ESPECIFICACIONES TECNICAS

ADQUISICIÓN DE SOFTWARE ANTIVIRUS - ANTIMALWARE CORPORATIVO

I. DEPENDENCIA QUE REQUIERE EL BIEN

Oficina de Tecnologías de la Información y Comunicaciones de la Oficina General de Estadística y Tecnologías de la información y Comunicaciones.

II. OBJETIVO QUE JUSTIFICA LA ADQUISICIÓN

Adquisición de una solución de antivirus corporativo para proteger de infecciones por virus informático y malware a los equipos informáticos de la entidad, fortalecer y asegurar la disponibilidad de la red de datos, así como también el acceso a las aplicaciones que brinda el Ministerio de Trabajo y Promoción del Empleo – MTPE.

III. FINALIDAD PÚBLICA

El Ministerio de Trabajo y Promoción del Empleo, tiene como visión promover empleo decente y productivo, por lo cual diseña, articula y ejecuta políticas que generen oportunidades dignas dentro del desarrollo personal, laboral contribuyendo el fortalecimiento del sistema democrático en las relaciones laborales. En ese sentido, la contratación del bien y su posterior implementación permitirá garantizar que las estaciones de trabajo posean una solución que detecte, bloquee y elimine códigos maliciosos para el correcto intercambio de información y compatibilidad con el parque informático de la sede central, por lo que la solución deberá contar con el licenciamiento de antivirus y antimalware garantice la disponibilidad de los servicios informático brindados por el Ministerio de Trabajo Promoción y Empleo, buscando la atención eficiente y ágil al ciudadano.

IV. CARACTERÍSTICAS GENERALES DE LA SOLUCIÓN DE PROTECCIÓN PARA ESTACIONES DE TRABAJO (PC'S Y SERVIDORES):

4.1 Generalidades

a) El Ministerio de Trabajo y Promoción del Empleo requiere contar con una solución antivirus y antimalware, para la protección de virus informáticos y software malicioso, el cual deberá ser de la misma marca, con el fin de garantizar la compatibilidad y la operatividad de ambas soluciones con todas sus funcionalidades, sin que afecte la performance de los equipos EndPoints.

b) El proveedor debe considerar en su propuesta, todos los aspectos técnicos necesarios para instalar de manera satisfactoria la solución en la totalidad de los equipos Informático de la institución.

c) Cualquier componente o requisito previo que no se contemple en su propuesta, deberá ser asumido por el contratista.

d) Se deberá implementar la última versión estable del producto ofertado, con soporte del fabricante.

e) El postor deberá presentar una carta emitida por el fabricante para la distribución del producto ofertado, donde el fabricante esté acreditando su respaldo técnico para la distribución y comercialización de las licencias materia de este proceso. Dicha carta deberá ser presentada en la Propuesta Técnica.

f) La solución SOFTWARE ANTIVIRUS - ANTIMALWARE CORPORATIVO, debe proteger de infecciones por virus informático y/o software malicioso a las computadoras personales (CPU), computadoras portátiles y servidores a través de una consola. El cual debe incluir una licencia para los equipos informáticos detallados en el siguiente cuadro:

Ítem	Descripción de equipos	SO	Cantidad
1.	Computadoras de escritorio	Windows	1476
2.	Computadoras portátiles	Windows	201
3.	Servidores Virtual	Windows	20
4.	Servidores Virtual	Linux	74
		Total	1771

4.2 Características Técnicas

- Se debe entender como una solución de seguridad de Endpoint a la protección de los equipos de la red sean estas estaciones, servidores y portátiles sin distinción alguna con una solución software que proteja a la red, los aplicativos, los servicios de correo electrónico e Internet de amenazas tales como los virus, troyanos, macrovirus, adware, spyware, gusanos, rootkits y todo tipo de programa malicioso (malware) incluyendo la protección contra ransomware. Así mismo la solución de Endpoint deberá permitir el control de dispositivos, el control de aplicaciones y el control de acceso a la red en todos los equipos de la red.
- Todas las características técnicas de la solución requerida deberán ser sustentadas por el postor con documentación del fabricante, manuales, brochures y/o capturas de pantalla de la solución con la finalidad de verificar el cumplimiento de cada una de ellas, que deben ser presentados en la etapa de presentación de ofertas.
- Cuando nos referimos a "una solución de seguridad antimalware", se quiere decir que la herramienta de informática o de tecnología de la información, puede estar compuesta de uno o más módulos del mismo fabricante de software y cumplan con las siguientes características técnicas mínimas:

4.2 Características de la solución de Endpoint para estaciones de trabajo

- Deberá soportar los sistemas operativos de estaciones de trabajo en versiones de 32 y 64 bits de Microsoft Windows 7, 8 y 10.
- La solución deberá proteger contra virus, troyanos, macrovirus, adware, spyware, gusanos, rootkits y todo tipo de programa malicioso (malware) incluyendo la protección contra ransomware.
- La solución contra ransomware deberá ser un módulo específico que realice el bloqueo de amenazas de día cero y ataques de ransomware como Locky, WannCry, Petya, etc. sin requerir la actualización de firmas.
- La solución contra ransomware deberá monitorear y bloquear cambios no autorizados en el Endpoint como cifrados masivos, cambios en el sistema, modificación de llaves en el registro o creación de archivos y carpetas en áreas no autorizadas del sistema operativo.

