



PERÚ

Ministerio del Interior

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"  
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

## REQUERIMIENTO

### A. ESPECIFICACIONES TÉCNICAS

#### I. DENOMINACIÓN DE LA CONTRATACIÓN (Obligatorio)

Adquisición de software antivirus para las estaciones de trabajo y servidores del Ministerio del Interior.

#### II. FINALIDAD PÚBLICA (Obligatorio)

Mantener la continuidad de los servicios de TI brindados por el Ministerio del Interior a favor del ciudadano, a partir de la adecuada detección y protección de los equipos de la red corporativa, frente a diversos ataques cibernéticos por parte de software no deseado y virus informáticos.

#### III. ACTIVIDAD DEL POI VINCULADA A LA CONTRATACIÓN (Obligatorio)

La presente contratación de servicio se encuentra enmarcada dentro del POI 2024 del Ministerio del Interior, Objetivo Estratégico Institucional N° 8: Fortalecer la gestión institucional en el Ministerio del Interior, Acción Estratégica Institucional N° 08.01: Procesos Operativos y Administrativos Optimizados para el fortalecimiento institucional.

Actividad POI COD AOI00002500120 Gestión de los Servicios Tecnológicos y de Comunicaciones.

#### IV. OBJETIVO DE LA CONTRATACIÓN (Obligatorio)

Adquirir una solución antivirus para la detección, protección y corrección de ciberataques de software malicioso (malware) y amenazas emergentes, que permitan mantener la confidencialidad, la disponibilidad e integridad de datos e información almacenada en las estaciones de trabajo; así como en los servidores del Ministerio del Interior.

#### V. ALCANCE Y DESCRIPCIÓN DE LOS BIENES A CONTRATAR (Obligatorio)

##### 5.1. DESCRIPCIÓN Y CANTIDAD DE LOS BIENES

Ítem	Descripción	Instalación	Cantidad	Cantidad Total	Unidad de Medida	Vigencia
1	ADQUISICIÓN DE SOLUCIÓN ANTIVIRUS PARA MINISTERIO DEL INTERIOR (*)	MININTER	2, 649	2,983	Unidades	3 años
		MININTER- DIGIMIN	334			
		MININTER- PROCURADURIAS	353	353	Unidades	1 año

(\*) La adquisición debe incluir como mínimo dos (02) consolas de administración centralizadas, las cuales estarán destinadas para ser instaladas, dentro de las instalaciones de nuestra Entidad, una en la sede MININTER y otra en sede MININTER-DIGIMIN.

**PERÚ****Ministerio del Interior***"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"**"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"*

Descripción	Instalación	Equipo	Cantidad	Cantidad Total	Unidad de Medida	Vigencia
<b>ADQUISICIÓN DE SOLUCIÓN ANTIVIRUS PARA MINISTERIO DEL INTERIOR (*)</b>	MININTER	Estaciones de Trabajo Windows	2120	2649	Unidades	3 años
		Estaciones de Trabajo MAC	7			
		Laptops Windows	440			
		Laptops MAC	1			
		Servidores Windows	49			
		Servidores Linux	32			
	MININTER-DIGIMIN	Estaciones de Trabajo Windows	258	334	Unidades	1 año
		Laptops Windows	58			
		Servidores Windows	18			
	MININTER-PROCURADURIAS	Estaciones de Trabajo Windows	283	353	Unidades	1 año
		Laptops Windows	70			

(\*) La adquisición debe incluir como mínimo dos (02) consolas de administración centralizadas, las cuales estarán destinadas para ser instaladas, dentro de las instalaciones de nuestra Entidad, una en la sede MININTER y otra en sede MININTER-DIGIMIN.

EL PROVEEDOR al momento de presentar su oferta, deberá presentar documentación técnica (brochures o datasheet o catálogos o manuales o folletos, dichos documentos podrán ser presentados en su idioma *original*) *en cumplimiento al artículo 59 del reglamento de contrataciones*, donde evidencie el cumplimiento de las características técnicas mínimas, para lo cual deberá adjuntar un cuadro comparativo de las características solicitadas versus las ofertadas y el número de folio donde se evidencia el cumplimiento y/o carta emitida por el fabricante donde se confirme el cumplimiento de las características técnicas mínimas, la misma que deberá estar acompañada de su debida traducción por traductor público juramentado o traductor colegiado, certificado, según corresponda.

