TÉRMINOS DE REFERENCIA
SERVICIO DE SUSCRIPCIÓN DE UN SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM) EN NUBE

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 de un servicio de suscripción de un sistema de gestión de información y eventos de seguridad (Security Information Event Management (SIEM)) en nube.

2. OBJETIVO

Realizar el almacenamiento, consolidación, correlación y finalmente el análisis de estos registros y eventos de seguridad, de manera que puedan ser explotados y permita un análisis en tiempo real, y brinde una visión rápida sobre el estado de una amenaza o vulnerabilidad en curso para poder responder de manera oportunidad a dicho evento, lo cual permitirá mejorar la seguridad a la información en el Ministerio de Transportes y Comunicaciones (MTC).

3. ANTECEDENTE

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

Se busca implementar una solución robusta que brinde un sistema de alerta temprana a través de la recolección de eventos que permitan prevenir los incidentes de ciberseguridad, los cuales de concretarse podrían dañar la imagen institucional del MTC y también la disponibilidad de los servicios digitales que se brindan a los ciudadanos.

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:

5.1. ALCANCE Y DESCRIPCIÓN DEL SERVICIO

ÍTEM	OBJETO	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA	DETALLE
1	**PRESTACIÓN PRINCIPAL**	CONTRATACIÓN DE UN SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE	1	Unidad	LICENCIA

		SEGURIDAD EN NUBE EN MODALIDAD SaaS.			
	PRESTACIÓN ACCESORIA	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 un sistema de gestión de información y eventos de seguridad en nube.
  Incluye: Activación.

- **PRESTACIÓN ACCESORIA**
  - Soporte técnico.
  - Capacitación.

5.2.1. PRESTACIÓN PRINCIPAL:

CARACTERISTICAS TÉCNICAS MÍNIMAS	
1. Aspectos Generales.	a) La solución debe consistir en una licencia de suscripción en nube que permita realizar la correlación y análisis de registros y eventos de seguridad del MTC. b) Se requiere de un SIEM en nube modalidad SaaS administrable desde una consola que brinde visibilidad sobre el rendimiento de los sistemas, servicios y los eventos de seguridad. c) El fabricante ofertante deberá disponer de un método de licenciamiento escalable tanto por número de dispositivos como por EPS asociados. d) La solución debe permitir un crecimiento de EPS, en caso se requiera, a lo largo del contrato de servicio. e) El SIEM debe estar licenciado para soportar al menos 6600 EPS de dispositivos de red y soluciones de seguridad como Firewalls, switches, routers y servidores entre otros. f) La solución estará licenciada para mantener una base de datos con eventos online de al menos treinta (30) días. g) La solución deberá brindar UEBA sea como funcionalidad nativa o a través de licenciamiento con soporte de al menos cien (100) agentes avanzados para servers Linux/Windows y cincuenta (50) agentes UEBA.[1] h) Deberá incluir (01) un colector con las siguientes características mínimas: – Deberá ser un hardware de propósito específico o virtualizado considerando incluir hardware de primer uso y el software licenciado necesario para el correcto funcionamiento de la solución. En caso se trate de componente basado en hardware, este debe cumplir con las siguientes características mínimas: – Contar mínimo con 04 interfaces RJ45 de 1GE. – Capacidad mínima para 3.5 TB. En caso se trate de colectores virtualizados, este debe cumplir con las siguientes características mínimas: – Hipervisor licenciado VMWARE vSphere ó Microsoft Hyper-V

