a todos los equipos (computadoras, servidores), debe tener la capacidad de actualizar los paquetes de instalación con las últimas vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas.

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:38:08 -05:00

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:32:33 -05:00

k) Debe contar con filtros de control que permitan detectar de forma rápida los equipos no protegidos o los que no cumplen con las políticas de seguridad.
l) El administrador deberá poder crear políticas desde la consola para evitar el uso de aplicaciones no deseadas, así como eliminar, autorizar y limpiar las mismas en los clientes.
m) La consola deberá poder utilizar al menos 3 tipos diferentes de mecanismos para detectar equipos en la red (TCP/IP, Active Directory y otros).
n) La consola deberá ser capaz de determinar equipos que cumplan con las políticas centrales y/o fueron modificadas localmente. Eventualmente deberá poder "forzar" a los equipos a cumplir con las políticas centrales con tan solo indicarlo.
o) La consola deberá contar con un sistema de reportes y mecanismos de notificación de eventos vía correo electrónico.
p) La consola deberá almacenar un histórico de eventos de cada equipo administrado pudiéndose conocer también el nombre del equipo, descripción, SO, Service Pack, IP, Grupo, última actualización, eventos de error, etc. Accesibles desde la misma consola.
q) La consola deberá administrar el sistema de prevención contra intrusiones de host (HIPS) y el sistema de protección contra desbordamiento de buffers (BOPS) como políticas de seguridad.
r) El sistema para la delegación de roles deberá contener un administrador de permisos, pudiendo crear distintos perfiles con permisos particulares para cada administrador.
s) La consola deberá permitir crear excepciones para el control de dispositivos (control total, solo lectura y bloqueo) y filtro web (por nombre de dominio, dirección IP y dirección IP con mascará de subred) para un grupo particular de equipos o toda la red.
t) Debe incluir la capacidad para la desinfección y limpieza remota de adware/aplicaciones potencialmente peligrosas, así como también de virus, troyanos, gusanos, rootkits y spyware.
u) La consola deberá permitir acceder a un sistema de visualización y búsqueda de eventos para las políticas de HIPS, dispositivos y firewall. Asimismo, debe proporcionar la siguiente información de las computadoras:
   - ✓ Si el antivirus está instalado;
   - ✓ Si el antivirus ha iniciado;
   - ✓ Si el antivirus está actualizado;
     - ✓ Minutos/horas desde la última conexión de la máquina con el servidor administrativo;
     - ✓ Minutos/horas desde la última actualización de vacunas
     - ✓ Fecha y horario de la última verificación ejecutada en la máquina;
     - ✓ Versión del antivirus instalado en la máquina;
     - ✓ Si es necesario reiniciar la computadora para aplicar cambios;
     - ✓ Fecha y horario de cuando la máquina fue encendida;
     - ✓ Cantidad de virus encontrados (contador) en la máquina;
     - ✓ Nombre de la computadora;
     - ✓ Dominio o grupo de trabajo de la computadora;
     - ✓ Fecha y horario de la última actualización de vacunas;
     - ✓ Sistema operativo con Service Pack;
     - ✓ Vulnerabilidades de aplicativos instalados en la máquina
v) La consola debe de disponer de una herramienta nativa de Backup que permita salvaguardar todas las configuraciones todas las bases de datos, realizadas en el sistema, sin necesidad de detener los servicios, para una posterior recuperación de los mismo.

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:38:27 -05:00

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:32:41 -05:00

6.1.11. ADMINISTRACIÓN DE LICENCIAS.

La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso se restaure el sistema o cambie de equipo, por parte de la Entidad.

6.1.12. ALERTAS Y REPORTES

a) La solución deberá ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alerta de registros, etc.)
b) La solución podrá generar reportes gráficos, imprimibles y exportables de la cobertura de versiones, actualizaciones e infecciones.
c) La solución deberá contener un sistema de reportes que permitir ver el estado de la protección de la red en línea. Este sistema debe mostrar en tiempo real lo que está ocurriendo en la red.
d) La solución deberá incorporar un sistema de reportes que permita programar la creación y envió de reportes en formato PDF y HTML y XML vía correo electrónico en una determinada hora y fecha de día.
e) Capacidad de realizar inventario de hardware de todas las máquinas clientes.
f) Capacidad de realizar inventario de aplicativos de todas las máquinas clientes.
g) Capacidad de diferenciar máquinas virtuales de máquinas físicas.