## 5.2. CARACTERÍSTICAS TÉCNICAS MÍNIMAS

A continuación, se describen las características técnicas mínimas:

### 5.2.1. Características técnicas mínimas de la solución ANTIVIRUS PARA ESTACIONES DE TRABAJO

Nº	Características Técnicas Mínimas	Descripción
1	Compatibilidad	El software debe ofrecer soporte multiplataforma, siendo compatible con sistemas operativos de 64 bits, incluyendo Windows 10 y versiones superiores así como Mac OS 14.x y versiones superiores.



*"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"*

*"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"*

	Características Técnicas Mínimas	Descripción
2	Detección y Prevención de Malware y Amenazas Emergentes	La protección proporcionada por el software debe incluir, como mínimo, detección basada en firmas, análisis de comportamiento, técnicas heurísticas, evaluación de la reputación de archivos y detección basada en métodos de aprendizaje automático (machine learning) y/o inteligencia artificial.
3		El software antivirus debe ofrecer protección mínima contra una amplia gama de amenazas, incluyendo virus, troyanos, macro virus, adware, spyware, gusanos, keyloggers, rootkits, ransomware (como Locky, WannaCry, Petya y otros), así como cualquier otro tipo de software malicioso (malware), ataques de día cero y amenazas emergentes.
4		El software debe monitorear y bloquear cambios no autorizados en el sistema y en el agente antivirus, incluyendo modificaciones en el registro, así como la creación de archivos y carpetas en áreas no permitidas del sistema operativo (opcional). <sup>1</sup>
5		El software deberá detectar y eliminar el malware detectado
6		El software debe proporcionar protección tanto contra vulnerabilidades nuevas como existentes.
7		El software debe permitir realizar acciones sobre el malware detectado, como desinfectar, eliminar, enviar a cuarentena, o solicitar la acción del usuario, tanto durante el escaneo en tiempo real como en el escaneo manual.
8		El software debe ser capaz de analizar archivos comprimidos en formatos como ZIP, RAR, 7-Zip, TAR, y GZ.
9		El software debe ofrecer opciones para incluir o excluir programas que podrían ser detectados como sospechosos, tales como instaladores de aplicaciones internas, actualizadores de programas u otras aplicaciones.
10	Protección en Tiempo Real	El software debe ser capaz de identificar y bloquear ataques de día cero y ransomware sin necesidad de actualizaciones de firmas, y estas capacidades deben estar integradas directamente en el motor antimalware.
11		El software debe incluir protección contra vulnerabilidades conocidas en las estaciones de trabajo especificados en el numeral 1 del presente cuadro.
12		El software debe detectar la presencia de botnets en la LAN mediante el análisis del tráfico de consultas DNS en el host, así como identificar ransomware y amenazas avanzadas (ATP).
13		El software debe ser capaz de analizar las unidades de red.
14		El software debe ser capaz de revisar la reputación de los archivos en tiempo real para detectar y bloquear malware sospechoso o desconocido de manera inmediata.
15	Actualizaciones	El software debe permitir la gestión y actualización a través de una consola centralizada.
16		La instalación y actualización del software antivirus para estaciones de trabajo se podrá realizar tanto desde la red institucional como fuera de ella a través de internet.
17	Protección Web	El software debe permitir el bloqueo de cookies maliciosas y/o cookies de seguimiento de navegación creadas por los navegadores.
18		El software debe permitir la navegación basada en la reputación de los sitios web, bloqueando el acceso a aquellos clasificados como inseguros. La evaluación de la reputación de los sitios se realizará mediante consultas a la nube de seguridad del fabricante.
19		El software debe permitir la creación de una lista de sitios de confianza, a los cuales los usuarios podrán acceder sin necesidad de consultar la reputación de estos sitios. La funcionalidad debe admitir la inclusión de dominios completos (por ejemplo, ejemplo.com) y subdominios (por ejemplo, www.ejemplo.com).
20		El software debe permitir la creación de una lista de sitios no permitidos, bloqueando el acceso a estos sitios sin necesidad de consultar la reputación de los mismos. La funcionalidad debe admitir la inclusión de dominios completos (por ejemplo, ejemplo.com) y subdominios (por ejemplo, www.ejemplo.com).
21		El software debe proteger la navegación de los usuarios en sitios bancarios y sitios confiables que utilicen el protocolo HTTPS, con el fin de prevenir ataques de phishing y el robo de datos personales.

<sup>1</sup> Texto actualizado a razón de la consulta N° 10 de BAFING S.A.C.



