TÉRMINOS DE REFERENCIA

NOMBRE DE LA CONTRATACIÓN

SERVICIO DE EMULACION DE ATAQUES DE PROXIMA GENERACIÓN

1. ÁREA USUARIA

Oficina de Tecnologías de la Información y Comunicaciones (OTIC) de la Superintendencia Nacional de Fiscalización Laboral (SUNAFIL).

2. FINALIDAD PÚBLICA

Garantizar la continuidad operativa y el fortalecimiento de la ciberseguridad institucional de la SUNAFIL mediante la incorporación de una plataforma de emulación de ataques de próxima generación, que permita validar de manera continua la resiliencia tecnológica, procedimental y del personal frente a amenazas reales y avanzadas, asegurando el cumplimiento normativo y la protección integral de la información. De esta manera, se potenciará la productividad institucional y se facilitará el cumplimiento de los objetivos estratégicos y operativos de SUNAFIL, mejorando el servicio de fiscalización y promoción laboral en beneficio de la ciudadanía.

3. OBJETIVOS

3.1. Objetivo General:

Contratar el servicio de emulación de ataques de próxima generación para validar integralmente la infraestructura tecnológica de la SUNAFIL, asegurando detección temprana, respuesta efectiva y mejora continua de la postura de seguridad digital.

3.2. Objetivos Específicos:

a. Ejecutar pruebas de emulación de ataques en red, endpoints y procesos de seguridad, utilizando muestras reales y scripts personalizados mapeados al MITRE ATT&CK.
b. Generar reportes detallados y trazables sobre vectores vulnerados, recomendaciones de mitigación y cumplimiento normativo.
c. Implementar mecanismos de aislamiento granular en endpoints para contener amenazas activas sin afectar la operación institucional.
d. Fortalecer las competencias del personal de ciberseguridad mediante la exposición controlada a escenarios realistas de ataque y evasión.

4. PLAN OPERATIVO INSTITUCIONAL (POI)

Meta 154: “APLICACIÓN Y SOPORTE DE TECNOLOGÍAS INFORMÁTICAS”
Actividad Operativa AOI00151000966: “Gestión de los Servicios TIC’s”

5. DESCRIPCIÓN DEL SERVICIO

ÍTEM	CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN SIGA
1	1	Servicio	Servicio emulación de ataques de próxima generación

El postor debe realizar un servicio continuo y a demanda de la entidad, considerando las siguientes características:

5.1. Características de la contratación:

Se debe brindar un servicio de utilice una plataforma para realizar pruebas de emulaciones de ataques mediante el uso de muestras reales, ataques y scripts desarrollados y manipulados para probar realmente los diferentes sistemas, procesos y personal de ciberseguridad que se tienen desplegados.

Las emulaciones deben permitir como mínimo validar los vectores de red, endpoint y ejecución.

La plataforma debe permitir la emulación de 1 agente concurrente y cumplir con las siguientes características:

FUNCIONALIDAD	DESCRIPCIÓN
Tipo de licenciamiento	• La solución deberá contar con licenciamiento digital (no físico) y acceso a portal o consola web.
Muestras	• La solución debe incluir una biblioteca extensa de artefactos de amenazas, tanto conocidos como desconocidos, para replicar escenarios y pruebas de seguridad reales. • La solución debe ser capaz de emular ataques utilizando muestras de malware ofuscadas con técnicas listadas en MITRE, evaluando la capacidad de las soluciones de seguridad para detectar y responder a amenazas que utilizan técnicas avanzadas de evasión • La solución debe permitir la descarga segura de muestras de malware de la libreria, facilitando el análisis detallado y la investigación por parte de los equipos de seguridad. • Muestras Mapeadas al framework MITRE ATT&CK: La solución debe utilizar muestras de amenazas que estén mapeadas al marco de referencia MITRE ATT&CK resaltando las técnicas y subtecnicas de cada muestra, asegurando que las emulaciones cubran una amplia gama de técnicas y tácticas empleadas por atacantes en el mundo real. • La solución debe mostrar las actividades de comportamiento de las muestras, clasificándolas como maliciosas, sospechosas e informativas. Esto debe incluir detalles específicos de las acciones realizadas por las muestras durante las emulaciones. • La solución debe permitir la carga manual de muestras, así como la carga automatizada a través de API. Debe proporcionar opciones para la eliminación segura de las muestras, permitiendo una mayor

