

**PERÚ****Ministerio  
de Transportes  
y Comunicaciones****Secretaría General****Oficina General de  
Tecnología de la  
Información**

"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

**TÉRMINOS DE REFERENCIA  
SERVICIO DE SUSCRIPCIÓN DE UNA LICENCIA DE SOFTWARE DE  
PROTECCIÓN, DETECCIÓN Y RESPUESTA EXTENDIDA (XDR) PARA LOS  
EQUIPOS INFORMÁTICOS DEL MTC**

Unidad Orgánica:	Oficina General de Tecnología de la Información
Meta Presupuestaria:	Sec. Fun. 0295 - Desarrollo y Mantenimiento de los Sistemas Informáticos
Actividad del POI	AO100107200151 Gestión de la Infraestructura Tecnológica y Seguridad Informática

**1. DENOMINACIÓN DE LA CONTRATACIÓN**

Contratación del servicio de suscripción de una licencia de software de protección, detección y respuesta extendida (XDR), para los equipos informáticos del Ministerio de Transportes y Comunicaciones - MTC

**2. OBJETIVO**

Contratación de un servicio de suscripción de una licencia de seguridad basada en software para los equipos informáticos del Ministerio de Transportes y Comunicaciones (MTC), que incluya capacidades de protección avanzada, detección temprana de amenazas y respuesta eficiente ante incidentes de seguridad.

**3. ANTECEDENTES**

Actualmente el MTC cuenta con más de trescientos (300) servidores entre físicos y virtuales; así como equipos de cómputo (estaciones de trabajo) críticos, los cuales requieren la protección, detección y respuesta ante amenazas cibernéticas que podrían afectar la disponibilidad e integridad de la información.

Que, la Resolución Ministerial N° 658-2021-MTC/01, aprueba el Texto Integrado del Reglamento de Organización y Funciones del Ministerio de Transportes y Comunicaciones, en su artículo 83 precisa:

*"Funciones de la Oficina de Infraestructura Tecnológica y Seguridad Informática del Reglamento de Organización y Funciones: "Diseña lineamientos, directivas, protocolos y otros documentos de gestión para la implementación de las **materias de seguridad informática**, en coordinación con el órgano competente del ministerio; así como realizar acciones de seguimiento para su cumplimiento"*

**4. FINALIDAD PÚBLICA**

Brindar una capa de seguridad en la infraestructura informática del Ministerio de Transportes y Comunicaciones (MTC) mediante la contratación de una solución integral basada en software que permita proteger, detectar y responder ante amenazas cibernéticas, asegurando así la continuidad y la confidencialidad de las operaciones del Ministerio.

**5. ACTIVIDADES A REALIZAR**

La solución ofertada deberá regirse por lo indicado en las características y descripciones detalladas en el ítem 5.1 y conforme a lo siguiente:

**PERÚ****Ministerio  
de Transportes  
y Comunicaciones****Secretaría General****Oficina General de  
Tecnología de la  
Información**

"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

**5.1. ALCANCE Y DESCRIPCIÓN DEL SERVICIO**

ÍTEM	OBJETO	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA	DETALLE
1	<b>PRESTACIÓN PRINCIPAL</b>	CONTRATACIÓN DE UNA LICENCIA DE SOFTWARE DE SEGURIDAD XDR PARA 450 EQUIPOS.	1	Unidad	LICENCIA
	<b>PRESTACIÓN ACCESORIA</b>	SOPORTE TÉCNICO.	1	Servicio	SOPORTE TÉCNICO.
		CAPACITACIÓN	1	Servicio	CAPACITACIÓN

**5.2. CARACTERÍSTICAS DEL SERVICIO**

Las cuales se desagregarán en:

➤ **PRESTACIÓN PRINCIPAL**

Contratación del servicio de suscripción de una licencia de software de protección, detección y respuesta extendida (XDR), para los equipos informáticos del Ministerio de Transportes y Comunicaciones – MTC. Incluye: Activación.

➤ **PRESTACIÓN ACCESORIA**

- Soporte técnico.
- Capacitación.

**5.2.1. PRESTACIÓN PRINCIPAL:**

<b>CARACTERÍSTICAS TÉCNICAS MÍNIMAS</b>	
<b>1. Aspectos Generales.</b>	a) La solución debe consistir en un software de seguridad que brinde protección, detección y respuesta extendida (XDR) a través de una licencia para cuatrocientos cincuenta (450) equipos de cómputo. b) Deberá brindar un almacenamiento de telemetría del endpoint cuya información deberá estar disponible como historial por lo menos treinta (30) días. c) Deberá contar con soporte del fabricante durante todo el tiempo de servicio. d) Deberá haber logrado una efectividad de protección de ataques de 100% según el reporte de MITRE ATT&CK de los últimos dos (02) años. e) Deberá estar ubicado como uno de los líderes dentro del cuadrante mágico de Gartner para soluciones EPP (Endpoint Protection Platform) durante los últimos dos (02) años. f) El postor podrá integrar tecnologías de diferentes marcas para cumplir los requerimientos mínimos solicitados en las presentes especificaciones técnicas.
<b>2. Características de seguridad.</b>	<b>2.1 Protección contra exploits</b> a) Debe identificar y bloquear técnicas de explotación sin necesidad de utilizar firmas y/o heurísticas. La solución no deberá tener ningún componente que requiera actualizar una base de datos de firmas. b) El bloqueo de exploits deberá ser posible incluso en procesos desarrollados inhouse, la solución deberá permitir especificar los nombres de los procesos que serán protegidos contra exploits. c) Deberá proteger la explotación de vulnerabilidades de sistemas operativos y aplicaciones que incluso se encuentren sin el parche de seguridad instalado.