*"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"*

*"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"*

	Características Técnicas Mínimas	Descripción
22	Escaneo	El software debe realizar una exploración automática inicial tras su instalación para garantizar que la estación de trabajo esté protegida desde el primer momento.
23		El software debe permitir realizar análisis manuales de archivos, con opciones para configurar el escaneo de todos los archivos o de archivos con extensiones específicas.
24		El software debe permitir realizar análisis manuales con opciones de prioridad normal o en segundo plano, para evitar interrumpir las actividades de los usuarios.
25		El software debe permitir, como mínimo, la exclusión de archivos, extensiones, carpetas y unidades, tanto para el escaneo en tiempo real como para el escaneo manual.
26	Firewall Integrado.	El software debe incluir un cortafuego personal (firewall) avanzado que permita bloquear el tráfico malicioso en la LAN.
27		Opcionalmente, el firewall podrá incluir un Sistema de Prevención de Intrusiones (IPS) a nivel de host y/o un Sistema de Prevención de Intrusiones Basado en Host (HIPS), ambos con la capacidad de operar de manera independiente.
28		El firewall deberá desactivar automáticamente el firewall de Windows para evitar conflictos de configuración y garantizar una protección unificada.
29		El firewall deberá permitir la configuración de reglas personalizadas en los perfiles predefinidos del software.
30	Control de Dispositivos y Periféricos.	El software debe permitir la creación de políticas para gestionar el acceso a los dispositivos, incluyendo la capacidad de permitir o bloquear la escritura y el acceso.
31		El software debe permitir la creación de múltiples grupos de dispositivos, con la capacidad de aplicar reglas diferentes a cada grupo. Además, debe permitir la detección automática de los dispositivos conectados a la PC y su inclusión en el listado de grupos de dispositivos.
32		El software debe permitir la detección de dispositivos de los siguientes tipos: USB Mass Storage, DVD/CD-ROM, módems y cámaras.
33	Inducción	Se deberá proporcionar un entrenamiento básico sobre la instalación, configuración, actualización y resolución de problemas del software antivirus en estaciones de trabajo. Este entrenamiento estará dirigido a 6 profesionales de la Entidad y tendrá una duración mínima de 02 horas, realizándose de manera presencial en las instalaciones de la Entidad o de forma virtual (en línea con el expositor). El expositor deberá ser personal certificado por el fabricante de la solución propuesta. Se entregarán certificados de participación a los profesionales designados por la Entidad, y además, se proporcionarán enlaces oficiales de la marca para autoaprendizaje.

### 5.2.2. Características técnicas mínimas de la solución ANTIVIRUS PARA SERVIDORES FÍSICOS y VIRTUALES

Nº	Características Técnicas Mínimas	Descripción
1	Compatibilidad	Como mínimo, el software debe ser compatible con los siguientes sistemas operativos de servidor 64 bits: Microsoft Windows 2016, 2019, 2022 Y sistemas operativos Linux, incluyendo CentOS, Red Hat y Ubuntu, tanto para entornos virtuales y físicos. Para los sistemas operativos Linux Centos se considerará versiones compatibles de la solución ofertada. <sup>2</sup>
2		El software debe optimizar el uso de recursos para no impactar con los servicios desplegados en los servidores: - Optimizar el consumo de recursos, como memoria, CPU y espacio en disco, en máquinas virtuales.