6.1.13. NAVEGACIÓN HTTP / HTTPS:

a) Deberá revisar y detectar virus en las comunicaciones que se efectúen por medio de los navegadores web.
b) Deberá revisar y bloquear códigos maliciosos de Internet.
c) Deberá tener un filtro de URL's de páginas web.
d) Deberá permitir hacer reglas de restricción de navegación basado en el nombre de host, IP y/o grupos.
e) Un nuevo componente de seguridad del tráfico: ahora puede proteger su servidor de las amenazas web enviadas a través del tráfico HTTP o HTTPS y de otras amenazas basadas en el correo electrónico. Este nuevo componente admite los siguientes escenarios de protección:
   - ✓ Protección antivirus y antiphishing del tráfico de correo electrónico mediante una extensión de Microsoft Outlook.
   - ✓ Protección antivirus y antiphishing del tráfico web.
   - ✓ Verificación de enlaces utilizando bases de datos de direcciones web maliciosas.
   - ✓ Verificación de enlaces utilizando bases de datos basadas en la nube de direcciones web maliciosas.
   - ✓ Control de recursos web basado en categorías.

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:38:45 -05:00

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:32:48 -05:00

6.1.14. TRANSFERENCIA DE CONOCIMIENTO.

- El contratista deberá brindar una capacitación integral para el personal técnico de la SUTRAN, la misma que podrá realizarse de manera presencial o virtual.
- El postor dará una capacitación técnica sobre el funcionamiento del software de antivirus ofertado con una duración de cinco (5) horas como mínimo.
- La capacitación será brindada para un total de cuatro (04) personas como mínimo.
- El contenido de la capacitación deberá desarrollar como mínimo los siguientes temas:

- Instalación
- Configuración
- Administración
- Solución de problemas sobre los componentes de la herramienta
- Durante el curso de capacitación el oferente deberá realizar pruebas de ataques reales, infectando una máquina de prueba
- Despliegue de políticas de seguridad de las consolas y sub consolas instaladas en la red de SUTRAN.

- El expositor deberá ser un personal certificado por el fabricante, el cual deberá contar por lo menos con una experiencia de dos (02) años en el uso y administración de la herramienta antivirus.
- Al finalizar la capacitación, el contratista deberá otorgar certificados de Operador y Administrador de Consola del producto adquirido a los participantes.

6.1.15. SOPORTE TÉCNICO.

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:39:41 -05:00

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:32:58 -05:00

a) Soporte y actualización de licencias antivirus por el periodo de ejecución del servicio.
b) El contratista debe contar con soporte técnico 24x7x365 con la posibilidad de escalar casos técnicos en cualquier momento hacia la casa matriz haciendo uso del sistema del fabricante.
c) El contratista brindará los datos como números telefónicos y correos electrónicos para las coordinaciones y comunicación con la Entidad.
d) Si en caso la llamada realizada por el personal de soporte técnico no tuviera éxito en contactarse, se procederá a enviar un correo electrónico que deberá asignar el contratista para la atención inmediata, una vez realizado él envió el contratista tendrá que devolver la llamada en un tiempo máximo de 180 minutos.
e) Si se presenta cualquier incidencia o vulnerabilidad en la red de la solución de seguridad del contrato, el área usuaria reportará la incidencia a través de correo electrónico y el contratista tendrá un tiempo de respuesta de 04 horas como máximo desde reportada la incidencia, para dar solución a la incidencia reportada.
f) El proveedor podrá brindar el soporte de forma remota, para lo cual se le brindará el acceso respectivo para evaluar la incidencia y atenderla. Luego de atendida la incidencia, el proveedor deberá remitir un correo electrónico indicando la culminación de la atención.
g) En caso la incidencia no pueda ser atendida de forma remota, el proveedor asignará un técnico el cual se apersonará a las instalaciones de la Entidad, dentro de las 24 horas siguientes de ser reportada la incidencia.