PERÚ

Ministerio  
de Transportes  
y Comunicaciones

Secretaría General

Oficina General de  
Tecnología de la  
Información

"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

	<p>d) La protección contra vulnerabilidades deberá ser independiente al CVE identificado, la solución deberá proteger cualquier intento de explotación incluyendo a vulnerabilidades de día cero que no tengan un CVE.</p> <p>e) Bloquear técnicas de explotación de vulnerabilidades, como mínimo Return Oriented Programming (ROP), Heap Spray, Jit Spray, Shell link, Structured Exception Handler, CPL Execution Process.</p> <p>f) Identificación y prevención de intentos de escalación de privilegios a nivel de Kernel.</p> <p>g) Capacidad de crear un snapshot (dump) de la memoria RAM al momento de prevenir la ejecución de una técnica de explotación, con la finalidad de proporcionar información forense sobre el evento.</p> <p>h) Prevención de técnicas de explotación que utilizan Java Deserialization, Kernel Integrity Monitor (KIM), Local Threat Evaluation Engine (LTEE), Reverse Shell Protection, Shellcode Protection, SO Hijacking Protection, Webshell.</p> <p>i) Todas las capacidades de prevención de exploits deberán estar disponibles de manera offline, sin necesidad de tener una conexión a la consola.</p> <p><b>2.2 Protección contra malware</b></p> <p>a) Deberá contar con funcionalidades de antimalware de siguiente generación, entendiéndose antimalware de siguiente generación como plataformas que utilizan algoritmos de aprendizaje de máquina (machine learning) para detectar y bloquear el malware; no deberá tener ningún componente que requiera actualizar una base de datos de firmas de antivirus.</p> <p>b) El algoritmo de machine learning deberá operar de manera local en el endpoint sin depender de una conexión permanente a la consola.</p> <p>c) Deberá ser capaz de enviar a cuarentena un archivo malicioso que intente copiarse o escribirse en alguna carpeta del endpoint, sin necesidad de que el archivo sea ejecutado.</p> <p>d) Deberá ser capaz de detectar y bloquear cambios sospechosos en la imagen UEFI, que intenten comprometer el proceso de arranque del host, antes de que se cargue el sistema operativo.</p> <p>e) Debe prevenir el robo de contraseña a partir de la lectura de la memoria RAM (mimikatz)</p> <p>f) Contar con un módulo de prevención contra ransomware que podrá ser configurado en modo normal y riguroso.</p> <p>g) Capacidad de prevenir ataques de Cryptomining a partir del comportamiento del objeto ejecutado.</p> <p>h) Deberá ofrecer protección contra scripts de tipo webshell.</p> <p>i) Deberá ser capaz de prevenir ataques basados en el Bypass del UAC (User Account Control) que intenten escalar privilegios.</p> <p>j) Deberá ser capaz de analizar datos de paquetes de red para detectar comportamientos maliciosos</p> <p>k) Adicionalmente a la protección basada en machine learning, deberá contar con la capacidad de identificar el comportamiento de la amenaza, de tal forma que la actividad maliciosa de un archivo se pueda detectar y bloquear en una fase temprana.</p> <p>l) Capacidad de prevenir contra shells reversos (reverse shell) para sistemas operativos Linux.</p> <p>m) Capacidad para bloquear ataques que permitan a un contenedor tener acceso al sistema operativo del host (container escaping) para sistemas Linux.</p> <p>n) Capacidad de poder colocar los malware en una carpeta de cuarentena</p> <p>o) Capacidad de colocar en lista permitida los archivos o directorios, para exceptuar la inspección.</p>
--	--



- p) Capacidad de realizar escaneos a demanda y programados, con el objetivo de identificar malware dormido en los endpoints.

### **2.3 Sandboxing**

- a) El agente deberá ser capaz de enviar automáticamente el archivo a un entorno de sandbox para ser emulado. Esta capacidad deberá estar disponible para sistemas Windows, MacOS, Linux y Android.
- b) El sandbox podrá ser del mismo fabricante que el agente de seguridad o un fabricante tercero integrado.
- c) El sandbox deberá estar basado en nube y debe tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
- d) El sandbox deberá soportar el análisis de al menos 500 mil archivos por día. El sandbox deberá tener capacidad de analizar archivos de hasta 100 MB de peso o superior.
- e) Deberá garantizar la privacidad y seguridad del contenido de los archivos analizados, para lo cual se requiere que cuente como mínimo con las certificaciones SOC2 Plus de AICPA, ISO 27001, ISO 27017 e ISO 27018.

### **2.4 Control de dispositivos**

- a) Debe permitir gestionar los puertos USB que permitan conectar dispositivos como: discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles, unidades lectoras de discos floppy externas con conexión USB.
- b) Debe de permitir generar perfiles de excepciones para poder conectar dispositivos en puertos USB utilizando los siguientes parámetros: tipo de dispositivo, tipo de permiso a asignar (lectura/escritura o sólo lectura), fabricante (debe de contener una lista predeterminada), producto (debe de contener una lista predeterminada) y número de serie.
- c) Las políticas generadas deben de poder asignarse a un endpoint en particular, a un grupo de endpoints.
- d) Deberá ser capaz de integrarse a Active Directory para establecer políticas de control de USB en base a grupos de LDAP.
- e) Debe de permitir la creación de excepciones temporales a partir de una alerta registrada, para permitir el dispositivo solo durante un tiempo configurable.
- f) Capacidad de añadir nuevos tipos de dispositivos agregando el GUID de Windows correspondiente.

### **2.5 Telemetría y colección de datos y eventos**

- a) Para los equipos con sistema operativo Windows, el agente deberá poder capturar lo siguiente:
- Proceso ejecutado, incluyendo el tiempo de inicio, el tamaño del archivo asociado.
  - Actividades de creación, escritura, renombre, eliminación, modificación de archivos.
  - Archivos DLL: ruta completa, dirección base, id del proceso, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL.
  - Creación y terminación de los procesos, incluyendo los siguientes atributos: nombre del proceso padre, ID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.
  - Inyecciones en hilos de procesos: ID del hilo padre, ID del hilo nuevo o que se ha terminado, proceso que inició el hilo (en caso de ser un proceso distinto).



PERÚ

Ministerio  
de Transportes  
y Comunicaciones

Secretaría General

Oficina General de  
Tecnología de la  
Información

"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

	<ul style="list-style-type: none"> <li>• Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP), solicitudes DNS, conexiones y desconexiones HTTP.</li> <li>• Estadísticas de red: volumen de tráfico en eventos de subida y descarga de tráfico TCP.</li> <li>• Acciones sobre los registros de Windows: Configuración o eliminación de valores del registro. Creación, modificación, eliminación, adición, restauración y guardado de llaves del registro. Con los siguientes parámetros: ruta del registro del valor o llave que fue modificado; nombre del valor o llave modificado; datos del valor modificado.</li> <li>• Sesiones del sistema operativo: inicio de sesión, cierre de sesión, conexión y desconexión. Considerando los siguientes atributos: inicio de sesión interactivo, id de la sesión, estado de la sesión, y si la sesión es local o remota.</li> <li>• Llamadas (calls) RPC y llamadas de Sistema (Syscall)</li> <li>• Logs de eventos de Windows, incluyendo eventos de Seguridad, Aplicación.</li> </ul> <p>b) <u>Para los equipos con sistema operativo Linux, el agente deberá poder capturar lo siguiente:</u></p> <ul style="list-style-type: none"> <li>• Para los archivos: las acciones de creación, apertura, escritura y eliminación, incluyendo la ruta completa del archivo y el hash del archivo (para ciertos archivos y sólo si el archivo fue escrito). Información del copiado o renombrado de los archivos, incluyendo las rutas completas tanto del archivo original como del modificado. Las acciones para cambiar el dueño (chown) y el modo (chmod) de los archivos, incluyendo la ruta completa del archivo, así como el nuevo dueño o nuevos atributos.</li> <li>• Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.</li> <li>• Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).</li> <li>• Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.</li> <li>• Logs de eventos de autenticación.</li> </ul> <p>c) <u>Para los equipos con sistema operativo MacOS, el agente deberá poder capturar lo siguiente:</u></p> <ul style="list-style-type: none"> <li>• Actividades de creación, escritura, renombre, eliminación, modificación de archivos.</li> <li>• Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.</li> <li>• Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).</li> <li>• Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.</li> <li>• Logs de eventos de autenticación.</li> </ul> <p>d) La solución deberá poder almacenar la información recolectada en formato raw log (log crudo) por al menos 30 días.</p>
--	--