<sup>2</sup> Texto actualizado a razón de la consulta N° 11 de BAFING S.A.C



*"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"*

*"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"*

Nº	Características Técnicas Mínimas	Descripción
3	Detección y Prevención de Malware y Amenazas Emergentes	La protección proporcionada por el software debe incluir, como mínimo, detección basada en firmas, análisis de comportamiento, técnicas heurísticas, evaluación de la reputación de archivos y detección basada en métodos de aprendizaje automático (machine learning) y/o inteligencia artificial.
4		El software antivirus debe ofrecer protección mínima contra una amplia gama de amenazas, incluyendo virus, troyanos, macro virus, adware, spyware, gusanos, keyloggers, rootkits, ransomware (como Locky, WannaCry, Petya y otros), así como cualquier otro tipo de software malicioso (malware), ataques de día cero y amenazas emergentes.
5		El software debe ofrecer opciones para incluir o excluir programas que podrían ser detectados como sospechosos, tales como instaladores de aplicaciones internas, actualizadores de programas u otras aplicaciones.
6		El software debe permitir realizar acciones sobre el malware detectado ya sea para desinfectar, eliminar, preguntar por la acción al Administrador del Servidor o enviar a la cuarentena tanto para el escaneado en tiempo real como para el escaneado manual.
7		El software como mínimo deberá incluir la protección contra vulnerabilidades nuevas y existentes.
8	Protección en Tiempo Real	El software debe ser capaz de identificar y bloquear ataques de día cero y ransomware sin necesidad de actualizaciones de firmas, y estas capacidades deben estar integradas directamente en el motor antimalware.
9		El software debe incluir protección contra vulnerabilidades conocidas en los servidores especificados en el numeral 1 del presente cuadro.
10		El software debe monitorear y bloquear cambios no autorizados en el sistema y en el agente antivirus, incluyendo modificaciones en el registro, así como la creación de archivos y carpetas en áreas no permitidas del sistema operativo (Opcional). <sup>3</sup>
11		El software debe detectar la presencia de botnets en la LAN mediante el análisis del tráfico de consultas DNS en el host, así como identificar ransomware y amenazas avanzadas (ATP).
12		El software debe ser capaz de analizar las unidades de red.
13		El software debe ser capaz de analizar archivos comprimidos en formatos como ZIP, RAR, 7-Zip, TAR, y GZ.
14		El software debe ser capaz de revisar la reputación de los archivos en tiempo real para detectar y bloquear malware sospechoso o desconocido de manera inmediata.
15	Actualizaciones	El software debe permitir la gestión y actualización a través de una consola centralizada.
16		La instalación y actualización del software antivirus para servidores debe poder realizarse desde la red institucional.
17	Escaneo	El software debe permitir realizar análisis manuales de archivos, con opciones para configurar el escaneo de todos los archivos o de archivos con extensiones específicas.
18		El software debe permitir realizar análisis manuales con opciones de prioridad normal o en segundo plano, para evitar interrumpir las actividades de los Administradores.
19		El software debe permitir, como mínimo, la exclusión de archivos, extensiones, carpetas y unidades, tanto para el escaneo en tiempo real como para el escaneo manual.
20	Inducción	Se deberá proporcionar un entrenamiento básico respecto a la instalación, configuración, actualización y resolución de problemas del software antivirus en Servidores, el cual estará dirigido a 6 profesionales de la Entidad, con un tiempo mínimo de duración de 02 horas, a realizarse de manera presencial en las instalaciones de la Entidad o de manera virtual (en línea con el expositor), siendo el expositor, personal certificado por el fabricante de la solución propuesta. Se deberá entregar certificados de participación a los profesionales designados por la Entidad, así mismo se deberá proporcionar links oficiales de la marca para autoaprendizaje.

<sup>3</sup> Texto actualizado a razón de la consulta N° 12 de BAFING S.A.C.



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

### 5.2.3. Características técnicas mínimas de la Consola Centralizada de Administración de la solución ANTIVIRUS

Nº	Características Técnicas Mínimas	Descripción
1	Instalación	Para la instalación de las dos consolas centralizadas, una en la sede MININTER y otra en la sede MININTER-DIGIMIN, la entidad suministrará los recursos de hardware necesarios para implementar los dos servidores virtuales. El proveedor deberá entregar todas las licencias necesarias para su correcta implementación y funcionamiento, incluyendo las del sistema operativo.
2		La consola de administración centralizada debe poder instalarse en sistemas operativos, Windows 2016, Windows 2019 o Superior, así como en servidores Linux.
3	Interfaz	La consola de administración centralizada debe estar disponible en un entorno web, permitiendo acceso y gestión a través de un navegador web.
4		La consola debe incluir un dashboard gráfico (Tablero de Informes) que permita visualizar y analizar informes clave de manera clara y eficiente.
5	Gestión Centralizada	La consola debe permitir la gestión centralizada de estaciones de trabajo y servidores, ofreciendo un control unificado y eficiente desde una única interfaz.
6		La Consola debe permitir la configuración de actualizaciones automáticas.
7		La Consola debe permitir la configuración del escaneo en tiempo real.
8		La Consola debe permitir la configuración del escaneo manual.
9		La Consola debe permitir la configuración de la detección de malware y spyware.
10		La Consola debe permitir la gestión de la cuarentena central de manera eficiente.
11		La Consola debe permitir la configuración de los niveles de seguridad del firewall personal.
12		La Consola debe permitir la configuración de las reglas del firewall.
13		La Consola debe permitir la configuración de los servicios del firewall.
14		La Consola debe permitir la configuración del control de dispositivos.
15	Gestión de Licencias	La Consola debe permitir la configuración de la protección de navegación.
16		La Consola debe permitir la configuración del envío de alertas por correo electrónico y/o syslog.
17	Gestión de Licencias	El software debe ofrecer una gestión flexible de licencias, permitiendo su reasignación y reutilización en caso de que un equipo sea dado de baja o reemplazado debido a obsolescencia tecnológica.
18		La consola de administración centralizada debe contar una cuarentena centralizada para el malware, facilitando la gestión y el aislamiento de amenazas detectadas en toda la red desde una única ubicación.
19	Informes y Análisis	La consola debe permitir la generación de reportes que permitan visualizar en tiempo real el estado de la protección de la red.
20		La consola debe permitir la generación de reportes gráficos imprimibles y exportables, de las versiones, actualizaciones e infecciones.
21		La consola centralizada debe proporcionar un reporte en tiempo real del estado de la red, incluyendo:
22		✓ Promedio de protección.
23		✓ Estado de las actualizaciones.
24		✓ Estado de la protección de malware
25		✓ Estado de la instalación del antivirus.
26		✓ Propiedad de los equipos como (Hostname, IP, Dominio/Grupo)
27		La consola debe permitir la creación y envío de reportes en cualquiera de los siguientes formatos: PDF y/o CSV o HTML(opcional) vía correo electrónico. <sup>4</sup>
28		La consola debe permitir la creación de reportes personalizados.
29		La consola debe permitir generar reportes detallados por usuario para evaluar el cumplimiento de políticas