6.2. CONSIDERACIONES PARA LA EJECUCIÓN DEL SERVICIO:

a) A fin de poder elaborar su mejor propuesta, el contratista podrá realizar una visita a la Oficina de Tecnología de Información y solicitar la información pertinente, durante los horarios de oficina (8:30 am – 5:30 pm), a fin de obtener un mejor conocimiento de la implementación, equipamiento técnico, necesidades de configuración de los equipos u otros componentes, que tengan que incluir en la implementación y ejecución del requerimiento.
b) El contratista deberá garantizar la operatividad de los servicios ininterrumpido durante el período de inicio de la implementación.
c) Cualquier solicitud posterior de reconfiguración del servidor donde se instalará la consola de antivirus, deberá realizarse sin costo adicional para SUTRAN.
d) El software de antivirus provisto por el contratista debe cumplir con las características técnicas propuestas.

e) El contratista deberá de realizar la configuración y despliegue de la solución de software antivirus ofertada en las computadoras personales de la entidad. Estas labores serán supervisadas y coordinadas con la Oficina de Tecnología de Información.

7. REQUERIMIENTO DEL PROVEEDOR Y DE SU PERSONAL.

7.1. Del Proveedor.

El Postor deberá de presentar documentación que acredite lo siguiente:

a. **Perfil**

- ✓ Ser persona jurídica
- ✓ No tener impedimento para contratar con el Estado, conforme al artículo 11° de la Ley de Contrataciones del Estado.
- ✓ Registro Único de Contribuyente (RUC) vigente.
- ✓ Registro Nacional de Proveedores (RNP) vigente.
- ✓ El Postor deberá acreditar la autorización o representación otorgada por el fabricante de las licencias ofertadas mediante una carta simple.

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:39:25 -05:00

b. **Experiencia**

El postor debe acreditar un monto facturado acumulado mínimo de S/.50,000.00 (cincuenta mil con 00/100 soles) por la contratación de servicios de instalación de soluciones de software de antivirus o de venta de licencias de software antivirus, durante los cinco (05) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:33:07 -05:00

c. **Acreditación**

Copia simple de contratos u ordenes de servicio, y su respectiva conformidad; o comprobantes de pago cuya cancelación se acredita documental y fehacientemente, con voucher de depósito, reporte de estado de cuenta, cancelación en el documento, entre otros, correspondientes a un máximo de veinte (20) contrataciones

7.2. Del Personal clave.

El contratista deberá de proponer el siguiente personal especializado para el desarrollo de las labores y despliegue y configuración del antivirus ofertado.

Un (01) Especialista.

Formación:
Profesional bachiller o titulado en: Ingeniero Eléctrico o Ingeniero Electrónico o Ingeniero Industrial o Ingeniero Sistemas o Ingeniero Informático o Ingeniero de Software o Ingeniero Industrial.
Experiencia:
Deberá contar con tres (03) años de experiencia en actividades relacionadas a la configuración de antivirus como especialista en Sistemas de software de antivirus corporativo.

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:33:18 -05:00

Capacitación:
Curso relacionado a la configuración de Sistemas de software de antivirus corporativo, otorgada por el fabricante del software de antivirus propuesto.

Acreditación:
Se deberá adjuntar constancias y/o certificados que acrediten la experiencia y la capacitación.

8. PLAZOS DE EJECUCIÓN DEL SERVICIO.

- El plazo máximo para la configuración y despliegue de la solución de software antivirus, así como para la transferencia de conocimiento será de quince (15) días calendarios contabilizados a partir del día siguiente de la suscripción del contrato o aceptación de la orden de servicio.

  Culminado la configuración y despliegue del software antivirus, el contratista emitirá un acta de despliegue y configuración de las licencias desplegadas el cual estará suscrita por el personal de OTI y el proveedor.

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:39:11 -05:00

- La suscripción de las licencias de software antivirus tendrá una vigencia de trecientos sesenta y cinco (365) días calendarios, el cual iniciará desde el vencimiento del actual licenciamiento o contrato vigente en la entidad.

9. LUGAR DE ENTREGA

La prestación del servicio será realizada en la sede central de la SUTRAN ubicado en Av. Arenales N°452, Jesús María, Lima.

10. FORMA DE PAGO.

La Entidad se obliga a pagar la contraprestación al Contratista en soles, en un único pago, previa conformidad emitida por la Oficina de Tecnología de Información (OTI) y recepción del comprobante de pago.