**2.6 Capacidades de analítica y detección de amenazas**

- a) Deberá mostrar una secuencia gráfica del incidente de seguridad que correlacione las alertas individuales con el objetivo de identificar la causa raíz. Esta secuencia gráfica deberá ser construida de manera automática a partir de la inteligencia artificial de la plataforma.
- b) Deberá mostrar información de los procesos correlacionados en la secuencia gráfica, mostrando los siguientes datos: ruta de ejecución, nombre de usuario que ejecutó el proceso, entidad que firmó el proceso, valor SHA256 del ejecutable relacionado con el proceso, veredicto del análisis del sandbox y línea de comandos de la ejecución.
- c) Por cada proceso correlacionado en la secuencia gráfica del incidente se deberá mostrar lo siguiente:
  - Fecha, hora, hostname, dirección IP, nombre del usuario, sistema operativo del equipo que generó el proceso.
  - Alertas relacionadas al proceso analizado con su respectiva descripción, acción tomada sobre la alerta, categoría de la amenaza, ejecutable que lo inicializó, táctica y técnica del ataque según el framework MITRE ATT&CK.
  - Actividad de la red del proceso: IP y puerto origen, IP y puerto destino, resolución del DNS, país destino, indicar si la conexión fue exitosa o fallida.
  - Creación, escritura, lectura, eliminación, renombre, cambio de atributos, hash en SHA256 y MD5 de los archivos relacionados al proceso analizado. En caso del renombre deberá mostrar el nombre anterior y actual para facilitar la investigación del analista.
  - Creación, apertura, escritura, eliminación, renombre, cambio de atributos de los directorios relacionados al proceso analizado.
  - Actividad sobre la clave y valores de registros, tales como creación, eliminación, carga, apertura, renombre, escritura, del proceso analizado.
  - Mostrar los system calls, rpc calls y procesos inyectados sobre cada proceso analizado.
  - Deberá contar con un mecanismo inteligente que separe de manera automática los binarios y DLLs no significados de la secuencia gráfica del incidente.
- d) Deberá tener más de 500 casos de uso automáticos de detección de amenazas complejas basadas en comportamiento y procesadas con inteligencia artificial.
- e) Deberá permitir crear reglas personalizadas de detección de amenazas, las cuales deberán estar basados en comportamientos de los usuarios y hosts, para ello deberá ser posible especificar en la regla uno o varios de los siguientes atributos: actividad de archivos (lectura, borrado, modificación, escritura); ejecución de procesos y línea de comando ejecutada; cambios en las claves de registro de Windows, especificando el nombre, valor de la clave de registro y tipo de operación (creación, lectura, edición); acceso a DLL de Windows; eventos de login o logout; interacción del endpoint con cualquier IP privada o pública, especificando el puerto origen y/o destino.
- f) Deberá permitir enriquecer las reglas de correlación con atributos asociados a Tácticas y Técnicas de Ataque, Tipo de Amenaza, Severidad.
- g) Deberá contar con integración al Active Directory para extraer información contextual del usuario, incluyendo el departamento en el cual labora, número de teléfono, última fecha de autenticación.
- h) El timeline del ataque deberá mostrar el intento de ataque en diferentes fases de explotación acorde al Framework MITRE ATT&CK, tales como Ejecución, Persistencia, Descubrimiento, Desplazamiento Lateral, Command & Control, Exfiltración.

**2.7 Capacidades de investigación y Threat Hunting**

- a) Deberá permitir realizar búsquedas avanzadas sobre la actividad de los endpoints:
- Actividad de los archivos, identificando las siguientes operaciones: creación, lectura, eliminación, escritura y renombrar.
  - Actividad de red, identificando el tráfico saliente, entrante, IP origen e IP destino, Puerto origen y Puerto destino, protocolo de red.
  - Actividad en el registro Windows, identificando la creación, eliminación, renombrado, definición de valores, eliminación de valores de las llaves de registro.
  - Actividad de procesos, identificando si se trata de una ejecución o inyección, ruta desde donde se ejecuta, comando que inicializa el proceso, usuario, hash en SHA256 y MD5.
  - Actividad en el Log de Eventos de Windows, identificando la descripción, ID del evento, nivel, mensaje, nombre del proveedor y usuario.
  - Actividad de autenticación al endpoint
  - Permitir realizar búsquedas en base a cualquier dato recopilado por la plataforma.
  - Permitir seleccionar las columnas y orden de los datos mostrados como resultados de las búsquedas.
  - Los resultados de las búsquedas deberán poder ser mostrados en una tabla o una gráfica de tipo pye, columnas, burbuja y área, con la finalidad de facilitar el análisis del investigador.
  - Deberá contar con una librería predeterminada de búsquedas habituales realizadas en una labor de threat hunting. Esta librería podrá ser editada según la labor del investigador.
- b) Deberá contar con un lenguaje propio para realizar consultas de la telemetría almacenada, deberá incluir al menos los siguientes criterios: Filtros por cada atributo recolectado del endpoint (procesos, archivos interacciones de red, login/logout, actividad en claves de registro y DLLs) con coincidencia total o parcial de cada atributo; uso operadores booleanos (and, or, not); operadores de comparación (igual, no igual, mayor que, menor que, mayor o igual que, menor o igual que); capacidad para especificar un límite de resultados (top 10, 20, 100, 500, 1000, personalización en general); operadores de comparación de datos; operadores matemáticos (promedio, contar, contar-distinto, máximo, mínimo, sumar); uso de expresiones regulares.
- c) Las búsquedas deberán estar disponibles tanto para endpoints en línea y fuera de línea.
- d) Permitir seleccionar las columnas y orden de los datos mostrados como resultados de las búsquedas.
- e) La solución debe contar con columnas de los dashboards de visualización de datos y deberán de ser configurables, para poder seleccionar las que sean del interés del analista.
- f) Las búsquedas deberán de poder programarse para ser ejecutadas en un día y hora determinados durante una sola ocasión y también de manera recurrente.
- g) Deberá contar con una librería predeterminada de búsquedas habituales realizadas en una labor de threat hunting. Esta librería podrá ser editada según la labor del investigador.
- h) Todas las opciones de búsqueda anteriormente detalladas deberán poder ser utilizadas para configurar reglas personalizadas de seguridad, que permitan generar una alerta cuando exista alguna coincidencia en el log (o logs) recolectados con la regla de búsqueda.