<sup>4</sup> Texto actualizado a razón de la consulta N°3 de GIDTEC SAC



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

Nº	Características Técnicas Mínimas	Descripción
30	Parches y Actualizaciones	La consola debe reportar las actualizaciones faltantes del sistema operativo de las estaciones de trabajo y servidores o
31		La consola debe comparar periódicamente el software antivirus instalado en las estaciones de trabajo y servidores, para identificar las actualizaciones faltantes y las vulnerabilidades del mismo antivirus. <sup>5</sup>
32		La consola debe descargar los paquetes antivirus necesarios para corregir vulnerabilidades y aplicar los parches correspondientes al mismo software antivirus. <sup>6</sup>
33		La consola debe permitir la programación de instalaciones automáticas basadas en un día y hora específico.
34		La consola debe permitir descargar la actualizaciones del producto desde la misma consola o desde el repositorio más cercano para minimizar el consumo del ancho de banda institucional.
35		La consola debe permitir la gestión centralizada de las actualizaciones del producto y las firmas de malware, así como la creación de repositorios para gestionar estas actualizaciones.
36	Integración	La consola debe soportar la integración con el Directorio Activo.
37	Políticas de Seguridad	La consola debe permitir la configuración de políticas que impidan la desinstalación del software antivirus en estaciones de trabajo y servidores, incluso cuando el usuario tenga privilegios de administrador.
38		La consola debe permitir la configuración de políticas que bloqueen y/o desactiven el acceso a las opciones de configuración del antivirus.
39	Notificaciones y Alertas	La consola debe permitir la configuración de alertas y reportes
40		La consola debe permitir notificar eventos de virus a través de diversos medios, como correo electrónico y alertas de registro
41	Control de Acceso y Gestión de Roles	El acceso a la consola de administración centralizada debe requerir autenticación de doble factor (2FA) para garantizar un nivel adicional de seguridad. Los usuarios deberán proporcionar una segunda forma de verificación, como un código enviado a un dispositivo móvil o una aplicación de autenticación, correo, además de sus credenciales de inicio de sesión.
42	Inducción	Se deberá proporcionar un entrenamiento básico sobre la administración, generación de reportes, despliegue masivo para instalación, actualización y aplicación parches en estaciones de trabajo, servidores y agentes antivirus, reasignación de licencias, configuración de políticas, resolución de problemas y otros. Este entrenamiento estará dirigido a 6 profesionales de la Entidad y tendrá una duración mínima de 08 horas. El cual se realizará de manera presencial en las instalaciones de la Entidad o de forma virtual (en línea con el expositor). El expositor deberá ser personal certificado por el fabricante de la solución propuesta. Se entregarán certificados de participación a los profesionales designados por la Entidad y se proporcionarán enlaces oficiales de la marca para autoaprendizaje.

### 5.3. LA INSTALACIÓN Y CONFIGURACIÓN

La solución ofertada, incluirá la instalación y configuración de las consolas de administración centralizada y de los agentes antivirus en las estaciones de trabajo y servidores de manera remota y/o presencial. Aquellas estaciones de trabajo y/o servidores inaccesibles por motivos diversos como falta acceso al equipo, falta de permisos de administración, errores en el sistema operativo entre otros no serán tomados en cuenta para la conformidad, los cuales posteriormente a ser corregidos, la instalación será realizada por los especialistas técnicos de la Entidad.