- La solución debe integrar dos motores antimalware para una mejor protección y como doble capa de protección antimalware. El motor principal deberá ser del fabricante de la solución propuesta y el secundario de un tercero. Ambos motores deberán funcionar al mismo tiempo para una óptima protección.
- La solución deberá estar incorporado como Líder o Visionario en el Cuadrante de Gartner del año 2018 así como tener una efectividad de seguridad de más del 98% en el informe de NSS Labs EAP 2019.
- La solución deberá incorporar un módulo de protección basado en la nube el cual deberá tener acceso rápido a las amenazas nuevas directamente desde el laboratorio del fabricante.
- El Endpoint deberá tener funcionalidades para convertirse en un servidor de actualizaciones de la LAN usando para ello la tecnología neigbordcast pudiendo convertirse en servidor o cliente de actualizaciones al mismo tiempo. Esta característica deberá poder ser activada o desactivada desde la consola central y no requerirá la instalación de agentes adicionales.
- El Endpoint deberá tener funcionalidades para buscar actualizaciones en cualquier otro Endpoint de la LAN para lo cual deberá usar el protocolo UDP (neigbordcast) para realizar consultas en la LAN.
- La solución deberá analizar el tráfico web y eliminar el malware detectado, así mismo, en caso el análisis tome más de 1 minuto deberá poder mostrar un indicador de progreso de análisis.
- La solución deberá detectar la presencia de Botnets en la LAN analizando el tráfico generado por consultas DNS en el host, así como ransomware y ATP.
- La solución deberá analizar las unidades de red.
- La solución deberá analizar archivos comprimidos (zip, arj, lzh, tar, gz, etc.)
- La solución deberá permitir realizar exclusiones de archivos, extensiones, carpetas y unidades tanto para el modo de escaneado en tiempo real como manual.
- La solución deberá permitir realizar exclusiones de procesos tanto para el modo de escaneado en tiempo real como manual.
- La solución deberá permitir el bloqueo de cookies de seguimiento de la navegación de los usuarios creado por los navegadores.
- La solución deberá incluir un módulo que revise la reputación de los archivos en tiempo real con la finalidad de detectar en tiempo real malware sospechoso o desconocido.
- La solución deberá evaluar amenazas usando técnicas de monitoreo de los procesos sospechosos inyectando ya sea una DLL de monitoreo o integrando una mini-máquina virtual que rastree y monitoree el comportamiento de los procesos.
- La solución deberá contar con opciones para incluir o excluir programas que puedan ser detectados como comportamiento sospechoso como los instaladores de aplicaciones internas, actualizadores de programas u otras aplicaciones. La exclusión deberá poder realizarse usando el hash SHA-1 de la aplicación el cual podrá ser marcado como confiable o No confiable.

- La solución deberá permitir realizar el análisis manual de los archivos pudiendo configurarse ya sea para todos los archivos o para determinadas extensiones de archivos.
- La solución deberá permitir realizar acciones sobre el malware detectado ya se para informar, desinfectar, eliminar, renombrar, preguntar por la acción al usuario o enviar a la cuarentena tanto para el escaneado en tiempo real como para el escaneado manual.
- La solución deberá poder realizar el análisis manual ya sea en prioridad normal o en segundo plano con la finalidad de no interrumpir las labores de los usuarios.
- La solución deberá incluir un módulo para el control de aplicaciones que permita controlar la ejecución de ciertas aplicaciones en el equipo del usuario.
    - Deberá permitir crear reglas en base al origen y destino del archivo en base a su ubicación, sha1, prevalencia, reputación, nombre del archivo, versión del archivo, descripción del archivo, nombre del producto, fabricante, por derechos de autor, nombre del signatario, si contiene una firma verdadera, por tipos de nombre y extensión y por la línea de comandos que ejecuta la aplicación.
    - Deberá permitir crear notas de las reglas de detección creadas con el fin de contar con una bitácora de consultas.
    - Deberá contar con una opción para habilitar o desactivar una regla de control de aplicaciones.
- La solución deberá incluir un módulo de protección en la navegación web el cual deberá permitir asegurar la navegación realizando las siguientes acciones:
    - Navegación basada en la reputación de los sitios web permitiendo bloquear el acceso a un sitio web clasificado como inseguro. La reputación de sitios deberá realizarse mediante consultas a la nube de seguridad del fabricante.
    - Deberá mostrar las reputaciones de los sitios web en los resultados de búsqueda en sitios como Google, Yahoo, Bing, etc.
    - Permitir al usuario continuar la navegación en páginas bloqueadas la misma que debe poder ser desactivada centralmente.
    - Deberá permitir crear sitios de confianza a los cuales podrán navegar los usuarios sin necesidad de consultar la reputación de los mismos. La creación deberá admitir dominios completos (p.e. ejemplo.com) y sub-dominios (p.e. www.ejemplo.com).
    - Deberá permitir crear sitios no permitidos a los cuales los usuarios no podrán navegar sin necesidad de consultar la reputación de los mismos. La creación deberá admitir dominios completos (p.e. ejemplo.com) y sub-dominios (p.e. www.ejemplo.com).
- La solución deberá incluir un módulo para el control de contenido web pudiendo realizar las siguientes acciones:
    - Bloqueo de la navegación en sitios de categorías específicas.
    - Incluir al menos 32 categorías de sitios web predefinidas como aborto, publicidad, adulto, alcohol, anonimizadores, subastas, banca, blogs, chat,

citas, drogas, entretenimiento, apuesta juegos, piratería, odio, búsqueda de trabajo, servicios de pago, estafa, compras en línea, redes sociales, descargas de software, spam, medios de trasmisión, violencia, warez, armas, correo web, P2P, etc.
    - Filtrar el tipo de contenido que los usuarios pueden descargar desde el internet pudiendo realizar reglas de bloqueo por tipo de archivo (p.e. application/x-executable) y por extensión (p.e *.exe).
- La solución deberá incluir un módulo para el control de conexiones el cual deberá permitir proteger la navegación de los usuarios a sitios de banco, sitios de comercio electrónico y sitios confiables que se definan mediante el protocolo HTTPS con la finalidad de evitar el phishing o robo de datos a los usuarios.
- La solución deberá incluir un cortafuego personal (firewall) avanzado que permita bloquear el tráfico malicioso en la LAN. Este módulo deberá:
    - Incluir un IPS a nivel de host o HIPS.
    - Bloquear fragmentos de IP basados en el tamaño definido en la consola de gestión.
    - Permitir el filtrado de tráfico IPV6.
    - Permitir configurar tarjetas de red confiables.
    - Desactivar el firewall de Windows automáticamente.
    - Incluir al menos 8 tipos de perfiles predefinidos por el fabricante como las mejores prácticas de seguridad informática como Móvil, Oficina, Oficina con uso compartido de archivos e impresoras, Estricto, Normal, Personal, Permitir todo y Cuarentena de red.
    - Incluir reglas de cortafuegos predefinidas para bloquear el tráfico de malware usado para ataques laterales en una red LAN. Estás reglas deberán ser actualizadas y mantenidas por el fabricante.
    - Permitir añadir reglas personalizas en los diferentes perfiles predefinidos.
    - Permitir activar o desactivar una regla definida.
    - Deberá permitir crear reglas para la Cuarentena de equipos basado en políticas de seguridad o falta de actualizaciones según el tiempo establecido por el administrador de la solución.
- La solución deberá incluir un módulo para la protección contra vulnerabilidades y actualizaciones de software centralizada.
- La solución deberá incluir un módulo para la protección de dispositivos de almacenamiento extraíble el cual deberá:
    - Crear políticas para permitir, bloquear la escritura y bloquear el acceso a los dispositivos.
    - Permitir o bloquear la ejecución de binarios almacenados en el dispositivo (.exe, .bat, .com, etc) con la finalidad de evitar la entrada de malware desde dispositivos desconocidos a la red.
    - Detectar dispositivos de tipo:
        - USB Mass Storage
        - Wireless
        - DVD/CD-ROM
        - Windows CE ActiveSync