**2.8 Capacidades de gestión de incidentes**

- a) Deberá agrupar todas las alertas relacionadas a un incidente de seguridad de manera automática.
- b) Por cada incidente mostrado deberá mostrar los elementos relacionados como ejecutables, hashes, direcciones IP.
- c) Deberá mostrar los hosts y usuarios asociados al incidente.
- d) Las alertas e incidentes de seguridad deberán tener una valoración cualitativa de al menos 4 niveles de severidad: bajo, medio, alto y crítico. Estos niveles de severidad podrán ser modificados de manera manual o automática.
- e) Tener la capacidad de poder agrupar las alertas relacionadas en incidentes, así como proporcionar un contexto de este.
- f) Debe tener la capacidad de poder extraer los elementos importantes o relevantes de las alertas, y mostrarlos a manera de resumen en la pantalla de análisis del incidente.
- g) Debe contar con un dashboard donde se muestran los incidentes de seguridad que no han sido atendidos (clasificados de acuerdo con su criticidad en alta, media y baja), un resumen sobre los incidentes de seguridad (clasificados por su plataforma, etc.)
- h) Debe permitir asignar cada alerta de seguridad a un analista administrador de la consola, esta asignación se puede hacer de forma manual o automática en base a ciertos criterios de la alerta. Por cada asignación que se realice se deberá notificar vía correo al analista.
- i) Cada incidente de seguridad debe tener un estado, tales como abierto, en proceso, cerrado, resuelto, o estados equivalentes.
- j) Debe permitir colocar un comentario por cada incidente, con el objetivo de llevar un seguimiento de este durante la investigación.
- k) Debe contar con un dashboard donde se describen las características de los incidentes de seguridad que se han generado. Este dashboard debe de permitir analizar a mayor detalle las alertas de seguridad, incluyendo los reportes generados por el agente.
- l) Debe tener un dashboard para monitorear el MTTR (mean time to response) en la gestión de incidentes.
- m) Deberá tener un motor automático de scoring de incidentes, que permitan dar una valoración cuantitativa en un puntaje de 0 a 100 en base a determinados criterios de cada alerta de seguridad, éste deberá de funcionar de manera paralela a la valoración cualitativa de los incidentes y alertas de seguridad.

**2.9 Capacidades de Threat Intelligence**

- a) Capacidad de alimentar la plataforma de Indicadores de Compromiso (IOC) de manera manual o automática vía API
- b) Los IOC soportados deberán ser de tipo Hash, Ruta, Nombre de archivo, Dominio, Dirección IP.
- c) Capacidad de agregar IOC de manera individual o masiva (por ejemplo, subiendo un archivo CSV)
- d) Capacidad de colocar un nivel de reputación, confiabilidad del IOC y una fecha de expiración.
- e) Debe poder integrarse a una plataforma tercera de Threat Intelligence como Virus Total.
- f) Mostrar un mapa geográfico que permita analizar la dirección IP detectada como parte de incidente, como mínimo deberá mostrar lo siguiente: fecha de registro, ISP (Internet Service Provider), país. La información deberá poder ser mostrada en base al país, proceso, puerto e IP destino.
- g) Deberá contar con un dashboard que permita analizar el comportamiento del hash de un archivo en particular, mostrando su nivel de reputación y si dicho hash ha sido detectado en otras alertas e incidentes.





PERÚ

Ministerio  
de Transportes  
y Comunicaciones

Secretaría General

Oficina General de  
Tecnología de la  
Información

"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

	<p><b>2.10 Capacidades de respuesta</b></p> <ol style="list-style-type: none"> <li>Deberá ser posible colocar en lista bloqueada y/o lista permitida uno o más hashes.</li> <li>Deberá permitir colocar en cuarentena un archivo malicioso detectado y/o bloqueado. La colocación en cuarentena deberá poder realizarse de manera manual y automática.</li> <li>Capacidad de extraer el archivo dump de la memoria RAM del endpoint a partir de una alerta revisada.</li> <li>Capacidad de extraer el malware o archivo sospechoso del endpoint hacia la consola, para poder ser analizado por el investigador</li> <li>Debe ser posible aislar el endpoint de la red para que no tenga comunicación con ningún dispositivo de la red interna o externa.</li> <li>Capacidad de configurar reglas de automatización que permitan ejecutar una acción determinada en los endpoints en base condiciones de alertas de seguridad, como mínimo estas reglas deberán permitir las siguientes acciones de manera automática: aislar el endpoint, hacer un escaneo de malware, extraer el malware desde el endpoint.</li> <li>Deberá ser posible realizar una conexión remota a cada endpoint que forme parte de una investigación para ejecutar las siguientes acciones: <ul style="list-style-type: none"> <li>Listar procesos y archivos</li> <li>Ejecutar instrucciones por línea de comandos (CMD y Powershell para el caso de Windows; Bash para el caso de Linux y MacOS).</li> <li>Ejecutar scripts basados en Python</li> </ul> </li> <li>Capacidad de ejecutar scripts remotamente a múltiples endpoints de manera concurrentes.</li> <li>Deberá contar con una librería de scripts predefinidos y deberá ser posible configurar scripts personalizados basados en Python.</li> <li>Capacidad de tareas remotas a múltiples endpoints, como mínimo cerrar procesos, eliminar archivos, eliminar y/o modificar claves de registro.</li> <li>Mostrar sugerencias para las remediaciones de un equipo comprometido.</li> <li>Capacidad de integración con un SIEM vía Syslog y plataformas SOAR.</li> </ol> <p><b>2.11 Descubrimiento de activos</b></p> <ol style="list-style-type: none"> <li>Deberá contar con un mecanismo para descubrir dispositivos de la red sin el agente instalado.</li> <li>El descubrimiento deberá tener la capacidad para identificar la dirección IP del equipo y el Sistema Operativo que no tienen el agente instalado.</li> <li>Permitir exceptuar los segmentos de red que no se desean escanear.</li> <li>Deberá contar con el licenciamiento adecuado para el descubrimiento de dispositivos en las diferentes sedes de la entidad.</li> </ol> <p><b>2.12 Capacidades de visibilidad del endpoint</b></p> <ol style="list-style-type: none"> <li>Deberá poder generar un inventario de las aplicaciones instaladas en las computadoras con sistema operativo Windows, MacOS y Linux</li> <li>Deberá generar un inventario de características de hardware del endpoint, como mínimo cantidad de memoria RAM; tipo, marca y capacidad de procesador; almacenamiento del disco duro; identificar si es servidor, desktop o laptop; sistema operativo y arquitectura.</li> <li>Deberá poder listar los usuarios locales creados en el endpoint y su respectivo estado (activo o inactivo)</li> </ol>
--	--