[1] De acuerdo a la observación N° 11 del postor AB Soluciones Globales S.R.L

	– Procesador de 8 núcleos mínimo. – Memoria RAM de 16 GB mínimo. – Espacio en disco de 3.5 TB mínimo.[2]
2. Características	**2.1 <u>Análisis de seguridad en tiempo real</u>** a) El SIEM debe de disponer en tiempo real de análisis de información, mediante un procesamiento avanzados de logs y la correlación de eventos en tiempo real, que permitan apoyar tanto la operación de sistemas y servicios como la gestión de las mismas. b) Realizar un descubrimiento y categorización de dispositivos de red, servidores, usuarios y aplicaciones en profundidad, manteniendo una base de datos de configuraciones (CMDB) directamente a través del SIEM o integrándose con sistemas CMDB siempre actualizada mediante redescubrimientos programados. Los sistemas CMDB deberán ser incluidos en la propuesta del postor.[3] c) Arquitectura escalable, con capacidad de operación tanto en entornos de datacenter como cloud, con almacenaje de eventos y correlación distribuida de eventos en tiempo real. d) La solución debe soportar capacidades UEBA (User and Entity Behavior) usando Machine Learning para detectar comportamientos inusuales de usuarios y entidades evitando que el administrador escriba reglas complejas. e) La solución debe integrarse a un asistente virtual con inteligencia artificial (IA) generativa (OpenAI) o similar, que permita guiar y potenciar las acciones de los analistas de seguridad durante la investigación de incidentes, búsqueda de amenazas, respuesta y otras opciones.[4] f) Debe poseer varios modelos UEBA (User and Entity Behavior) basados en Machine Learning que detecten eventos inusuales como mínimo: ○ Detectar inicios de sesión simultáneos de dos países diferentes, ○ Detectar inicios de sesión simultáneos de dos ubicaciones geográficas improbables, ○ Anomalía de comportamiento de inicio de sesión: inicio sesión en servidores y en momentos en que normalmente no se inicia sesión, etc. ○ Detectar tráfico a dominios generados dinámicamente. Debe tener una gran cantidad de reglas de anomalías de comportamiento incorporadas que funcionen de forma inmediata pero que el usuario puede adaptar a su propio entorno. ○ Permitir que el administrador pueda escribir nuevas reglas a través de la GUI, probarlas con eventos reales y luego implementarlas en el sistema. g) Correlación de eventos SOC/NOC, para disponer en un único punto de gestión de datos no sólo de eventos de seguridad, sino también de: ○ Rendimiento y disponibilidad ○ CPU, memoria y almacenamiento. ○ Detección de cambios de configuración. ○ Monitorización de transacciones sintéticas. ○ Cuadros de mando dinámicos.

[2] De acuerdo a la observación N° 04 del postor Hynet S.A.C, N° 09 y N° 10 del postor AB Soluciones Globales S.R.L., y N° 33 del postor Enebro Ingeniería S.A.C.
[3] De acuerdo a la observación N° 12 del postor AB Soluciones Globales S.R.L.
[4] De acuerdo a la observación N° 13 del postor AB Soluciones Globales S.R.L. y consulta N° 34 del postor Enebro Ingeniería S.A.C.

	h) Actualización continua del contexto, de los dispositivos, su software y parches instalados, así como los servicios en ejecución. i) Análisis del rendimiento de aplicaciones y sistemas junto con datos del entorno para identificar rápidamente problemas de seguridad. j) Contexto de usuario, en tiempo real, con seguimiento de direcciones IP, cambios de identidad de usuario, contexto de datos de ubicación física y geo-localización. k) Detectar dispositivos, aplicaciones de red y cambios de configuración no autorizados. **2.2 Biblioteca de remediación** a) Disponibilidad de un conjunto de respuestas pre-configuradas ante eventos de seguridad, de manera que se permita no sólo la detección sino también la remediación automatizada ante determinadas amenazas. b) Posibilidad de ampliar esta biblioteca con desarrollo de scripts personalizados. **2.3 Informes de cumplimiento** a) Informes predefinidos listos para ser utilizados, que soporten una amplia gama de necesidades de auditoría y cumplimiento normativo, incluyendo: PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13 y SANS Critical Controls. b) La analítica avanzada debe permitir que los incidentes detectados se asignen a las categorías MITRE ATT&CK. De esta manera, la herramienta permitirá a los analistas de seguridad, en priorizar los incidentes según la categoría de ataque. **2.4 Supervisión del rendimiento** Debe soportar al menos cinco (05) de las supervisiones solicitadas a continuación: a) Monitor de métricas de sistema. b) Estado del sistema a través de SNMP, WMI, PowerShell. c) Estado de aplicaciones a través de JMX, WMI, PowerShell. d) Monitoreo de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster. e) Monitorización del rendimiento de aplicaciones a medida: Bases de datos - Oracle, MS SQL, MySQL a través de JDBC. f) Análisis de flujo y rendimiento de la aplicación – Netflow, SFlow, Cisco AVC e IPFIX. g) Posibilidad de agregar métricas personalizadas. h) Métricas de base y detección de desviaciones.[5] **2.5 Supervisión del cambio de configuraciones en tiempo real** a) Recopilar archivos de configuración de red, almacenados en un repositorio versionado. b) Recopilar las versiones de software instaladas, almacenadas en un repositorio versionado. c) Detección automatizada de cambios en la configuración de la red y el software instalado. d) Detección automatizada de cambios de archivos y carpetas - Windows y Linux con detalles técnicos. e) Detección automatizada de cambios desde un archivo de configuración. f) Posibilidad de detección automatizada de cambios en el registro de Windows a través de agente.