- Floppy Drives
- Modems
- COM & LTP
- Impresoras
- Lectores de Smart Cards
- Cámaras y Scanners
- IrDA
- Bluetooth
- Controladores de Bus IEEE 1394

4.3 Características de la solución de Endpoint para servidores físicos y virtuales

- Deberá soportar los sistemas operativos de servidor Microsoft Windows 2008, 2012, 2016.
- La solución deberá proteger contra virus, troyanos, macrovirus, adware, spyware, gusanos, rootkits y todo tipo de programa malicioso (malware) incluyendo la protección contra ransomware.
- La solución contra ransomware deberá ser un módulo específico que realice el bloqueo de amenazas de día cero y ataques de ransomware como Locky, WannCry, Petya, etc. sin requerir la actualización de firmas.
- La solución contra ransomware deberá monitorear y bloquear cambios no autorizados en el Endpoint como cifrados masivos, cambios en el sistema, modificación de llaves en el registro o creación de archivos y carpetas en áreas no autorizadas del sistema operativo.
- La solución debe integrar dos motores antimalware para una mejor protección y como doble capa de protección antimalware. El motor principal deberá ser del fabricante de la solución propuesta y el secundario de un tercero. Ambos motores deberán funcionar al mismo tiempo para una óptima protección.
- La solución deberá incorporar un módulo de protección basado en la nube el cual deberá tener acceso rápido a las amenazas nuevas directamente desde el laboratorio del fabricante.
- El Endpoint deberá tener funcionalidades para convertirse en un servidor de actualizaciones e la LAN independiente del sistema operativo en el que funcione. Esta característica deberá poder ser activada o desactivada desde la consola central y no requerirá la instalación de agentes adicionales.
- El Endpoint deberá tener funcionalidades para buscar actualizaciones en cualquier otro Endpoint de la LAN para lo cual deberá usar el protocolo UDP para realizar consultas en la LAN.
- La solución deberá analizar el tráfico web y eliminar el malware detectado, así mismo, en caso el análisis tome más de 1 minuto deberá poder mostrar un indicador de progreso de análisis.
- La solución deberá detectar la presencia de Botnets en la LAN analizando el tráfico generado por consultas DNS en el host, así como ransomware y ATP.
- La solución deberá analizar las unidades de red.
- La solución deberá analizar archivos comprimidos (zip, arj, lzh, tar, gz, etc.)

- La solución deberá permitir realizar exclusiones de archivos, extensiones, carpetas y unidades tanto para el modo de escaneado en tiempo real como manual.
- La solución deberá permitir realizar exclusiones de procesos tanto para el modo de escaneado en tiempo real como manual.
- La solución deberá permitir el bloqueo de cookies de seguimiento de la navegación de los usuarios creado por los navegadores.
- La solución deberá incluir un módulo que revise la reputación de los archivos en tiempo real con la finalidad de detectar en tiempo real malware sospechoso o desconocido.
- La solución deberá evaluar amenazas usando técnicas de monitoreo de los procesos sospechosos inyectando ya sea una DLL de monitoreo o integrando una mini-máquina virtual que rastree y monitoree el comportamiento de los procesos.
- La solución deberá contar con opciones para incluir o excluir programas que puedan ser detectados como comportamiento sospechoso como los instaladores de aplicaciones internas, actualizadores de programas u otras aplicaciones. La exclusión deberá poder realizarse usando el hash SHA-1 de la aplicación el cual podrá ser marcado como confiable o No confiable.
- La solución deberá permitir realizar el análisis manual de los archivos pudiendo configurarse ya sea para todos los archivos o para determinadas extensiones de archivos.
- La solución deberá permitir realizar acciones sobre el malware detectado ya se para informar, desinfectar, eliminar, renombrar, preguntar por la acción al usuario o enviar a la cuarentena tanto para el escaneado en tiempo real como para el escaneado manual.
- La solución deberá poder realizar el análisis manual ya sea en prioridad normal o en segundo plano con la finalidad de no interrumpir las labores de los usuarios.
- La solución deberá permitir la integración con Microsoft AMSI para el escaneado de malware desde aplicaciones de terceros en forma integrada.
- La solución deberá permitir configurar el escaneado en baja prioridad con la finalidad de minimizar el uso de recursos en los equipos.
- La solución deberá incluir un módulo para el control de aplicaciones que permita controlar la ejecución de ciertas aplicaciones en el equipo del usuario:
    - Deberá permitir crear reglas en base al origen y destino del archivo en base a su ubicación, sha1, prevalencia, reputación, nombre del archivo, versión del archivo, descripción del archivo, nombre del producto, fabricante, por derechos de autor, nombre del signatario, si contiene una firma verdadera, por tipos de nombre y extensión y por la línea de comandos que ejecuta la aplicación.
    - Deberá permitir crear notas de las reglas de detección creadas con el fin de contar con una bitácora de consultas.
    - Deberá contar con una opción para habilitar o desactivar una regla de control de aplicaciones.