PERÚ

Ministerio  
de Transportes  
y Comunicaciones

Secretaría General

Oficina General de  
Tecnología de la  
Información

"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

	<p>d) Deberá poder listar los autoruns, servicios y unidades o carpetas compartidas para el caso de Windows.</p> <p>e) Deberá mostrar los daemons para el caso de MacOS y Linux</p> <p>f) Deberá ser capaz de guardar un histórico diario de estos inventarios, para poder comparar cambios que hubiesen ocurrido. Este histórico deberá estar disponible por al menos 30 días.</p> <p><b>2.13 Capacidades de análisis de vulnerabilidades</b></p> <p>a) Deberá mostrar las vulnerabilidades de los sistemas operativos de los endpoints, ofreciendo detalles de los CVEs, incluyendo el nivel de severidad y métricas según la base de datos de vulnerabilidades de NIST.</p> <p>b) Deberá mostrar los KB instalados por cada endpoint.</p> <p>c) Deberá mostrar las vulnerabilidades a nivel de las aplicaciones instaladas en sistemas Linux.</p> <p>d) Deberá permitir exportar en un archivo leíble en Excel todas las vulnerabilidades identificadas en cada endpoint.</p>
<b>3. Características del agente de la solución.</b>	<p>a) Deberá ser un agente ligero que incluso pueda convivir con cualquier otro software instalado en el endpoint.</p> <p>b) Soporte para las siguientes versiones de sistemas operativos:</p> <ul style="list-style-type: none"> <li>• Windows 8.1 y superior, Windows Server 2012 y superior</li> <li>• MacOS 10.13 y superior</li> <li>• Linux, distribuciones: CentOS 6 y superior, Debian 8 y superior, Red Hat Enterprise Linux 6 y superior, Suse for Enterprise 12.1 y superior, Ubuntu Server 12 y superior, Amazon Linux 2017 y 2018, Oracle Linux 6 y superior.</li> <li>• Android y iOS.</li> </ul> <p>c) No debe requerir el reinicio del equipo para que agente se encuentre operativo.</p> <p>d) Deberá estar protegido ante intentos de desinstalación o manipulación del agente.</p> <p>e) Deberá ser posible definir diferentes password de seguridad para diferentes grupos de endpoints.</p>
<b>4. Características de gestión de la solución.</b>	<p>a) La consola deberá estar basada 100% en nube, con el objetivo de no depender ni administrar infraestructura física local. La nube del fabricante deberá contar con las siguientes características:</p> <ul style="list-style-type: none"> <li>• Contar con la certificación SOC2 Tipo II o SOC2 Plus de AICPA, ISO 27001, ISO 27017, ISO 27018.</li> <li>• Contar con doble factor de autenticación para el login.</li> <li>• Permitir el acceso solo desde un rango de IP pública de la Entidad.</li> </ul> <p>b) La consola debe permitir la gestión de usuarios mediante roles preconfigurados y debe ser capaz de crear roles personalizados.</p> <p>c) Permite utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente.</p> <p>d) Cuenta con la capacidad de crear grupos que pueden alimentarse de forma estática y dinámica.</p> <p>e) Capacidad de personalización del dashboard para mostrar los widgets según las necesidades de la Entidad.</p> <p>f) Capacidad de almacenar una auditoría de eventos sobre las acciones realizadas en la consola</p> <p>g) Deberá permitir el envío automático de alertas al correo electrónico cuando se identifica una actividad maliciosa. Podrán aplicarse filtros a dichas alertas para solo mostrar las de mayor relevancia.</p> <p>h) Deberá permitir la generación de reportes a través de plantillas preconfiguradas y también permitir definir reportes personalizados.</p> <p>i) Mantener un historial de los reportes que han sido generados para su posterior consulta.</p> <p>j) Los reportes podrán ser enviados de forma automática y programada a una o más direcciones de correos electrónicos.</p>



PERÚ

Ministerio  
de Transportes  
y Comunicaciones

Secretaría General

Oficina General de  
Tecnología de la  
Información

"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

## **REQUISITOS DE LA OFERTA**

El postor para la presentación de la oferta, deberá acreditar con hojas de datos y/o datasheets y/u hojas técnicas y/o brochure, el cumplimiento de las características indicadas en el numeral 5.2.1, ítem N° 2, N° 3 y N° 04, y sus respectivos subítem de los términos de referencia, en idioma español. Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado.

### **5.2.2. PRESTACIÓN ACCESORIA**

#### **A) SOPORTE TÉCNICO**

- La prestación accesoria tendrá una vigencia de veinticuatro (24) meses, equivalentes a setecientos treinta (730) días calendario, y se inicia desde el día siguiente de la firma del acta de instalación y puesta en funcionamiento de la solución ofertada.
- El contratista debe contar con un Centro de Operaciones de Seguridad para el servicio de monitoreo local 24x7x365 con línea de comunicación gratuita 0800 para la atención de todos los incidentes de seguridad. El número deberá ser presentado para la suscripción del contrato.
- La ENTIDAD podrá abrir casos directamente con el fabricante, de requerirlo, por lo que el contratista deberá brindarle los accesos correspondientes.
- Contar con una mesa de ayuda propia para brindar el soporte 24x7x365 incluidos domingos y feriados.
- El servicio de soporte técnico a través de la mesa de ayuda comprenderá la solución de cualquier tipo de evento o problema que cause una interrupción parcial o total del servicio de la ENTIDAD, así como a la pérdida de la calidad o degradación del mismo. Adicionalmente, comprenderá la atención de consultas, solicitudes de reportes y solicitudes de análisis de auditoría; a todo ello se le denominará "requerimiento".
- Deberá brindar soporte técnico in situ a cargo de expertos profesionales en análisis de seguridad informática, quien asistirá a la ENTIDAD en forma personal en caso de fallas que no puedan ser solucionadas de manera remota, garantizando que la solución quede operativa y en óptimas condiciones.
- La generación del ticket del servicio de soporte técnico se efectuará a través de línea telefónica, correo electrónico u otros medios disponibles. Una vez recibida tal notificación, la mesa de ayuda del contratista, registrará el requerimiento o falla del servicio y proporcionará a la ENTIDAD un número de ticket.
- El nivel de servicio estará definido de acuerdo al siguiente plazo de atención.

Nivel de atención	Plazo
Brindar una atención que no implique un incidente con el software ofertado.	Hasta cuatro (04) horas.
Brindar el soporte correctivo y resolver incidentes reportados.	Hasta veinticuatro (24) horas.
En caso de que el incidente no pueda ser resuelto vía mesa de ayuda y el contratista deba escalarlo directamente al fabricante.	Hasta setenta y dos (72) horas.





PERÚ

Ministerio  
de Transportes  
y Comunicaciones

Secretaría General

Oficina General de  
Tecnología de la  
Información

"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

- El contratista a través del Centro de Operaciones de Seguridad, deberá monitorear los equipos de seguridad a través de una plataforma de monitoreo que permita tener un panorama integral de todos los dispositivos suministrados, evaluar el rendimiento y enviar alertas de forma automática sobre el estado de salud de los dispositivos.
- De producirse la publicación de alguna actualización del software ofertado durante el periodo de servicio contratado, el contratista deberá comunicarlo al personal responsable de la Oficina de Infraestructura Tecnológica y Seguridad Informática para la instalación, sin que esto signifique costos adicionales a la entidad.