[5] De acuerdo a la observación N° 17 del postor AB Soluciones Globales S.R.L. y consulta N° 38 del postor Enebro Ingeniería S.A.C.

3	**Contexto del dispositivo y de la aplicación.**	a) Dispositivos de red incluyendo switches, routers, WLAN. b) Dispositivos de seguridad - Firewalls, IPS de red, gateways Web/Mail, protección contra malware, escáneres de vulnerabilidades. c) Servidores, incluyendo Windows, Linux, AIX. Opcionalmente HP UX.[6] d) Servicios de infraestructura incluyendo DNS, DHCP, DFS, AAA, controladores de dominio, VoIP. e) Aplicaciones orientadas al usuario, incluidos servidores Web, servidores de aplicaciones, correo, bases de datos. f) Dispositivos de almacenamiento como NetApp, EMC, Nutanix, Dell. g) Cloud Apps, incluyendo AWS, Box.com, Okta, Salesforce.com. h) Infraestructura de la nube incluyendo AWS. i) Dispositivos ambientales como UPS, HVAC, hardware del dispositivo. j) Infraestructura de virtualización incluyendo VMware ESX, Microsoft Hyper-V Scalable.
4	**Recolección de log.**	a) Recopilación, análisis, normalización, indexación y almacenamiento de logs de seguridad a velocidades que permitan una óptima operación de la solución.[7] b) Debe contar con una amplia gama de métodos de recopilación de datos basados en agentes y sin agentes para recopilar registros de una variedad de dispositivos y aplicaciones, que incluyen al menos dos (02) de las siguientes tecnologías: SNMP, Syslog, Windows Management Instrumentation (WMI) and Open Management Infrastructure (OMI), Cisco SDEE, Checkpoint LEA, JDBC, VMware SDK, JMX, Telnet, SSH, NetFlow, HTTPS, IMAP, POP, entre otros.[8] c) Soporte inmediato para una amplia variedad de sistemas de seguridad y APIs de proveedores, tanto locales como en la nube. d) La solución debe soportar agentes de Windows, que puedan proporcionar una colección de eventos altamente escalable y rica, incluida la supervisión de integridad de archivos, los cambios de software instalados y la supervisión de cambios en el registro. e) La solución debe soportar agentes de Linux para la supervisión de integridad de archivos. f) Capacidad para modificar los analizadores directamente desde la interfaz gráfica de usuario y aplicarlos en el sistema en ejecución sin pérdida de tiempo de inactividad y de evento. g) Creación de nuevos analizadores (plantillas XML) a través del entorno de desarrollo integrado y capacidad para compartir a través de la función de exportación / importación. h) Recopilación segura y fiable de eventos para usuarios y dispositivos ubicados en cualquier lugar.
5	**Notificación y gestión de incidentes.**	a) Contar con framework de notificación de incidentes basado en políticas. b) Posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico. c) Integración basada en API a sistemas externos de ticketing - ServiceNow, Salesforce, ConnectWise, Remedy y Jira.