Todas las tareas necesarias para la puesta en producción de la solución ofertada, incluyendo instalación de licencias, personalización de la solución y otros para su correcto funcionamiento serán de total y exclusiva responsabilidad del proveedor.

<sup>5</sup> Texto actualizado a razón de la consulta N° 05 de GIDTEC SAC.

<sup>6</sup> Texto actualizado a razón de la consulta N° 06 de GIDTEC SAC.





PERÚ

Ministerio del Interior

*"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"*  
*"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"*

#### SEDE MININTER

- Instalación, configuración y actualización de la consola centralizada en su última versión estable totalmente licenciada y funcionando correctamente.
- Instalación, configuración y actualización del agente antivirus en su última versión estable en por lo menos 10 estaciones de trabajo con su respectiva licencia activada.
- Instalación y configuración del agente antivirus en su última versión estable en por lo menos 10 servidores.
- Se firmará un acta de instalación y configuración de la consola centralizada e instalación de los agentes antivirus en las estaciones de trabajo y servidores de la sede MININTER.

#### DIGIMIN-MININTER

- Instalación, configuración y actualización de la consola centralizada en su última versión estable totalmente licenciada y funcionando correctamente.
- Instalación, configuración y actualización del agente antivirus en su última versión estable en por lo menos 10 estaciones de trabajo con su respectiva licencia activada.
- Instalación y configuración del agente antivirus en su última versión estable en por lo menos 10 servidores.
- Se firmará una de acta de instalación y configuración de la consola centralizada e instalación de los agentes antivirus en las estaciones de trabajo y servidores de Sede DIGIMIN-MININTER.

A la firma del contrato, el proveedor deberá proporcionar por escrito los datos de las personas designadas para la instalación, configuración y actualización de la solución, consignando nombres y apellidos, función, cargo, e-mail y teléfono.

#### **5.4. SOBRE EL SOPORTE TÉCNICO:**

El proveedor deberá ofrecer soporte técnico remoto 24/7 durante un período de 3 años, disponible a través de teléfono, portal web (opcional), correo electrónico. Además, cuando la situación o el evento lo requiera, se deberá proporcionar soporte técnico presencial, según lo solicite el personal técnico de la entidad.<sup>7</sup>

Al momento de la firma del contrato, el proveedor deberá proporcionar por escrito los datos de las personas designadas para la atención de problemas, consignando nombres y apellidos, su función, cargo, correo electrónico y número de teléfono. Además, el proveedor deberá mantener esta información actualizada en caso de que se produzcan cambios en su estructura organizacional.

#### **VI. REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS (De corresponder)**

La prestación deberá estar alineado a las normas vigentes que se encuentren basados en:

- Ley N° 27658 - Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 29733 – Ley de Protección de Datos Personales.
- LEY N° 27806 - Ley de Transparencia y Acceso a la Información Pública.
- La Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición.
- RM 0531-2021-IN Política General de Seguridad de la Información del MININTER.

<sup>7</sup> Texto actualizado a razón de la consulta N° 13 de SOLUZIONI GROUP S.A.C.





PERÚ

Ministerio del Interior

*"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"*

*"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"*

**VII. ACONDICIONAMIENTO, MONTAJE, INSTALACIÓN O PUESTA EN MARCHA (De corresponder)**

No corresponde

**VIII. REQUISITOS MÍNIMOS DEL PROVEEDOR (Obligatorio)**

- ✓ Tener RNP Vigente.
- ✓ Tener RUC habilitado.
- ✓ EL PROVEEDOR debe ser representante acreditado en el país o canal autorizado para la distribución o venta de productos del fabricante de antivirus ofertado. Se acreditará con carta del fabricante o su representante en el Perú, para la firma del contrato.

**IX. PLAZO DE ENTREGA (Obligatorio)**

**PLAZO DE INSTALACIÓN Y CONFIGURACIÓN**

El plazo máximo de instalación y configuración de los bienes es de quince (15) días calendarios contabilizado a partir del día siguiente de suscrito el Contrato y cuyo cumplimiento será formalizado, mediante entrega de guía de remisión y documentación requerida que será ingresada en el Almacén Central del MININTER.