- La solución deberá incluir un módulo de protección en la navegación web el cual deberá permitir asegurar la navegación realizando las siguientes acciones:
  - Navegación basada en la reputación de los sitios web permitiendo bloquear el acceso a un sitio web clasificado como inseguro. La reputación de sitios deberá realizarse mediante consultas a la nube de seguridad del fabricante.
  - Deberá mostrar las reputaciones de los sitios web en los resultados de búsqueda en sitios como Google, Yahoo, Bing, etc.
  - Permitir al usuario continuar la navegación en páginas bloqueadas.
  - Deberá permitir crear sitios de confianza a los cuales podrán navegar los usuarios sin necesidad de consultar la reputación de los mismos. La creación deberá admitir dominios completos (p.e. ejemplo.com) y sub-dominios (p.e. www.ejemplo.com).
  - Deberá permitir crear sitios no permitidos a los cuales los usuarios no podrán navegar sin necesidad de consultar la reputación de los mismos. La creación deberá admitir dominios completos (p.e. ejemplo.com) y sub-dominios (p.e. www.ejemplo.com).
- La solución deberá incluir un módulo para el control de contenido web pudiendo realizar las siguientes acciones:
  - Bloqueo de la navegación en sitios de categorías específicas.
  - Incluir al menos 32 categorías de sitios web predefinidas como aborto, publicidad, adulto, alcohol, anonimizadores, subastas, banca, blogs, chat, citas, drogas, entretenimiento, apuesta juegos, piratería, odio, búsqueda de trabajo, servicios de pago, estafa, compras en línea, redes sociales, descargas de software, spam, medios de trasmisión, violencia, warez, armas, correo web, P2P, etc.
  - Filtrar el tipo de contenido que los usuarios pueden descargar desde el internet pudiendo realizar reglas de bloqueo por tipo de archivo (p.e. application/x-executable) y por extensión (p.e *.exe).
- La solución deberá incluir un módulo para el control de conexiones el cual deberá permitir proteger la navegación de los usuarios a sitios de banco y sitios confiables que se definan mediante el protocolo HTTPS con la finalidad de evitar el phishing o robo de datos a los usuarios.
- La solución deberá incluir un módulo para la protección contra vulnerabilidades y actualizaciones de software centralizado.
- La solución deberá incluir un agente liviano independiente y/o agnóstico del Hypervisor para entornos virtuales permitiendo asegurar los servidores en la nube pública o privada. Además, deberá:
  - Reducir el uso de recursos como memoria, CPU, y espacio en disco en máquinas virtuales.
  - Contar con un agente de scaneado liviano
  - Contar con un sistema de protección antimalware basado en la reputación de archivos.

4.4 Características de la consola de administración centralizada

- La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas/reutilizadas en caso que un equipo sea dado de baja o cambiada por obsolescencia tecnológica.
- Deberá soportar la instalación de una Consola Central en Windows.
- El instalador de la Consola Central deberá incluir su propio manejador de base de datos y no deberá sobrepasar de 240Mb de tamaño incluyendo todos los componentes necesarios para su instalación y despliegue (Pre-requisitos, Base de datos, Instalador de la Consola) para la óptima distribución en la red.
- Deberá soportar base de datos de terceros como Microsoft SQL Server o MySQL.
- La comunicación entre la Consola y los Clientes deberá realizar mediante un canal seguro como HTTPS o vía Certificados Digitales.
- La Consola Central deberá poder realizar:
  - La gestión centralizada de estaciones y servidores en la red.
  - La configuración de actualizaciones automáticas.
  - La configuración del escaneado en tiempo real.
  - La configuración del escaneado manual.
  - La configuración de la detección de malware y spyware.
  - La gestión de la cuarentena central.
  - La configuración de los niveles de seguridad del firewall personal.
  - La configuración de las reglas de firewall.
  - La configuración de los servicios de firewall.
  - La configuración del control de aplicaciones.
  - La configuración del control de dispositivos
  - La configuración del escaneado de tráfico web.
  - La configuración de la protección de navegación.
  - La configuración de políticas de filtrado de contenido por categorías.
  - La configuración del envío de alertas por correo o syslog.
- Deberá permitir la gestión centralizada de actualizaciones, siendo la Consola Central el único equipo en poder descargar actualizaciones desde el fabricante y como herramienta de backup se deberá poder configurar políticas para la descarga de actualizaciones en los Endpoint desde el fabricante en caso la Consola Central tenga una falla o se encuentre en mantenimiento.
- Deberá permitir la instalación y desinstalación remota del software en el Endpoint centralizadamente.
- Deberá contar con una Cuarentena de Malware centralizada.
- Deberá permitir la desinstalación de software de terceros al momento de realizarse el despliegue o instalación centralizada de los Endpoints.
- La consola deberá reportar el estado la red en tiempo real como:
  - Promedio de protección.
  - Estado de las actualizaciones.
  - Estado de la protección de malware
  - Estado de la instalación del Endpoint.
  - Propiedad de los equipos como (Hostname, IP, Dominio/Grupo)

- La consola deberá permitir configurar los Endpoint como servidores de actualizaciones usando para ello la tecnología P2P o Neigborcast vía el protocolo UDP.
- La consola deberá gestionar el módulo de protección contra vulnerabilidades y parches de software multi-fabricante para estaciones y servidores que deberá:
  - Reportar las actualizaciones faltantes del sistema operativo y aplicaciones de terceros en los equipos de la red.
  - Comparar periódicamente el software instalado en el Endpoint e identificar las actualizaciones faltantes y las vulnerabilidades encontradas.
  - Descargar a la Consola Central los paquetes y/o programas necesarios para corregir las vulnerabilidades y parches encontrados con el fin de optimizar el uso de ancho de banda en la red.
  - Contar con una opción para visualizar las vulnerabilidades y actualizaciones pendientes encontradas en la red y que Endpoints se encuentran afectadas por cada una de ellas.
  - Contar con una opción para visualizar las vulnerabilidades y actualizaciones pendientes encontradas en la red por Endpoint.
  - Permitir enviar mediante una política la actualización centralizada de programas y vulnerabilidades en programas de Microsoft y Sistemas Operativos, Java, Mozilla, Google, Adobe, Services Pack, Winzip, Apple, Sun y otras aplicaciones usadas en entornos corporativos.
  - Permitir la instalación automática y centralizada de actualizaciones, parches y/o correcciones de vulnerabilidades en el sistema operativo y aplicaciones existentes en el Endpoint de acuerdo a las políticas definidas por el administrador de la consola.
  - Permitir programar la instalación de actualizaciones según su importancia (Crítico, Crítico y Vulnerable y Todas) en forma centralizada.
  - Permitir programar la instalación automática basado en un día y hora.
  - Analizar el Endpoint en búsqueda de aplicaciones vulnerables al inicio del equipo o en según una programación establecida en la consola central.
  - Permitir excluir la instalación de actualizaciones según el tipo de software el cual deberá poder definirse por diversos criterios como:
    - Nombre del producto
    - ID del Bulletin de seguridad del fabricante
    - Service Pack
    - Nombre del parche
    - Severidad o Gravedad de la actualización
  - Descargar las actualizaciones desde la consola central o desde el repositorio más cercano con la finalidad de no consumir el ancho de banda de la institución.
- La consola deberá permitir crear repositorios o consolas distribuidas que gestionen las actualizaciones tanto del producto, firmas de malware y gestionar centralizadamente en cada punto las descargas del módulo del control de vulnerabilidades y parches con la finalidad de minimizar el uso del ancho de banda.