[6] De acuerdo a la observación N° 19 del postor AB Soluciones Globales S.R.L.
[7] De acuerdo a la consulta N° 44 de postor Enebro Ingeniería S.A.C.
[8] De acuerdo a la observación N° 39 del postor AB Soluciones Globales S.R.L.

		d) Sistema incorporado de ticketing.
6	**Analítica y escalabilidad**	a) Búsqueda de eventos en real - sin necesidad de indexación. b) Búsquedas por palabras clave basadas en atributos de eventos analizados. c) Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API. d) Match de patrones complejos en tiempo real. e) Uso de objetos CMDB y datos de usuario/identidad y ubicación en búsquedas y reglas. f) Programación de informes y entregas de resultados por correo electrónico a los principales interesados. g) Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.). h) Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico. i) Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes. j) Análisis escalable mediante la adición de nodos o equivalente.[9] k) Posibilidad de priorización de los informes de incidentes.
7	**Integración de tecnología externa.**	a) Integración con cualquier sitio web externo para la búsqueda de direcciones IP. b) Integración basada en API para fuentes externas de inteligencia de amenazas. c) Integración bidireccional basada en API con sistemas de help desk – soportado para ServiceNow, ConnectWise y Remedy. d) Integración bidireccional basada en API con CMDB externas – soportado para ServiceNow, ConnectWise y Salesforce. e) Opcionalmente debe ofrecer soporte de Kafka para la integración con informes mejorados de análisis, como ELK, Tableau y Hadoop.[10] f) API o tecnología similar para una fácil integración con sistemas de aprovisionamiento. g) API o tecnología similar para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervisión. h) API o tecnología similar para integrar inteligencia externa de amenazas - Dominios de malware, IPs, URL, hashes, nodos Tor.[11] i) Integración para fuentes de inteligencia de amenazas populares - ThreatStream, SANS, Zeus, Dragos, ThreatConnect, etc. j) Tecnología para manejar grandes fuentes de información de amenazas - descarga incremental y compartición entre nodos, comparación de patrones en tiempo real con el tráfico de red. k) Compatibilidad con TAXII y STIX.
8	**Administración**	a) GUI basada en web, a ser posible HTML5. b) Control de acceso basada en roles para restringir el acceso a la GUI y a los datos.

[9] De acuerdo a la observación N° 23 del postor AB Soluciones Globales S.R.L
[10] De acuerdo a la consulta N° 24 del postor AB Soluciones Globales S.R.L
[11] De acuerdo a la observación N° 25 y N° 40 del postor AB Soluciones Globales S.R.L

	c) Todas las comunicaciones entre módulos están protegidas por HTTPS. d) Auditoría completa de la actividad del usuario. e) Fácil actualización de software con un mínimo tiempo de inactividad y pérdida de eventos. f) Actualización de la base de conocimientos (analizadores, reglas, informes) sencilla. g) Opcional archivado basado en políticas.[12] h) Hashing de registros a tiempo para no repudio y verificación de integridad. i) Autenticación de usuario flexible – local, y externa a través de Microsoft AD y OpenLDAP, Cloud SSO/SAML a través de Okta.
9 Supervisión	a) Sistema de monitorización de estado - a través de Ping, SNMP, WMI, Uptime Analysis. Opcionalmente: interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento.[13] b) Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP. c) Monitorización del hardware y del entorno.

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 cuadro N° 01 "**Características técnicas para acreditar**", en idioma español. Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado.

CUADRO N° 01 - CARACTERÍSTICAS TÉCNICAS PARA ACREDITAR

1. Características técnicas	a) Realizar un descubrimiento y categorización de dispositivos de red, servidores, usuarios y aplicaciones en profundidad, manteniendo una base de datos de configuraciones (CMDB) siempre actualizada mediante redescubrimientos programados. b) Debe poseer varios modelos UEBA (User and Entity Behavior) basados en Machine Learning que detecten eventos inusuales como mínimo: • Detectar inicios de sesión simultáneos de dos países diferentes, • Detectar inicios de sesión simultáneos de dos ubicaciones geográficas improbables. • Anomalía de comportamiento de inicio de sesión: inicio sesión en servidores y en momentos en que normalmente no se inicia sesión, etc. • Detectar tráfico a dominios generados dinámicamente. Debe tener una gran cantidad de reglas de anomalías de comportamiento incorporadas que