El proveedor deberá presentar:

- ✓ La guía de remisión. Indicando en dicho documento, el número de contrato, el detalle de los productos adquiridos y el link del portal de Internet del fabricante, donde se debe poder validar que la solución de antivirus adquirida se encuentra registrada y activada a nombre del Ministerio del Interior.
- ✓ Acta de instalación y configuración de la consola centralizada e instalación de los agentes antivirus en las estaciones de trabajo y servidores de la Sede MININTER.
- ✓ Acta de instalación y configuración de la consola centralizada e instalación de los agentes antivirus en las estaciones de trabajo y servidores de la Sede DIGIMIN-MININTER.
- ✓ Certificados y Actas de Inducción del Personal de la Entidad.

**ACTIVACIÓN DE LAS LICENCIAS**

Como máximo siete (07) días calendarios, contados a partir del día siguiente de suscrito el contrato.

**X. DOCUMENTOS PARA LA FIRMA DEL CONTRATO:**

- El proveedor para la firma del contrato, debe acreditar mediante carta del fabricante o su representante en el Perú, ser representante acreditado en el país o canal autorizado para la distribución o venta de productos del fabricante del software de la solución ofertada.
- El proveedor para la firma del contrato, debe brindar los datos de las personas designadas para la instalación, configuración y actualización del producto adquirido, consignando nombres y apellidos, función, cargo, e-mail y teléfono.
- El proveedor para la firma del contrato, debe brindar los datos de las personas designadas para la atención de problemas, consignando nombres y apellidos, función, cargo, e-mail y teléfono.

**XI. ENTREGABLES:**



PERÚ

Ministerio del Interior

*"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"*

*"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"*

ENTREGABLES	PLAZO
<ul style="list-style-type: none"><li>- Guía de remisión, indicando en dicho documento, el número de contrato, el detalle de los productos adquiridos y el link del portal de Internet del fabricante, donde se debe poder validar que la solución de antivirus adquirida, se encuentra registrada y activada a nombre del Ministerio del Interior.</li><li>- Acta de instalación y configuración de la consola centralizada e instalación de los agentes antivirus en las estaciones de trabajo y servidores de Sede MININTER.</li><li>- Acta de instalación y configuración de la consola centralizada e instalación de los agentes antivirus en las estaciones de trabajo y servidores de Sede DIGIMIN-MININTER.</li><li>- Certificados y Actas de Inducción del Personal de la Entidad.</li></ul>	Como máximo, quince (15) días calendarios, contabilizados a partir del día siguiente de suscrito el Contrato.

## XII. GARANTÍA COMERCIAL (Obligatorio)

**EL PROVEEDOR** garantizará que el bien suministrado sea la última versión estable anunciada por el fabricante.

**Alcance.** Contra defectos de diseño y/o fabricación, averías, entre otros, por un mal funcionamiento, o pérdida total de los bienes contratados, derivados de desperfectos o fallas ajenas al uso normal o habitual de los bienes, no detectables al momento que se otorgó la conformidad.

**Periodo de garantía:**

- ✓ 3 años, para licencias con vigencia de 3 años<sup>8</sup>.
- ✓ 1 año, para licencias con vigencia de 1 año<sup>9</sup>.

**Cómputo del periodo de garantía:** Contados a partir del mismo día de activada la suscripción de la solución antivirus.

## XIII. FORMA DE PAGO (Obligatorio)

Se realizará en una sola armada, previa conformidad emitida por la Oficina de Servicios de Tecnología y Comunicaciones (OSTC), de la Oficina General de Tecnologías de la Información y Comunicaciones (OGTIC), siempre que se verifique el cumplimiento de las condiciones establecidas en la presente contratación.

## XIV. LUGAR DE ENTREGA (Obligatorio)

La entrega de los bienes debe efectuarse en el Almacén Central del MININTER, ubicado en Plaza 30 de agosto s/n Urb. Corpac - San Isidro – Lima

El proveedor deberá presentar:

- ✓ La guía de remisión. Indicando en dicho documento, el número de contrato, el detalle de los productos adquiridos y el link del portal de Internet del fabricante, donde se debe poder validar que la solución de antivirus adquirida se encuentra registrada y activada a nombre del Ministerio del Interior.
- ✓ Acta de instalación y configuración de la consola centralizada e instalación de los agentes antivirus en las estaciones de trabajo y servidores de la Sede MININTER.
- ✓ Acta de instalación y configuración de la consola centralizada e instalación de los agentes antivirus en las estaciones de trabajo y servidores de la Sede DIGIMIN-MININTER.
- ✓ Certificados y Actas de Inducción del Personal de la Entidad.