- Los repositorios de actualizaciones deberán soportar como mínimo los mismos sistemas operativos Windows y Linux que la Consola Central.

- La solución deberá integrarse con el Directorio Activo ya sea para el despliegue como para la configuración de políticas.
- Permitir configurar mediante una política para evitar desinstalación de los Endpoints aun cuando el usuario en el Endpoint tenga privilegios de administrador.
- Permitir bloquear y/o desactivar mediante políticas el acceso a las opciones de configuración del Endpoint.
- Deberá contar con una opción para crear instaladores fuera de línea, es decir, instaladores del tipo click-and-run para la instalación del Endpoint en estaciones y servidores con un solo click.

4.5 Consideraciones de Alertas y Reporte

- Deberá incluir un sistema de generación de reportes gráficos empresarial y basado en gráficos. Este sistema deberá poder ser accesible vía Web desde cualquier punto de la red.
- Las alertas deberán poder ser enviados a servidores de análisis de datos como los SYSLOG.
- La solución deberá ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alertas de registros, etc.)
- La solución deberá generar reportes gráficos, imprimibles y exportables de la cobertura de versiones, actualizaciones e infecciones.
- La solución deberá contener un mecanismo de reportes que permite ver el estado de la protección de la red en línea.
- La solución deberá permitir acceder a reportes basados en el usuario que permita conocer rápidamente el cumplimiento de políticas por cada usuario
- La solución deberá incorporar un mecanismo de reportes que permita programar la creación y envío de reportes en formato PDF y HTML vía correo.
- La solución deberá incorporar un mecanismo de conexión con la base de datos para la creación de reportes personalizados.
- La solución deberá reportar la información de vulnerabilidades y actualizaciones de parches faltantes y aplicados en los diferentes equipos de la red.
- El postor deberá brindar el servicio de instalación, configuración de la solución en el 50% de los equipos administrados.
- El postor tendrá 30 días calendarios para realizar la implementación de la solución desde el día siguiente de habilitada las licencias.
- El fabricante deberá contar con un tiempo de respuesta ante nuevos malwares como máximo de cuatro (04) horas de reportado.

4.6 Capacitación

El contratista deberá considerar en su propuesta la capacitación del personal sobre la instalación, configuración y utilización de la solución de antivirus corporativo propuesto, para un mínimo de doce (12) colaboradores del MTPE.

a) Un curso no menor de doce horas (12) horas en las herramientas administrativas del software para cuatro (04) personas, y otro curso ocho (08) horas, en la utilización de la solución para ocho (08) personas de área de soporte, el mismo que debe ser dictado dentro de los treinta días calendarios, contados a partir del día siguiente de suscrito el contrato.
b) EL curso taller, será dictado en forma virtual, previa coordinación con la Oficina de Tecnologías de la Información y Comunicaciones.
c) Al finalizar este curso taller, se suscribirá un "Acta de Capacitación", en señal de conformidad y deberá incluir los certificados correspondientes a nombre de los participantes por el curso recibido.

V. PRESTACIONES ACCESORIAS

a) El soporte técnico para la solución de antivirus y antimalware solicitada, deberá ser brindado por el periodo de 365 días calendario, contabilizado a partir del día siguiente de la conformidad de la implementación de la solución.
b) Deberá brindar soporte técnico telefónico 24x7x365 escalable hacia la casa matriz incluido en la licencia y en español.
c) El servicio de Soporte Técnico comprenderá la solución de cualquier tipo de problema, incidente o avería a una interrupción parcial o total del servicio, así como a la pérdida de la calidad o degradación del mismo. A todo ello se le denominará Falla.
d) El servicio de Soporte Técnico comprenderá Consultas, solicitud de Reportes, solicitud de análisis de auditoría. A todo ello se le denominará Requerimiento.
e) Se encuentra incluido como parte del Soporte Técnico la protección y corrección ante infecciones de virus, malware, ransomware o cualquier tipo de amenaza que ocurra en los equipos de cómputo que cuentan con la solución de antivirus y antimalware brindada.
f) El servicio de Soporte Técnico comprenderá la instalación de parches, actualizaciones, nuevas versiones, vacunas, reglas, filtros, releases, bases de datos de firmas de virus, etc., de la solución ofertada antivirus y antimalware y sus reparaciones (parches, fixes).
g) El servicio de Soporte Técnico incluye el análisis, actualización, corrección y documentación de problemas en la solución implementada.
h) Deberá brindar soporte técnico In Situ a cargo de expertos profesionales en análisis de virus, malware y ransomware, el cual lo asistirá en forma personal. Se precisa, que el soporte técnico in situ se dará en caso de fallas que no puedan ser solucionados de manera remota.
i) El personal técnico que brinde el servicio de soporte técnico debe ser el mismo que ofertó en su propuesta técnica y formó parte de la implementación de la solución ofertada.
j) El contratista deberá asegurar que la solución completa quede operativa y en óptimas condiciones de seguridad y performance y restaurar a éstos su funcionamiento normal cuando una falla se produzca.

k) El contratista deberá proporcionar, sin costo adicional para el MTPE, cualquier complemento que no haya sido descrito en su propuesta técnica y cuya ausencia determine la imposibilidad de cumplir con lo solicitado como parte del soporte técnico.

l) Adicional a las atenciones de Requerimientos correspondientes al soporte técnico que pudieran presentarse, el contratista deberá efectuar como mínimo una revisión mensual con la finalidad de asegurar el correcto funcionamiento de la solución implementada, presentando el informe de revisión mensual, necesaria para la emisión de la conformidad.