[12] De acuerdo a la observación N° 26 del postor AB Soluciones Globales S.R.L
[13] De acuerdo a la observación N° 27 y N° 41 del postor AB Soluciones Globales S.R.L

	funcionen de forma inmediata pero que el usuario puede adaptar a su propio entorno. • Permitir que el administrador pueda escribir nuevas reglas a través de la GUI, probarlas con eventos reales y luego implementarlas en el sistema. c) Correlación de eventos SOC/NOC, para disponer en un único punto de gestión de datos no sólo de eventos de seguridad, sino también de: • Rendimiento y disponibilidad • CPU, memoria y almacenamiento. • Detección de cambios de configuración. • Monitorización de transacciones sintéticas. • Cuadros de mando dinámicos. d) Contexto de usuario, en tiempo real, con seguimiento de direcciones IP, cambios de identidad de usuario, contexto de datos de ubicación física y geo-localización.
2. Biblioteca de remediación	a) Disponibilidad de un conjunto de respuestas pre-configuradas ante eventos de seguridad, de manera que se permita no sólo la detección sino también la remediación automatizada ante determinadas amenazas.
3. Informes de cumplimiento.	a) Informes predefinidos listos para ser utilizados, que soporten una amplia gama de necesidades de auditoría y cumplimiento normativo, incluyendo: PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13 y SANS Critical Controls. b) La analítica avanzada debe permitir que los incidentes detectados se asignen a las categorías MITRE ATT&CK. De esta manera, la herramienta permitirá a los analistas de seguridad, en priorizar los incidentes según la categoría de ataque.
4. Supervisión del rendimiento.	Debe soportar al menos cinco (05) de las supervisiones solicitadas a continuación: a) Monitor de métricas de sistema. b) Estado del sistema a través de SNMP, WMI, PowerShell. c) Estado de aplicaciones a través de JMX, WMI, PowerShell. d) Monitoreo de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster. e) Monitorización del rendimiento de aplicaciones a medida: Bases de datos - Oracle, MS SQL, MySQL a través de JDBC. f) Análisis de flujo y rendimiento de la aplicación – Netflow, SFlow, Cisco AVC e IPFIX. g) Posibilidad de agregar métricas personalizadas. h) Métricas de base y detección de desviaciones.[14]
5. Supervisión del cambio de configuraciones en tiempo real	a) Detección automatizada de cambios de archivos y carpetas - Windows y Linux con detalles técnicos.
6. Analítica y escalabilidad.	a) Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas,

[14] De acuerdo a la observación N° 17 del postor AB Soluciones Globales S.R.L. y N° 38 del postor Enebro Ingeniería S.A.C.

	agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API.
7. Integración de tecnología externa	a) Integración bidireccional basada en API con sistemas de help desk – soportado para ServiceNow, ConnectWise y Remedy. b) Integración bidireccional basada en API con CMDB externas – soportado para ServiceNow, ConnectWise y Salesforce. c) Integración para fuentes de inteligencia de amenazas populares - ThreatStream, SANS, Zeus, Dragos, ThreatConnect, etc. d) Compatibilidad con TAXII y STIX.
8. Administración	a) Autenticación de usuario flexible – local, y externa a través de Microsoft AD y OpenLDAP, Cloud SSO/SAML a través de Okta.

5.2.2. PRESTACIÓN ACCESORIA

A) SOPORTE TÉCNICO

- El contratista deberá contar con un SOC y/o NOC para los procesos de monitoreo, gestión de incidentes y gestión de cambios.
- 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 solucionados 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 del servicio estará definido de acuerdo al siguiente plazo de atención:

Tabla N° 01

N°	Nivel de atención	Plazo
01	Brindar una atención que no implique un incidente con la solución ofertada.	Hasta cuatro (04) horas.
02	Brindar el soporte correctivo y resolver incidentes reportados.	Hasta veinticuatro (24) horas.
03	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.