#### **B) CAPACITACIÓN**

- El postor deberá considerar una capacitación oficial de la marca ofertada que incluya lo relacionado a la administración, gestión, resolución de problemas y buenas prácticas de la plataforma de seguridad ofertada.
- Deberá tener un mínimo de dieciséis (16) horas lectivas en modalidad virtual.
- La capacitación deberá ser realizada por un especialista certificado en la solución ofertada y para tres (03) colaboradores de la Oficina de Infraestructura Tecnológica y Seguridad Informática de la Oficina General de Tecnología de la Información.
- El contratista deberá enviar vía correo electrónico como mínimo un (01) día antes de iniciar el curso, el plan de capacitación (syllabus) a la casilla electrónica [UstrSegurinf@mtc.gob.pe](mailto:UstrSegurinf@mtc.gob.pe) para conocimiento de los participantes del programa.
- El plan de capacitación será validado por la Oficina de Infraestructura Tecnológica y Seguridad Informática, y quien deberá brindar su aprobación en un plazo no mayor a 24 horas a través de un correo electrónico dirigido al contratista.
- Deberá entregar un certificado oficial de capacitación a cada uno de los asistentes.
- El contratista deberá brindar todo el material teórico sobre la capacitación en formato digital para cada asistente de la capacitación, Esta documentación deberá estar en español (como caso excepcional se aceptará en inglés aquella documentación técnica que no pueda ser traducida) y en formato HTML o PDF o WORD.

## **6. PLAZO Y LUGAR DE EJECUCIÓN**

### **6.1. PLAZO DE LA PRESTACIÓN**

#### **6.1.1 PRESTACIÓN PRINCIPAL**

El plazo total de la prestación principal es de treinta (30) días calendario, contados a partir del día siguiente de la suscripción del contrato, divididos de la siguiente manera:

##### **➤ Plazo de entrega de la licencia de suscripción**

La entrega de la licencia de suscripción del software de seguridad será realizado en un plazo no mayor a quince (15) días calendario,



PERÚ

Ministerio  
de Transportes  
y Comunicaciones

Secretaría General

Oficina General de  
Tecnología de la  
Información

"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

contabilizado a partir del día siguiente de suscrito el contrato, y deberá ser remitido al correo electrónico [usrsegurinf@mtc.gob.pe](mailto:usrsegurinf@mtc.gob.pe), el mismo que es administrado por la Oficina de Infraestructura y Seguridad Informática de la Oficina General de Tecnología de la Información.

➤ **Plazo de instalación y puesta en funcionamiento**

La instalación y puesta en funcionamiento de la solución ofertada, será en un plazo no mayor a quince (15) días calendarios, contados a partir del día siguiente de la entrega de la licencia de suscripción.

Como máximo al día siguiente de concluida la etapa de instalación y puesta en funcionamiento de la solución ofertada, se formalizará mediante la respectiva acta de instalación y puesta en funcionamiento suscrita de modo conjunto por el representante del contratista y el especialista designado por la Oficina de Infraestructura Tecnológica y Seguridad Informática de la Oficina General de Tecnología de la Información.

**6.1.2 PRESTACIÓN ACCESORIA**

➤ **Capacitación**

La capacitación se realizará en un plazo no mayor a quince (15) días calendario, contabilizado a la firma del acta de instalación y puesta en funcionamiento de la solución ofertada.

➤ **Soporte técnico**

El soporte técnico a través de la mesa de ayuda y SOC es 24x7 durante los setecientos treinta (730) días calendario, contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de la solución ofertada.

**6.2. LUGAR DE LA PRESTACIÓN**

La prestación se brindará en modalidad remota o presencial en la Oficina General de Tecnología de la Información del Ministerio de Transportes y Comunicaciones, ubicada en la Sede Central (Jr. Zorritos N° 1203, Cercado de Lima).

La prestación principal relacionada a la instalación y puesta en funcionamiento de la solución ofertada se realizará en modalidad presencial en la Oficina General de Tecnología de la Información.

La prestación accesoria relacionada al soporte técnico se realizará de manera remota, salvo excepciones en caso de incidencia o falla que afecte la disponibilidad de la solución ofertada y se requiera la presencia del especialista de soporte técnico del contratista.

**7. ENTREGABLES**

El contratista deberá remitir a la entidad los siguientes entregables como parte de la prestación principal y accesoria.





PERÚ

Ministerio  
de Transportes  
y Comunicaciones

Secretaría General

Oficina General de  
Tecnología de la  
Información

"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

## 7.1. **PRESTACIÓN PRINCIPAL**

### ✓ **Entregable Único**

Será presentado hasta los siete (07) días calendario contados a partir del día siguiente de la firma del acta de instalación y puesta en funcionamiento de la solución ofertada, el cual comprenderá lo siguiente:

- Documento que acredite la licencia del software adquirido.
- Documento que indique la matriz de escalamiento para reportar incidentes: Nombre del contacto técnico, correo electrónico, número de teléfono.
- Informe técnico final de la instalación y puesta en funcionamiento de la solución ofertada.

## 7.2. **PRESTACIÓN ACCESORIA**

### **7.2.1. CAPACITACIÓN:**

#### **Entregable Único**

Será presentado hasta los siete (07) días calendario contados a partir del día siguiente de culminada la capacitación, el cual comprenderá lo siguiente:

- Certificados de capacitación de cada uno de los participantes.

### **7.2.2. SOPORTE TÉCNICO**

#### **Dos (02) entregables periódicos**

El contratista deberá entregar un informe técnico anual en donde considere los casos de soporte técnico realizados en el periodo.

La presentación de cada entregable se efectuará en un plazo máximo de siete (7) días calendario de culminado cada periodo anual, el mismo que deberá contener lo siguiente:

- ✓ Entregable Nro. 1: Informe que indique las atenciones realizadas (tickets) como parte del servicio de soporte técnico realizado dentro del primer año de servicio.
- ✓ Entregable Nro. 2: Informe que indique las atenciones realizadas (tickets) como parte del servicio de soporte técnico realizado dentro del segundo año de servicio.

La presentación de cada entregable será dirigido a la Oficina General de Tecnología de la Información y debe ser presentados a través de Mesa de Partes Virtual mediante el enlace: <https://mpv.mtc.gob.pe/> o de forma física en la Oficina de Atención al Ciudadano y Gestión Documental del MTC, sito en Jr. Zorritos N° 1203 – Cercado de Lima en el horario de 8:30 horas a 17:30 horas, siendo que los remitidos fuera de esa hora serán recepcionados como si hubiesen sido entregados al día siguiente hábil.

## 8. **REQUISITOS DEL PROVEEDOR**

### **8.1. CONDICIONES PARTICULARES**

- El postor debe ser representante autorizado o partner autorizado en el Perú, del software ofertado, para lo cual deberá una presentar carta del fabricante que lo acredite como representante o partner autorizado para comercializar y brindar los servicios de configuración, instalación y soporte. Dicho documento deberá ser presentado para la suscripción del contrato.



PERÚ

Ministerio  
de Transportes  
y Comunicaciones

Secretaría General

Oficina General de  
Tecnología de la  
Información

"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

## 8.2. RECURSOS A SER PROVISTOS POR EL CONTRATISTA

### 8.2.1 DEL PERSONAL CLAVE

#### a) UN (1) JEFE DEL PROYECTO

##### i) **Actividades**

Será el responsable de la coordinación y gestión durante toda la etapa de implementación de la solución de seguridad ofertada.