	personalización y gestión de la librería de muestras. • La solución debe permitir la adición de acciones de resolución de endpoint y de callback para las muestras nuevas cargadas. Esto proporcionará una mayor capacidad de personalización y control sobre las emulaciones de amenazas. • La solución debe proporcionar un enlace directo a VirusTotal o sitio similar de análisis de malware para cada muestra de amenaza utilizada en las emulaciones, permitiendo una verificación rápida y un análisis adicional de la muestra. • La solución garantizar que las muestras puedan atravesar el vector de red sin ser detectadas utilizando un método de cifrado propietario. Esto asegura que las pruebas de emulación puedan incluir muestras realistas en escenarios controlados sin comprometer la seguridad de la red.
Agente	• El agente debe permitir un despliegue sencillo y automatizado en los Endpoint para ejecutar emulaciones de amenazas sin interrumpir la operación normal de los dispositivos. • El agente debe ejecutar emulaciones en modo desatendido, sin la necesidad de intervención humana, garantizando que las pruebas se realicen de manera segura y sin afectar el rendimiento del Endpoint. • El agente debe ser compatible con múltiples sistemas operativos, incluidos Windows y Linux, para asegurar la cobertura de toda la infraestructura de la organización. • El agente debe estar diseñado para consumir una cantidad mínima de recursos del sistema en los endpoints donde está instalado, garantizando un impacto mínimo en el rendimiento. • El agente debe permitir el monitoreo en tiempo real de las actividades realizadas durante las emulaciones, proporcionando visibilidad instantánea de cualquier comportamiento sospechoso o malicioso. • El agente debe generar logs detallados de todas las actividades de emulación en los endpoints, proporcionando un historial completo para auditoría y análisis posterior. • El agente debe tener la capacidad de aislar completamente un endpoint de la red en tiempo real, bloqueando todas las comunicaciones entrantes y salientes para contener amenazas activas sin afectar otros sistemas. • El módulo de aislamiento del agente debe garantizar que todas las conexiones externas hacia servidores de comando y control (C2) y otras direcciones sospechosas sean bloqueadas inmediatamente durante una emulación o incidente de seguridad. • El agente debe permitir la contención rápida y efectiva de amenazas en endpoints aislados, asegurando que no se propaguen a otras partes de la red. • El módulo de aislamiento del agente debe ofrecer opciones de aislamiento granular, permitiendo al administrador definir qué tipos de comunicaciones permitir, como tráfico de red, acceso a recursos

	compartidos, o comunicaciones específicas con direcciones IP seleccionadas. • El agente debe monitorizar el comportamiento del endpoint mientras está en aislamiento, recopilando datos sobre cualquier comunicación de las emulaciones. • El módulo de aislamiento del agente debe generar notificaciones en tiempo real para alertar al equipo de seguridad cuando un endpoint es aislado y cuando el aislamiento no se encuentre activo. • El agente debe poder ejecutar el aislamiento de forma automatizada, siguiendo políticas predefinidas que determinen cuándo y cómo un endpoint debe ser aislado en caso de detección de una amenaza.
Plataforma	• La plataforma debe permitir la programación de emulaciones, facilitando que las pruebas de seguridad se ejecuten automáticamente en momentos específicos para una validación continua. • La plataforma debe soportar la ejecución repetida de emulaciones (ilimitadas), garantizando que las defensas se validen de manera continua. • La plataforma debe proporcionar análisis detallados de los resultados de cada emulación, incluyendo vectores vulnerados y recomendaciones de mitigación. • La plataforma debe vincular las muestras de amenazas con la matriz de MITRE ATT&CK, proporcionando a los equipos de seguridad una referencia clara sobre tácticas y técnicas utilizadas por atacantes. • La plataforma debe proporcionar una biblioteca extensiva de artefactos de amenazas, permitiendo personalizar y modificar las pruebas según las necesidades de seguridad y permitiendo que los usuarios puedan cargar sus propias muestras. • La plataforma debe ofrecer un tablero que permite visualizar el estado general de las emulaciones, resultados recientes, y la seguridad general de la organización en tiempo real. • La plataforma debe proporcionar un historial completo de las emulaciones realizadas, asegurando la trazabilidad para auditorías o análisis forense. • La plataforma debe soportar la ejecución simultánea de múltiples emulaciones en diferentes endpoints (concurrentes), optimizando la validación en infraestructuras grandes. • La plataforma debe soportar la emulación de ataques avanzados y persistentes (APT) por medio de muestras Custom o scripts, proporcionando un entorno de prueba realista para amenazas sofisticadas. • La plataforma debe permitir la emulación de ataques multivectoriales, probando simultáneamente varias tácticas utilizadas por los atacantes para comprometer un sistema. • La plataforma debe soportar la validación de entornos tanto en la nube como on-premises, permitiendo una evaluación integral de