B) CAPACITACIÓN

- El proveedor deberá considerar una capacitación 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 seis (06) horas lectivas en modalidad virtual.
- La capacitación deberá ser realizada por un (01) especialista certificado en la solución ofertada (personal clave 8.2.1 literal b) y para tres (03) colaboradores de la Oficina de Infraestructura Tecnológica y Seguridad Informática de la Oficina General de Tecnología de la Información.
- Deberá entregar un certificado de capacitación a cada uno de los asistentes.
- El proveedor 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 cincuenta (50) días calendario, contados a partir del día siguiente de la firma del contrato, divididos de la siguiente manera:

- **Plazo de entrega de la licencia de suscripción**

  La entrega de la licencia de suscripción del servicio de gestión de eventos de seguridad en nube será realizado en un plazo no mayor a cuarenta (40) días calendario[15], contabilizado a partir del día siguiente de suscrito el contrato, y deberá ser remitido al correo electrónico 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 diez (10) días calendarios, contados a partir del día siguiente de la entrega de la licencia de suscripción.

  En el mismo día 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**

[15] De acuerdo a la observación N° 01 del participante Hynet S.A.C.

El contratista deberá remitir vía correo electrónico como mínimo a los dos (02) días siguientes a la firma del acta de instalación, el plan de capacitación (syllabus) a la casilla electrónica UsrSegurinf@mtc.gob.pe para conocimiento de los participantes del programa de capacitación.

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. En caso de no ser aprobado, el contratista deberá remitir la subsanación en un plazo no mayor a dos (02) días de notificado.

La capacitación se realizará en un plazo no mayor a siete (07) días calendario, luego de ser aprobado (plan) por la OGTI.

- **Soporte técnico**

  La prestación accesoria (soporte técnico) tendrá una vigencia de veinticuatro (24) meses, equivalentes a setecientos (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.

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 Nº 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.

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, los cuales comprenderán lo siguiente:

  a. Documento que acredite la suscripción del servicio adquirido.
  b. Documento que indique la matriz de escalamiento para reportar incidentes: Nombre del contacto técnico, correo electrónico, número de teléfono.
  c. 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:

a. 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 Nº 1203 – Cercado de Lima.

8. REQUISITOS DEL PROVEEDOR

8.1. CONDICIONES PARTICULARES

El postor debe ser representante autorizado o partner o subsidiaria o filial autorizada en el Perú, de la solución ofertada, para lo cual deberá 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.

8.2. RECURSOS A SER PROVISTOS POR EL CONTRATISTA

8.2.1 DEL PERSONAL CLAVE

a) Un (01) JEFE DE PROYECTO

i) Actividades

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

ii) Perfil

- ✓ **Experiencia:**

Con experiencia mínima de cinco (05) años como Jefe o Supervisor o Gerente en la gestión de proyectos de soluciones de infraestructura tecnológica y/o seguridad informática.

✓ **Formación académica:**

- Profesional titulado en la carrera de Ingeniería de Sistemas, o Ingeniería Informática, o Ingeniería Electrónica, o Ingeniería de Telecomunicaciones, o Ingeniería de Redes, o Ingeniería de Seguridad y Auditoría Informática, o Ingeniería Empresarial y de Sistemas.[16]

Certificaciones:

- Debe contar con certificación oficial y vigente en ITIL Foundation Certificate.
- Debe contar con certificación oficial y vigente en PMP otorgado por PMI.
- Debe contar con certificación en ISO 20000 Gestión de Servicios de TI.

Para ello deberá adjuntar copia de los certificados o diplomas correspondientes.
Las certificaciones de capacitación deberán ser presentadas a la suscripción del contrato.

b) <u>DOS (02) ESPECIALISTAS</u>

i) Actividades

Serán responsables de la instalación, configuración y capacitación de la solución de gestión de eventos ofertada.

ii) Perfil

✓ **Experiencia:**

Con experiencia mínima de cinco (05) años en implementación y/o soporte y/o mantenimiento de soluciones de gestión de eventos.

✓ **Formación académica:**

- Mínimo Bachiller en la carrera de Ingeniería de Sistemas, o Ingeniería Informática, o Ingeniería Electrónica, o Ingeniería de Telecomunicaciones, o Ingeniería de Redes, o Ingeniería de Seguridad y Auditoría Informática, o Ingeniería Empresarial y Sistemas.