m) Al presentarse una Falla o un Requerimiento, la OTIC del MTPE realizará el reporte de la incidencia o requerimiento al Centro de Atención al Cliente del contratista. El reporte podrá realizarse por teléfono o correo electrónico, el mismo que será brindando en la documentación para la suscripción del contrato.

n) Una vez recibida tal notificación, el Centro de Atención al Cliente del contratista registrará el requerimiento de servicio y proporcionará al MTPE un número de ticket de avería.

o) Tiempo de solución que toma el personal técnico designado por el contratista para brindar el soporte, resolver el incidente o requerimiento reportado, contabilizado desde que se emite el ticket de atención. El proveedor deberá enviar el ticket de atención vía e-mail, en un tiempo máximo de 10 minutos de reportado el problema y deberá enviar un e-mail a la culminación del soporte, resolución del incidente o requerimiento reportado, en el cual deberá indicar las acciones que se tomaron y el tiempo de solución.

p) El nivel de atención es de acuerdo al siguiente cuadro:

Tipo de falla o requerimiento	Descripción de la falla o requerimiento	Tiempo máximo de solución
Falla crítica	Si se cumple cualquiera de los siguientes puntos: • Interrupción total del servicio o degradación del servicio brindado por la solución ofertada. • Infección de malware o ransomware afecte a un grupo igual o mayor de 05 estaciones de trabajo. • Exista una infección que comprometa la seguridad de la red de datos de la Institución.	04 horas
Falla leve	Si se cumple cualquiera de los siguientes puntos: • Falla en alguna funcionalidad que no afecta ni pone en riesgo el servicio brindado por la solución ofertada. • Infección de malware o ransomware afecta a un número menor a cinco usuarios. • La infección no compromete la seguridad de la red.	24 horas
Requerimiento	Solicitudes de informes o solicitudes de análisis de auditoría de seguridad o solicitudes de cambio de configuración. Se precisa, que el término "análisis de auditoría" se refiere al detalle técnico de los incidentes de seguridad suscitados.	48 horas

✓ De excederse los plazos indicados en el punto anterior, se deberá realizar el cálculo de penalidades, según la tabla indicada en el numeral XIV.

- ✓ El contratista tomará las acciones correspondientes para mitigar el incidente de seguridad del end point, se deberá realizar el soporte in situ, de un especialista del contratista, dentro del plazo señalado en las Especificaciones Técnicas (04 horas). Sin embargo, si por razones técnicas del producto (Fabricante), el virus, malware y/o ransomware no pueda ser eliminado, el contratista deberá presentar un informe indicando las razones por el cual no puede ser eliminado y en caso corresponda al producto (y no al Contratista), no será penalizado.
- ✓ En caso de un APT o un Ransomware, el contratista tomará las acciones correspondientes para procurar mitigar el incidente de seguridad del end point, se deberá realizar el soporte in situ de un especialista del Contratista, dentro del plazo señalado en las Especificaciones Técnicas (04 horas). Sin embargo, si por razones técnicas del producto (Fabricante) el APT o Ransomware no pueda ser eliminado, el Contratista deberá realizar un informe indicando las razones por el cual no puede ser eliminado y en caso corresponda al producto (Y no al Contratista), no será penalizado.
- ✓ El contratista deberá realizar en forma mensual el análisis y verificación de la seguridad en la red de la entidad.
- ✓ Luego de esta verificación, en lo siguientes diez (10) días de finalizado el mes, deberá presentar por la mesa de partes virtual de la Entidad, un informe de lo encontrado, recomendaciones de seguridad y el reporte del TOP 10 de malware detectado, TOP 10 de equipos infectados, Zonas o Grupos más infectados, Vulnerabilidades encontradas y corregidas.
- ✓ Deberá realizar en forma proactiva políticas de seguridad que permitan un mejor control de la seguridad en la red en cualquier momento ya sea in-situ o en forma remota.
- ✓ Deberá encargarse de realizar el Upgrade de la Consola y versiones de los clientes sean estaciones o servidores para lo cual deberá notificar al administrador de la red de dicha actividad.
- ✓ Deberá ejecutar el escaneado de vulnerabilidades de los servidores de la institución al inicio de la ejecución de la prestación principal y luego a los (06) seis meses con una herramienta de Análisis de vulnerabilidades de Ethical Hacking del mismo fabricante propuesto cuyo resultado será la presentación de un informe la misma que deberá contener lo siguiente:
  - ✓ Detalle técnico referente a la exploración, identificación y enumeración de sistemas operativos, servicios y aplicación Web.
  - ✓ Mapa de la aplicación Web, según los resultados obtenidos en las actividades de reconocimiento.
  - ✓ Vulnerabilidades identificadas, con riesgos estimados según CVSS versión 3.
  - ✓ Procedimientos de remediación para cada vulnerabilidad identificada.
  - ✓ Recomendaciones generales orientadas establecer controles que permitan minimizar riesgos, de acuerdo a los resultados globales de la evaluación.
  - ✓ Evidencias de las vulnerabilidades reportadas.

VI. PRODUCTOS A OBTENER

6.1 De la Prestación Principal

a) **Primer entregable**: Plan de trabajo o de implementación o de instalación o de despliegue del producto.

b) **Segundo entregable:** Se deberá realizar la entrega de las Licencias del Software Antivirus y Antimalware ofertado, las cuales tendrán una vigencia de doce (12) meses.

- ✓ La solución deberá contar con todos los manuales que permitan su instalación y configuración, paso a paso de toda la solución.
- ✓ El proveedor deberá entregar los manuales de usuario y de instalación de todos los productos ofertados en físico y/o formato digital.
- ✓ El proveedor deberá entregar un documento impreso refrendado por el fabricante que certifique el número de licencias de software antivirus y antimalware verificable en la web del fabricante, a nombre del Ministerio de Trabajo y Promoción del Empleo.

Los bienes (licencias) serán entregados en el almacén central del MTPE ubicado en la Avenida Salaverry 655, Jesús María – Lima, Perú.

c) **Tercer entregable.** Al finalizar la implementación de la solución; el contratista entregar lo siguiente.

- ✓ Informe final, el cual deberá tener un reporte de los equipos de cómputo instalados, indicando el nombre y la dirección IP de los equipos de (CPU), la sede en que fue instalada el antivirus y antimalware.

d) **Cuarto entregable:** Al finalizar la capacitación, el contratista deberá entregar lo siguiente:

- ✓ Certificados de las capacitaciones realizadas al personal del MTPE, indicando el nombre del participante, nombre del curso, fechas en las que se realizó la capacitación y el número de horas.
- ✓ Acta de finalización de cursos de capacitación, suscritas entre el contratista y el área usuaria.