##### ii) **Perfil**

###### ✓ **Experiencia:**

Con una experiencia mínima de tres (03) años como Jefe y/o Supervisor de proyectos de seguridad informática.

###### ✓ **Formación académica:**

- Profesional titulado en Ingeniería de Sistemas, o Ingeniería de Computación, o Ingeniería Electrónica, o Ingeniería Informática, o Ingeniería de Telecomunicaciones, o Ingeniería de Seguridad Informática.
- Debe contar con certificación vigente en ITIL Foundation Certificate o Lead Cybersecurity Professional Certificate.

Para ello deberá adjuntar copia del certificado o diploma correspondiente.

#### b) DOS (2) ESPECIALISTAS EN SEGURIDAD INFORMÁTICA

##### i) **Actividades**

Serán responsables de la implementación, soporte y capacitación de la solución ofertada.

##### ii) **Perfil**

###### ✓ **Experiencia:**

Con una experiencia mínima de dos (02) años como especialista técnico o ingeniero especialista en la implementación y/o soporte y/o técnico de soluciones de protección antimalware o soluciones de protección EDR o soluciones de detección y respuesta para la protección del endpoint.

###### ✓ **Formación académica:**

- Mínimo Bachiller en Ingeniería de Sistemas, o Ingeniería de Computación, o Ingeniería Electrónica, o Ingeniería Informática, o Ingeniería de Telecomunicaciones, o Ingeniería de Seguridad Informática.
- Deberán contar con una certificación técnica emitida por el fabricante del software ofertado.

Para ello deberá adjuntar copia del certificado o diploma correspondiente.

#### **Nota:**

Las certificaciones deberán ser presentadas como parte de la documentación para perfeccionar el contrato.

La experiencia se contabiliza desde la obtención del grado de bachiller.

**PERÚ****Ministerio  
de Transportes  
y Comunicaciones****Secretaría General****Oficina General de  
Tecnología de la  
Información**

"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

**9. FORMA DE PAGO**

La entidad debe pagar las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendarios siguientes de otorgada la conformidad correspondiente, según lo indicado a continuación:

**a) Prestación principal**

Único pago: 100% del monto correspondiente a la prestación principal.

**b) Prestación accesoria**

- **Sobre el servicio de capacitación**

El pago se efectuará en moneda nacional, en único pago correspondiente al 100% del monto total de la capacitación.

- **Sobre el servicio de soporte técnico**

La prestación accesoria correspondiente al soporte técnico tendrá el siguiente esquema de pago:

- ✓ Entregable 1: 50% del monto total del soporte técnico.
- ✓ Entregable 2: 50% del monto total del soporte técnico.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- ✓ Informe del funcionario responsable de la Oficina de Infraestructura Tecnológica y Seguridad Informática.
- ✓ Comprobante de pago.
- ✓ Presentación de los entregables indicados en el numeral 7.1 y 7.2 según corresponda.

La documentación se debe presentar en la Oficina de Atención al Ciudadano y Gestión Documental del MTC, sito en Jr. Zorritos N° 1203 –Cercado de Lima, en el horario de 8:30 horas a 17:30 horas, o a través de Mesa de Partes Virtual del MTC, accediendo desde el siguiente link: <https://mpv.mtc.gob.pe>, siendo que los remitidos luego del horario antes indicado serán recepcionados como si hubiesen sido entregados al día siguiente hábil

**10. PENALIDADES****10.1. Penalidad por mora**

En caso de retraso injustificado en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente 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 = 0.25 para plazos mayores a sesenta (60) días o;  
F = 0.40 para plazos menores o iguales a sesenta (60) días.





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

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En ese último caso, la calificación del retraso como justificado por parte de la Entidad no da lugar al pago de gastos generales ni costos directos de ningún tipo.

## 10.2. Otras penalidades

De acuerdo con el artículo 163 del Reglamento se considerarán además las siguientes penalidades:

N°	Supuestos de aplicación de penalidad	Procedimiento	Forma de cálculo (% por valor del servicio)
01	Por no prestar el servicio de soporte técnico o atención a consultas técnicas en un tiempo máximo de cuatro (4) horas.	Tiempo empleado por el CONTRATISTA para brindar una atención que no implique un incidente con el software ofertado. El tiempo se contabiliza desde la comunicación por parte de la entidad, el mismo se acreditará con el código de avería o de registro y/o correo electrónico. La Oficina de Infraestructura Tecnológica y Seguridad Informática, emitirá un informe técnico.	1% del valor de una (01) UIT por ocurrencia.
02	Por exceder el tiempo de presentación de los entregables.	Tiempo empleado por el CONTRATISTA para realizar la presentación de los entregables correspondientes a la prestación principal y accesoria. El tiempo se contabiliza conforme a lo indicado en el ítem 7.2. La Oficina de Infraestructura Tecnológica y Seguridad Informática, emitirá un informe técnico.	1% del valor de una (01) UIT por día de retraso
03	Por exceder el tiempo de resolución de incidentes, cuyo tiempo máximo es de veinticuatro (24) horas.	Tiempo empleado por el CONTRATISTA para brindar el soporte correctivo y resolver el incidente reportado. El tiempo se contabiliza desde que genera el ticket de atención al MTC. Nota: El CONTRATISTA deberá informar mediante correo electrónico el código del ticket del incidente reportado. La Oficina de Infraestructura Tecnológica y Seguridad Informática, emitirá un informe técnico.	2% del valor de una (01) UIT por ocurrencia.
04	Por exceder el tiempo de solución a errores (bug) propio del software, cuyo tiempo máximo de resolución es setenta y dos (72) horas.	En caso que el incidente no pueda ser resuelto vía mesa de ayuda y el Contratista deba escalarlo directamente al fabricante Asimismo, deberá cumplirse para casos en donde se pierda la gestión total de la consola de administración de la solución ofertada. La Oficina de Infraestructura Tecnológica y Seguridad Informática, emitirá un informe técnico.	3% del valor de una (01) UIT por ocurrencia.

UIT: Unidad Impositiva Tributaria.

Nota: Se precisa que, para la aplicación de penalidad, el cálculo se efectuará sobre la base de la UIT vigente a la fecha de haberse producido el incumplimiento.

## 11. MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

### 11.1 ÁREA QUE COORDINARÁ CON EL CONTRATISTA

El área que coordinará con el contratista es la Oficina de Infraestructura Tecnológica y Seguridad Informática de la Oficina General de Tecnología de la Información.



PERÚ

Ministerio  
de Transportes  
y Comunicaciones

Secretaría General

Oficina General de  
Tecnología de la  
Información

"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

## 12. **CONFORMIDAD**

### 12.1. **DE LA PRESTACION PRINCIPAL:**

La conformidad será emitida por la Oficina de Infraestructura Tecnológica y Seguridad Informática, en un plazo de siete (07) días calendario previa verificación del entregable correspondiente.