	toda la infraestructura de TI. • La plataforma debe proporcionar análisis comparativos entre emulaciones, permitiendo evaluar mejoras o retrocesos en la postura de seguridad a lo largo del tiempo. • La plataforma debe generar automáticamente reportes detallados que pueden utilizarse para demostrar cumplimiento con normativas y estándares de seguridad. • La plataforma debe permitir la gestión de 2FA para mayor seguridad compatible con la mayoría de los proveedores.
Amenazas Personalizadas	• La plataforma debe permitir la creación y ejecución de amenazas personalizadas mediante la carga de scripts en varios lenguajes, como Python, PowerShell, Bash, Perl, ruby como mínimo. • La plataforma debe permitir combinar scripts personalizados con artefactos preexistentes de la biblioteca para crear emulaciones más complejas y adaptadas a las necesidades específicas. • La plataforma debe soportar la carga automatizada de scripts personalizados a través de la API, permitiendo la integración de amenazas creadas por otros sistemas o herramientas. • La plataforma debe permitir que los scripts personalizados se ejecuten en varios sistemas operativos, como Windows y Linux, asegurando que las pruebas se adapten a diferentes entornos. • La plataforma debe permitir que las amenazas personalizadas se ejecuten bajo demanda, lo que otorga flexibilidad para realizar pruebas cuando sea necesario sin depender de horarios predefinidos. • La plataforma debe soportar la creación de amenazas que utilizan técnicas de evasión, permitiendo a los equipos de seguridad probar la capacidad de detección de las soluciones implementadas. • La plataforma debe permitir la carga y ejecución de scripts obfuscados, asegurando que las pruebas reflejen técnicas reales de ataque utilizadas para evitar la detección. • La plataforma debe proporcionar registros detallados de la ejecución de los scripts personalizados, incluyendo resultados y cualquier acción tomada por los sistemas de seguridad. • La plataforma debe soportar la importación de scripts desde repositorios externos, facilitando la creación rápida de nuevas amenazas basadas en ejemplos existentes por medido de API.
IOCs	• La plataforma debe permitir enviar automáticamente IOCs a través del agente, asegurando la ejecución de tareas de monitoreo críticas para la validación de IOCs. • La plataforma debe proporcionar un reporte detallado de los resultados, indicando los EventID específicos que deben ser monitoreados para cada comando de Sysmon ejecutado, facilitando la correlación de eventos. • La plataforma debe generar un reporte automatizado sobre si los IOCs fueron ejecutados correctamente, permitiendo a los equipos de seguridad verificar la integridad del proceso. • Configuración Personalizable de Comandos Sysmon: La plataforma debe permitir personalizar la configuración de los IOCs que se

	ejecutan, adaptándose a las necesidades específicas de cada entorno de seguridad. • La plataforma debe proporcionar reportes detallados de la validación de IOCs, especificando qué comandos fallaron o se ejecutaron correctamente y los event IDs asociados. • La plataforma debe permitir ejecutar los IOCs en múltiples endpoints de manera simultánea, asegurando una cobertura completa de la infraestructura en términos de validación de IOCs. • La plataforma debe proporcionar un registro histórico de los resultados de las validaciones de IOCs, permitiendo auditorías posteriores y revisiones en profundidad.
Aislamiento del agente	• Se debe garantizar que todas las comunicaciones no autorizadas a través de la red sean bloqueadas a nivel de kernel para máxima seguridad. • Se debe permitir únicamente la comunicación con la plataforma y terceros especificados, como soluciones EDR y SIEM, asegurando control total sobre las conexiones. • El aislamiento debe funcionar exclusivamente con IPv4, debiendo desactivarse IPv6 para evitar posibles vulnerabilidades. • El módulo de aislamiento se debe ejecutar por separado del proceso principal, lo que protege el aislamiento contra intentos de manipulación. • El aislamiento debe permanecer activo incluso si el proceso del agente es terminado, garantizando protección continua del endpoint. • Se deben utilizar ganchos a nivel de kernel para interceptar tráfico de red no autorizado antes de que llegue a su destino. • Debe ser capaz de detener cualquier intento de movimiento lateral dentro de la red desde el endpoint comprometido, mitigando propagación de ataques. • Debe ser capaz de crear una lista blanca de IPs específicas que pueden comunicarse con el agente, ofreciendo mayor flexibilidad en entornos controlados. • Si el aislamiento es interrumpido por cualquier razón, este debe ser capaz de reiniciarse automáticamente para mantener el endpoint protegido. • El aislamiento del agente debe estar disponible como mínimo para sistemas Windows, optimizando su funcionamiento para este entorno. • Durante las pruebas, se deben crean entornos de emulación aislados, asegurando que no se afecten sistemas de producción. • El agente debe prevenir la ejecución de emulaciones en entornos no virtualizados, evitando posibles riesgos en sistemas de producción. • Las emulaciones deben respetar las reglas de aislamiento, con configuraciones que van desde pruebas de red hasta ejecución completa, protegiendo siempre el entorno.