6.2 De la prestación accesoria

Informes mensuales, donde debe incluir reportes de infecciones bloqueadas y no bloqueadas en el periodo, versión de software o parches realizados, solicitudes de Fallas y Reportes correspondiente al periodo, debe incluirse el ticket de atención y el tiempo de solución por cada solicitud realizada.

VII. LUGAR Y PLAZO DE LA PRESTACIÓN

El plazo comprende las siguientes prestaciones:

7.1 Prestación Principal

El plazo de implementación para la prestación principal es de hasta cuarenta y cinco (45) días calendario, el mismo que comprende las siguientes actividades:

Primer entregable: Plan de trabajo, hasta los cinco (05) días calendario, contados a partir del día siguiente de la suscripción del contrato.

El Plan de Trabajo deberá ser aprobado mediante acta suscrita, por la Oficina de Tecnologías de la Información (OTIC), en un plazo máximo de dos (02) días calendario de presentado.
El lugar de presentación será a través de la ventanilla de tramite documentario de la Sede Central del Ministerio de Trabajo y Promoción del Empleo, Av. Salaverry 655, Distrito de Jesús María, Lima-Perú.

Segundo entregable: La entrega de licencias será hasta los quince (15) días calendario, contados a partir del día siguiente de la suscripción del contrato.

La entrega de licencia deberá ser aprobado mediante acta suscrita por la Oficina de Tecnologías de la Información y Comunicaciones (OTIC), en un plazo máximo de dos (02) días calendario de entregado.

Los bienes serán entregados en el almacén central del MTPE ubicado en la Avenida Salaverry 655, Jesús María – Lima, Perú.

Tercer entregable: El plazo de la etapa de implementación, será de hasta treinta (30) días calendario, contados a partir del día siguiente de la suscripción del acta de entrega de bienes.

La implementación y puesta en marcha, debe ser aprobado mediante acta suscrita por la Oficina de Tecnologías de la Información y Comunicaciones (OTIC). en un plazo máximo de tres (03) días calendario de presentado.

La implementación de los bienes adquiridos, será en las instalaciones del Ministerio de Trabajo y Promoción del Empleo – MTPE ubicado en la Avenida Salaverry 655, Jesús María, Lima-Perú.

Cuarto entregable: Capacitación, el plazo del dictado será dentro de los treinta (30) días calendarios, contados desde el día siguiente de suscrito el contrato.

El lugar de presentación será a través de la ventanilla de tramite documentario o mesa de partes virtual, de la Sede Central del Ministerio de Trabajo y Promoción del Empleo, Av. Salaverry 655, Distrito de Jesús María, Lima-Perú.

7.2 Prestación Accesoria

Soporte Técnico:
El plazo para las prestaciones accesorias brindada será por el periodo de 365 días calendario, en los cuales se brindará el soporte técnico y la remisión de informes mensuales.

VIII. FORMA DE PAGO

El pago se realizará de acuerdo al siguiente detalle:

De la prestación principal:

El pago de la prestación principal se realizará en dos (02) armadas, de acuerdo al siguiente detalle:

- Primer pago. - 80% de la prestación principal a la aprobación del primer y segundo entregable, previa conformidad emitida por la Oficina de Tecnologías de Información y Comunicaciones.

- Segundo pago. - 20% de la presentación principal, a la aprobación del tercer y cuarto entregable, previa conformidad emitida por la Oficina de Tecnologías de Información y Comunicaciones.

De la prestación accesoria:

El pago por el soporte técnico correspondiente a la Prestación Accesoria se efectuará en dos (02) pagos semestrales, luego de emitida la Conformidad respectiva, previamente se debe haber brindado el servicio de Soporte Técnico y la remisión de los Informes mensuales.

IX. CONFORMIDAD

La conformidad de la adquisición será otorgada por la Oficina de Tecnologías de la Información y Comunicaciones de la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones.

X. REQUISITOS MÍNIMOS QUE DEBE CUMPLIR EL POSTOR

El postor deberá contar con la acreditación del fabricante, como partner y/o distribuidor autorizado de la solución de antivirus y antimalware corporativo propuesto, con lo cual garantizará las acciones necesarias ante algún incidente por infección por software malicioso ante el fabricante del producto ofertado. Dicha condición deberá ser acreditado mediante carta y deberá ser presentada en la Propuesta Técnica, dirigida a la entidad convocante e indicando el número del proceso, en la cual indique que el proveedor es un distribuidor autorizado para su comercialización.

XI. PERSONAL CLAVE

(01) Especialista implementador

Funciones:

- Mantenimiento e Instalación de la consola (servidor del antivirus).
- Despliegue del antivirus en los servidores y en los usuarios finales.
- Mantenimiento o actualizaciones del antivirus antimalware

XII. RESPONSABILIDAD POR VICIOS OCULTOS

La recepción conforme de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos (artículo 173° del Reglamento de la Ley N° 30225, ley de contrataciones del Estado).

El plazo de responsabilidad del postor es de un (01) año contado a partir de la conformidad otorgada por LA ENTIDAD (artículo 40° de la Ley de Contrataciones del Estado).

XIII. PENALIDADES

Penalidad por Mora

En caso de retraso injustificado en la entrega y/o implementación del objeto del contrato, la entidad aplicará automáticamente una penalidad por mora por cada día de retraso y se calcula de acuerdo a la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{monto vigente}}{F \times \text{plazo vigente en días}}$$

Donde:

F = 0.40 para plazos menores o iguales a sesenta (60) días.

Monto = Es el monto total del entregable según contrato.

Tanto el monto como el plazo se refieren, según corresponda, al contrato o ítem que debió ejecutarse o, en caso que estos involucraran obligaciones de ejecución periódica, a la prestación parcial que fuera materia de retraso.

XIV. OTRAS PENALIDADES

En caso el proveedor se exceda en el tiempo de solución de averías críticas (04 horas como máximo), averías no críticas (24 horas como máximo) y Requerimientos (48 horas como máximo), según lo indicado en la tabla del numeral V, las horas de exceso serán consideradas para el cálculo de penalidades, según la tabla indicada líneas abajo. Se debe considerar que para realizar dicho cálculo se verificará los tiempos indicados en los informes mensuales que reporte el proveedor, los cuales serán contrastados con la información del ticket de atención enviada por mail según se indica en numeral V.