<sup>8</sup> Texto actualizado a razón de la consulta N° 17 de SOLUZIONI GROUP S.A.C.

<sup>9</sup> Texto agregado a razón de la consulta N° 17 de SOLUZIONI GROUP S.A.C.



PERÚ

Ministerio del Interior

*"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"  
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"*

#### **XV. CONFORMIDAD (Obligatorio)**

La conformidad será emitida por la Oficina de Servicios de Tecnología y Comunicaciones (OSTC) de la Oficina General de Tecnologías de la Información y Comunicaciones (OGTIC), previa verificación del cumplimiento de lo establecido en la presente contratación.

#### **XVI. PENALIDADES (Obligatorio)**

Penalidad por mora en la ejecución de la prestación del bien:

En caso de retraso injustificado en la ejecución de las prestaciones objeto de la orden de compra, la Entidad aplicará al proveedor una penalidad por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto total 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 fórmula:

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

Donde F tendrá los siguientes valores:

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

Tanto el monto como el plazo se refieren, según corresponda a la orden de servicio o ítem que debió ejecutarse o, en caso que estos involucren obligaciones de ejecución periódica a la presentación parcial que fuera materia de retraso.

La justificación de un retraso podrá ser considerado previa evaluación de la acreditación objetiva y fehacientemente por parte del proveedor, sustentando que el mayor tiempo transcurrido no le resulta imputable.

#### **XVII. OTRAS PENALIDADES (De corresponder)**

No corresponde

#### **XVIII. DISPOSICIONES DE CONFIDENCIALIDAD (Obligatorio)**

El proveedor se obliga a mantener y guardar estricta reserva y absoluta confidencialidad de todos los documentos e informaciones del Ministerio del Interior a los que tenga acceso en la ejecución de la contratación. 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 de la presente adquisición o vinculado con la ejecución del mismo, puedan ser conocidos a través del proveedor.

#### **XIX. CLÁUSULA DE ANTICORRUPCIÓN (Obligatorio)**

El proveedor declara y garantiza no haber, directa o indirectamente o tratándose de una persona jurídica a través de sus socios, integrante de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 138.4 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general cualquier beneficio o incentivo ilegal en relación a la presente adquisición.

Asimismo el proveedor se obliga a conducirse en todo momento, durante la ejecución de la orden de servicio, 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,



PERÚ

Ministerio del Interior

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

asesores y personas vinculadas a las que se refiere el artículo 138.4 Reglamento de la Ley de Contrataciones del Estado.

Además, 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 tuviera conocimiento; y adoptar medidas técnicas, organizativas y/o personales apropiadas para evitar los referidos actos o prácticas.

**XX. RESPONSABILIDAD POR VICIOS OCULTOS:**

El contratista es responsable por la calidad ofrecida y por los vicios ocultos por un plazo no menor de tres (03) años contados a partir de la conformidad otorgada por la Entidad. La recepción conforme de la entidad no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos.

**XXI. OTROS (De corresponder)**

No corresponde

**B. REQUISITOS DE CALIFICACIÓN**

A	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u> El postor debe acreditar un monto facturado acumulado equivalente a Cuatro cientos mil con 00/100 Soles (S/. 400,000.00) por la venta de bienes iguales o similares al objeto de la convocatoria, durante un periodo de ocho (8) años 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.</p> <p>Se consideran bienes similares a los siguientes:</p> <ul style="list-style-type: none"><li>a) Software o Appliance de Seguridad Antispam</li><li>b) Sistema de detección de intrusos (IDS) y/o Sistema de prevención de intrusos (IPS)</li><li>c) Firewall y/o Next Generation Firewall (NGFW)</li><li>d) Soluciones Antimalware para endpoint</li><li>e) Adquisición y/o Renovación de Licencias EDR Antivirus</li></ul> <p>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de Sesenta mil con 00/100 Soles (S/ 60,000.00), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) 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. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.</p> <p><u>Acreditación:</u> La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago<sup>10</sup>, correspondientes a un máximo de veinte (20) contrataciones.</p>

<sup>10</sup> Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"

(...)

"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".



En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.

En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.

Cuando en los contratos, órdenes de compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.

**Importante**

*En el caso de consorcios, sólo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*



PERÚ

Ministerio del Interior

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

**Importante**

- Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.
- El cumplimiento de las Especificaciones Técnicas se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento de algún componente de las características y/o requisitos funcionales. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.
- Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.

**Firma del Responsable del Área Usuaria**