### 12.2. **DE LAS PRESTACIONES ACCESORIAS:**

#### - **Sobre el servicio de soporte técnico y capacitación:**

La conformidad será emitida por la Oficina de Infraestructura Tecnológica y Seguridad Informática, en un plazo de siete (07) días calendario luego de la presentación del entregable que corresponda a lo indicado en el numeral 7.2.

## 13. **RESPONSABILIDAD POR VICIOS OCULTOS**

El CONTRATISTA es responsable por la cantidad ofrecida y por los vicios ocultos del servicio ofertados por un plazo de dos (02) años, contados a partir del día siguiente de la conformidad emitida por la Oficina de Infraestructura Tecnológica y Seguridad Informática.

## 14. **OTRAS CONDICIONES PARA LA EJECUCION DE LA PRESTACION**

### 14.1 **Subcontratación**

El contratista se encuentra en la obligación expresamente a no subcontratar y/o transferir y/o ceder y/o traspasar y/o subarrendar a terceros, total o parcialmente el servicio.

### 14.2 **Confidencialidad**

El contratista se encuentra en la obligación de mantener absoluta confidencialidad y reserva sobre cualquier información a la que tenga acceso en el cumplimiento de las obligaciones durante el periodo de contratación, en tal sentido, el contratista se compromete a no divulgar la información a la que tuvo acceso en el ejercicio de sus obligaciones.

### 14.3 **Sistema de contratación**

A suma Alzada.

## 15. **NORMAS ANTICORRUPCIÓN**

EL CONTRATISTA acepta expresamente que no llevará a cabo, acciones que están prohibidas por las leyes locales u otras leyes anti-corrupción. Sin limitar lo anterior, EL CONTRATISTA se obliga a no efectuar algún pago, ni ofrecerá o transferirá algo de valor, a un funcionario o empleado gubernamental o a cualquier tercero relacionado con el servicio aquí establecido de manera que pudiese violar las leyes locales u otras leyes anti-corrupción, sin restricción alguna.

En forma especial, EL CONTRATISTA declara con carácter de declaración jurada que no se encuentra inmerso en ningún procedimiento de carácter penal vinculado a presuntos ilícitos penales contra el Estado Peruano, constituyendo su declaración, la firma del mismo en el contrato de la que estos términos de referencia forman parte integrante.

## 16. **NORMAS ANTISOBORNO**

EL CONTRATISTA, no debe ofrecer, negociar o efectuar, cualquier pago, objeto de valor o cualquier dádiva en general, o cualquier beneficio o incentivo ilegal en





relación al contrato, que puedan constituir un incumplimiento a la ley, tales como robo, fraude, cohecho o tráfico de influencias, directa o indirectamente, o a través de socios, integrantes de los órganos de administración, apoderado, representantes legales, funcionarios, asesores o personas vinculadas.

Asimismo, el contratista se obliga a conducirse en todo momento, durante la ejecución del contrato. Con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participantes de los órganos de administración apoderados, representantes legales, funcionarios, asesores y personas vinculadas en virtud a lo establecido en el artículo 11º de la Ley de Contrataciones del Estado y el artículo 7º de su Reglamento.

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

De la misma manera, el proveedor es consciente que, de no cumplir con lo anteriormente expuesto, se someterá a la resolución del contrato y a las acciones civiles y/o penales que el MTC pueda accionar.

## 17. REQUISITOS DE CALIFICACIÓN

<b>B</b>	<b>CAPACIDAD TÉCNICA Y PROFESIONAL</b>
<b>B.3</b>	<b>CALIFICACIONES DEL PERSONAL CLAVE</b>
<b>B.3.1</b>	<b>FORMACIÓN ACADÉMICA</b>
	<p><u>Requisitos:</u>  <b>Un (01) Jefe del proyecto</b>  Profesional titulado en Ingeniería de Sistemas, o Ingeniería de Computación, o Ingeniería Electrónica, o Ingeniería Informática, o Ingeniería de Telecomunicaciones, o Ingeniería de Seguridad Informática.</p> <p><b>Dos (02) especialistas en seguridad informática:</b>  Mínimo Bachiller en Ingeniería de Sistemas, o Ingeniería de Computación, o Ingeniería Electrónica, o Ingeniería Informática, o Ingeniería de Telecomunicaciones, o Ingeniería de Seguridad Informática.</p> <p><u>Acreditación:</u>  El grado académico será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <a href="https://enlinea.sunedu.gob.pe/">https://enlinea.sunedu.gob.pe/</a> o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: <a href="https://titulosinstitutos.minedu.gob.pe/">https://titulosinstitutos.minedu.gob.pe/</a>, según corresponda.</p> <p>En caso el grado académico no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
<b>B.4</b>	<b>EXPERIENCIA DEL PERSONAL CLAVE</b>
	<p><u>Requisitos:</u>  <b>Un (01) Jefe del proyecto</b>  Con una experiencia mínima de tres (03) años como Jefe y/o Supervisor de proyectos de seguridad informática.</p> <p><b>Dos (02) especialistas en seguridad informática:</b>  Con una experiencia mínima de dos (02) años como técnico o ingeniero especialista en la implementación y/o soporte y/o técnico de soluciones de protección antimalware o soluciones de</p>



PERÚ

Ministerio  
de Transportes  
y Comunicaciones

Secretaría General

Oficina General de  
Tecnología de la  
Información

"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

	<p>protección EDR o soluciones de detección y respuesta para la protección del endpoint.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><b>Acreditación:</b> 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.</p> <div> <p><b>Importante</b></p> <ul style="list-style-type: none"> <li>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, la fecha de emisión y nombres y apellidos de quien suscribe el documento</li> <li>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.</li> <li>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</li> <li>Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.</li> </ul> </div>
<b>C</b>	<b>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</b>
	<p><b>Requisitos:</b> El postor debe acreditar un monto facturado acumulado equivalente a S/. 1,000,000.00 (un millón con 00/100 soles), por la contratación de servicios 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.</p> <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 S/ 110,000.00 (ciento diez mil con 00/100 soles) por la venta de servicios 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>Se consideran servicios similares a los siguientes: suscripción de licencias de antivirus, suscripción de licencias antimalware para endpoint y/o servidores, suscripción de licencias de soluciones antimalware para endpoint</p> <p><b>Acreditación:</b> La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, 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>1</sup>, correspondientes a un máximo</p>

<sup>1</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"  
(...)



PERÚ

Ministerio  
de Transportes  
y Comunicaciones

Secretaría General

Oficina General de  
Tecnología de la  
Información

"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

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 N° 8** referido a la Experiencia del Postor en la Especialidad

En el caso de servicios de ejecución periódica o continuada, 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 servicios 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 servicios 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

- *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.*
- *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".*

**CARLOS JOET ORTIZ ALBERCA**

**Director**

Oficina de Infraestructura Tecnológica y Seguridad Informática

*"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".*