La penalidad a evaluar de forma mensual estará en función de la siguiente tabla:

Otras penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
01	Cuando el exceso de horas por mes es mayor a 01 y menor igual a 03 horas	Monto prestación accesoria por 01 %	Informe de evaluación a la oficina de abastecimiento
02	Cuando el exceso de horas por mes es mayor a 03 y menor igual a 06 horas	Monto prestación accesoria por 02 %	Informe de evaluación a la oficina de abastecimiento
03	Cuando el exceso de horas por mes es mayor a 06 y menor igual a 09 horas	Monto prestación accesoria por 03 %	Informe de evaluación a la oficina de abastecimiento
04	Cuando el exceso de horas por mes es mayor a 09 y menor igual a 12 horas	Monto prestación accesoria por 04 %	Informe de evaluación a la oficina de abastecimiento
05	Cuando el exceso de horas por mes es mayor a 12 y menor igual a 16 horas	Monto prestación accesoria por 05 %	Informe de evaluación a la oficina de abastecimiento
06	Cuando el exceso de horas por mes es mayor a 16 y menor igual a 20 horas	Monto prestación accesoria por 06 %	Informe de evaluación a la oficina de abastecimiento
07	Cuando el exceso de horas por mes es mayor a 20 y menor igual a 24 horas	Monto prestación accesoria por 08 %	Informe de evaluación a la oficina de abastecimiento
08	Cuando el exceso de horas por mes es mayor a 24 horas	Monto prestación accesoria por 10 %	Informe de evaluación a la oficina de abastecimiento

Penalidad (1): El porcentaje de penalidad aplicable al pago semestral.

El Ministerio podrá cobrar una penalidad hasta un monto máximo equivalente al 10% del monto del pago de prestaciones accesorias. Cuando se llegue a cubrir el monto máximo de la penalidad (10%), la entidad podrá resolver el contrato por incumplimiento.

XV. CONFIDENCIALIDAD DE LA INFORMACIÓN:

El contratista se compromete y se obliga a no difundir a terceros la información obtenida, bajo responsabilidad de las acciones legales pertinentes por parte de la Entidad, en caso suceda lo contrario.

El contratista mantendrá en forma reservada toda la información suministrada por la Entidad y al finalizar el contrato, devolverá todos aquellos documentos que le fueron proporcionados. Esto incluye tanto material impreso como grabado en medios magnéticos y/o digitalizados.

Toda la información y/o documentación generada como parte de la adquisición será de propiedad exclusiva de la Entidad, no pudiendo el proveedor utilizarla fuera de la presente adquisición.

XVI. PROTOCOLO SANITARIO FRENTE A LA PROPAGACIÓN DEL COVID 19

Para el inicio de sus actividades, todo proveedor deberá tener en consideración lo siguiente:

✓ Contar con su "Plan para la Vigilancia, Prevención y Control de COVID-19 en el Trabajo". Mediante Decreto Supremo N° 117-2020-PCM, se establece en el numeral 1 de la primera disposición complementaria final que "Para la reanudación de las actividades (…), debiendo asimismo elaborar su "Plan para la vigilancia, prevención o control de COVID – 19 en el trabajo", el cual debe estar a disposición de los clientes y trabajadores asi como de las autoridades competentes, para su fiscalización. Asimismo, previo a la reanudación de las actividades, el referido Plan debe ser remitido vía correo electrónico al Ministerio de Salud, a la siguiente dirección: empresa@minsa.gob.pe, con lo cual, en cumplimiento además con los requisitos establecidos en el presente numeral, se entenderá que la entidad, empresa, persona jurídica o núcleo ejecutor cuenta con autorización automática para iniciar operaciones.

✓ Presentar al Ministerio de Trabajo y Promoción del Empleo, su "Plan para la Vigilancia, Prevención y Control de COVID-19 en el Trabajo", el cual será remitido a la Oficina General de Recursos Humanos y a la Oficina de Seguridad y Defensa Nacional, para su revisión correspondiente y posterior verificación de su cumplimiento durante la ejecución de sus actividades en las instalaciones del Ministerio de Trabajo y Promoción del Empleo.

✓ Implementar y garantizar el estricto cumplimiento de los lineamientos sanitarios frente al COVID 19, en todos los procesos y etapas de desarrollo y ejecución de los servicios que se realicen en la Unidad Ejecutora N° 001: Ministerio de Trabajo – Oficina General de Administración:

✓ Fase de inicio de actividades (planificación).

✓ Fase de ejecución (supervisión y verificación).

✓ Fase de cierre (conformidad y recepción).

Documentos a presentar para la suscripción del contrato.

• "Plan para la Vigilancia, Prevención y Control de COVID-19 en el Trabajo",

XVI. REQUISITOS DE CALIFICACION

A	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	Requisito: El postor debe acreditar un monto facturado acumulado equivalente a S/. 200,000.00 (doscientos mil con 00/100 soles), por las ventas 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 postores que declaren tener la condición de micro y pequeña empresa, se acredita una experiencia de 29,720.81 (Veintinueve mil, setecientos veinte con 81/100 soles), 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 Se consideran bienes similares a: ventas en adquisición de software antivirus y/o, adquisición de software antivirus que incluye instalación y/o adquisición de antivirus que incluye implementación de software y/o solución de antivirus y/o antimalware que incluye soporte para end point **Acreditación**: 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[1] correspondientes a un máximo de veinte (20) contrataciones. 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 Nº 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

[1] 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".*

	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 una persona absorbida 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 Nº 8** referido a la Experiencia del Postor en la Especialidad. **Importante** *En el caso de consorcios, solo 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".*
B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.1	**EXPERIENCIA DEL PERSONAL CLAVE**
	Requisitos: ✓ Un (01) año de experiencia laboral, en implementación y/o instalación y/o mantenimiento y/o soporte antivirus y/o antimalware para end point, del personal clave requerido como Especialista Implementador. Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias

	o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto. **Importante** • *El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores.* • *Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento y la fecha de emisión y nombres y apellidos de quien suscribe el documento.* • *En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.* • *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*