Para efecto de los pagos, el Contratista deberá presentar el comprobante de pago a través de mesa de partes virtual de la SUTRAN (http://www.sutran.gob.pe/mesa-de-partes-virtual/) o en físico a través de la plataforma de atención al ciudadano ubicado en la Av. Arenales 452 – Jesús María – Lima – Perú.

Los pagos obligatoriamente se efectuarán a través del abono en la respectiva cuenta interbancaria (CCI) abierta en alguna de las entidades del Sistema Financiero Nacional, dentro de los quince (15) días calendarios de otorgada la conformidad de la prestación.

11. CONFORMIDAD

La conformidad será emitida por la Oficina de Tecnología de Información (OTI), conforme con la Directiva N.º D004-2021-SUTRAN/05.1.1-001 V01.

12. PENALIDADES

La aplicación de penalidades por retraso injustificado en la atención del servicio requerido, según el plazo máximo establecido en el presente documento, será teniendo en cuenta que

para contrataciones de hasta 8UITs el monto máximo equivalente es de 5%, precisando la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.05 \times \text{Monto vigente}}{\text{“F” x Plazo vigente en días}}$$

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:33:26 -05:00

Donde “F” tiene los siguientes valores:

a. Para plazos menores o iguales a sesenta (60) días: “F” = 0.40
b. Para plazos mayores a sesenta (60) días: “F” = 0.25

13. CONFIDENCIALIDAD

El proveedor guardará, bajo responsabilidad a que hubiere lugar, estricta confidencialidad respecto de la información a la que acceda para la realización de sus actividades, así como de la información que produzca, la cual es de propiedad de la SUTRAN. Queda prohibida la utilización de la información proporcionada para un fin distinto al contratado, así como expresamente se prohíbe su divulgación por cualquier medio.

14. INCUMPLIMIENTO.

El incumplimiento de las obligaciones contenidas en el presente contrato constituye causal de resolución automática del contrato. La entidad, por decisión unilateral, podrá resolver el presente contrato, sin pago de indemnización por ningún concepto al proveedor, a simple solicitud de la Entidad. Para ello, la Entidad comunicara por escrito al domicilio o correo electrónico del proveedor, sobre la resolución del contrato. Las causales para la resolución del contrato, serán aplicadas de conformidad con el artículo 36 de la Ley y 164 del Reglamento.

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:38:57 -05:00

15. RESPONSABILODAD POR VICIOS OCULTOS.

El plazo máximo de responsabilidad del Contratista será de un (01) año contado a partir de la conformidad otorgada por la entidad.

16. ANTICORRUPCION

EL CONTRATISTA 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 puedan constituir un incumplimiento a la ley, tales como robo, fraude, cohecho o tráfico de influencias, directa o indirectamente, o a través de socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas, en concordancia a lo establecido en el artículo 11° de la Ley de contrataciones del Estado - Ley N° 30225, al numeral 7.1 del artículo 7° de su Reglamento Ley de Contrataciones del Estado aprobada mediante D.S N° 344-2018, y la vigente “Directiva que regula la contratación de bienes y servicios por montos menores o iguales a ocho (08) Unidades Impositivas Tributarias Vigentes de la SUTRAN” aprobado con código normativo D-004-2021-SUTRAN/05.1.1.-001 V01 mediante Resolución de Gerencia General N°029-2021-SUTRAN-GG.

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, participacioncitas, integrantes de los 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 del Estado y su Reglamento.

EL CONTRATISTA 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, organizacionales y/o de personal apropiadas para evitar los referidos actos o prácticas, a través de los canales dispuestos por la SUTRAN." De la misma manera, EL CONTRATISTA es consciente que, de no cumplir con lo anteriormente expuesto, se someterá a la resolución del Contrato y las Acciones Civiles y/o Penales que la SUTRAN pueda accionar".

.

Firmado digitalmente por TORRES ARROYO Jorge Antonio FAU 20536902385 soft
Motivo: Soy el autor del documento
Fecha: 27.10.2023 10:40:15 -05:00

Firmado digitalmente por CHAVEZ SIERRA Deyvid Valerio FAU 20536902385 soft
Motivo: Doy V° B°
Fecha: 27.10.2023 10:33:36 -05:00