Certificaciones:

- Deberán contar con una certificación técnica oficial vigente emitido por el fabricante de la solución de gestión de eventos ofertada. Para ello deberá adjuntar copia del certificado o diploma correspondiente.
- Adicionalmente deberá contar con al menos tres (03) de las siguientes certificaciones:
  - Deben contar con certificación en ISO 20000 Gestión de Servicios de TI.
  - Deben contar con certificación o constancia oficial en Ethical Hacking.

[16] De acuerdo a la consulta N° 05 del postor Hynet S.A.C.

- Deben contar con certificación en Ciberseguridad.
- Al menos un especialista deberá contar con Certificación oficial vigente en ITIL 4 fundamentos otorgado por una institución acreditada.

Nota:

- Las certificaciones y títulos deberán ser presentados como parte de la documentación para perfeccionar el contrato.
- La experiencia se contabiliza desde la obtención del grado de bachiller.

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 ofertado para la capacitación.

- **Sobre el servicio de soporte técnico**

  La prestación accesoria correspondiente al soporte técnico tendrá el siguiente esquema de pago:
  - ✓ Entregable N° 1: 50% del monto total del soporte técnico.
  - ✓ Entregable N° 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 emitiendo la conformidad.
✓ Comprobante de pago.
✓ Presentación de los entregables indicados en el numeral 7.1 y 7.2 según corresponda.

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 Nº 1203 – Cercado de Lima.

10. PENALIDADES

10.1. Penalidad por mora

En caso de retraso injustificado en la ejecución de las prestaciones objeto de la Orden, se aplicará al proveedor una penalidad por cada día del atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto de la Orden, La penalidad se aplicará automáticamente 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, a la Orden, o, en caso que estos involucraran obligaciones de ejecución periódica, a la prestación parcial 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 N° 163 del reglamento, se considerará 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 (04) horas, según numeral 1 de la Tabla N° 01.	Tiempo empleado por el CONTRATISTA para brindar una atención que no implique un incidente con la solución ofertada. 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 7.1 y 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, según numeral 2 de la Tabla N° 01.	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 de la solución ofertada cuyo tiempo máximo de resolución es setenta y dos (72) horas, según numeral 3 de la Tabla N° 01.	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.

12. CONFORMIDAD

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.

DE LAS PRESTACIONES ACCESORIAS

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 correspondiente al servicio de soporte técnico y capacitación indicado en el numeral 7.2.

13. RESPONSABILIDAD POR VICIOS OCULTOS

El CONTRATISTA es responsable por la cantidad ofrecida y por los vicios ocultos de los bienes y servicios 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

a. 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.

b. 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.

c. 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 la Orden de Servicio 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	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.4	**EXPERIENCIA DEL PERSONAL CLAVE**
	Requisitos: **Un (01) Jefe de proyecto.** Con experiencia mínima de cinco (05) años como Jefe o Supervisor o Gerente en la gestión de proyectos de soluciones de infraestructura tecnológica y/o seguridad informática. **Dos (02) Especialistas.** Con experiencia mínima de cinco (05) años en implementación y/o soporte y/o mantenimiento de soluciones de gestión de eventos. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado. 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: • *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.* • *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.* • *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.*

C	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/. 3,500,000.00 (tres millones quinientos mil con 00/100 soles) por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) 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. Se consideran similares a los siguientes: servicio de licenciamiento para el sistema de seguridad informática, o servicio de renovación de licenciamiento de software de la plataforma de seguridad, o servicio de renovación de licencia antimalware, o licenciamiento y soporte firewall, o renovación de soporte o mantenimiento de equipos de seguridad informática, o renovación de licencias de soluciones de seguridad informática, o servicio de protección, detección y respuesta extendida (XDR), o servicio de soporte de firewall de base de datos, o servicio de protección avanzada antimalware, o servicio de suscripción antimalware.[17] Acreditación: 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, 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 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**.

[17] De acuerdo a la consulta N° 29 del postor Enebro Ingeniería S.A.C.

	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 publicada 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. 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