5.2. Prestaciones accesorias a la prestación principal:

5.2.1. Mantenimiento preventivo y/o correctivo:

El contratista deberá realizar el mantenimiento de la solución parte del servicio que incluye:

- **Frecuencia definida**: Programar mantenimientos mensuales para asegurar la continuidad del servicio.
- **Actualizaciones de plataforma**: Inclusión de parches de seguridad, actualización de librerías de muestras y scripts, y compatibilidad con nuevas versiones de sistemas operativos en caso aplique.
- **Verificación de agentes**: Revisión de despliegue, consumo de recursos y funcionamiento de aislamiento en endpoints.
- **Pruebas de validación**: Ejecución de emulaciones controladas para confirmar que la plataforma mantiene su capacidad de detección y respuesta.
- **Documentación**: Reportes de mantenimiento con trazabilidad y evidencia de las acciones realizadas.
- **Gestión de fallas**: Corrección de errores en agentes, módulos de aislamiento o ejecución de scripts.
- **Reemplazo/ajuste de componentes**: Sustitución de librerías dañadas, restauración de configuraciones y recuperación de servicios afectados.
- **Registro de incidencias**: Bitácora detallada de problemas, acciones correctivas y resultados.
- **Informe**: El contratista deberá entregar un informe mensual que consolide todas las acciones preventivas y correctivas realizadas, incluyendo lecciones aprendidas y recomendaciones para el siguiente ciclo.

5.2.2. Soporte técnico:

El contratista deberá brindar soporte técnico durante la vigencia del contrato, que incluye

- **Modalidad**: Remoto (24x7) y presencial cuando sea requerido.
- **SLA**: Tiempo máximo de respuesta: 4 horas para incidentes críticos y 8 horas para incidentes no críticos; tiempo máximo de resolución: 24 horas para incidentes críticos y 72 horas para incidentes no críticos.
- **Alcance**: Atención de consultas, requerimientos y problemas relacionados con la solución parte del servicio principal.
- **Lugar de soporte presencial**: Instalaciones de la SUNAFIL, Av. Salaverry 655, Jesús María, Lima.
- **Personal de soporte**: El personal asignado debe cumplir con los requisitos establecidos en el numeral 5.4.2.
- **Informe**: El contratista deberá entregar un informe mensual consolidado de todas las atenciones realizadas, clasificadas por tipo de requerimiento y nivel de soporte.

5.2.3. Capacitación y/o entrenamiento:

No aplica

5.2.4. Otras prestaciones accesorias:

No aplica

5.3. Plan de trabajo:

El contratista deberá ejecutar el servicio de acuerdo al siguiente plan de trabajo:

FASE 1: IMPLEMENTACIÓN (Días 1 al 15)

N°	ACTIVIDAD	PLAZO	ENTREGABLE
1	Reunión de inicio y levantamiento de información de la infraestructura actual	Día 1-2	Acta de Reunión de inicio
2	Aprovisionamiento y configuración de la plataforma de emulación (cloud/SaaS + agentes en endpoints)	Día 2-5	Informe final de implementación
3	Instalación y despliegue de agentes en endpoints seleccionados (Windows/Linux)	Día 5-8	Informe final de implementación
4	Configuración de librerías de muestras y scripts personalizados mapeados al MITRE ATT&CK	Día 8-11	Informe final de implementación
5	Integración con soluciones de seguridad existentes (EDR, Firewall u otro componente como SIEM según indique la Entidad)	Día 11-13	Informe final de implementación
6	Pruebas de funcionamiento, validación de emulaciones y aislamiento de endpoints	Día 13-15	Acta de final de implementación

FASE 2: MANTENIMIENTO (Mes 1 al Mes 36)

N°	ACTIVIDAD	FRECUENCIA	ENTREGABLE
1	Mantenimiento preventivo (actualizaciones, verificación de agentes, pruebas de validación)	Mensual	Informe definido en el 5.2.1
2	Mantenimiento correctivo (gestión de incidencias, ajustes de componentes, recuperación de servicios)	Según ocurrencia, informar en su informe mensual.	Informe definido en el 5.2.1
3	Soporte técnico (consultas, requerimientos, asistencia operativa)	24x7 remoto / presencial según necesidad	Informe definido en el 5.2.2

5.4. Requisitos del proveedor y/o personal:

5.4.1. Requisitos del proveedor:

- Persona natural o jurídica con RUC activo y habido.
- Experiencia mínima de un (05) años en servicios de ciberseguridad para simulación de ataque.

5.4.2. Requisitos del personal:

El contratista deberá asignar al menos un (01) profesional responsable de la implementación y soporte del servicio, que cumpla con el siguiente perfil:

PERFIL	DESCRIPCIÓN
FORMACIÓN ACADÉMICA	Título profesional universitario o Bachiller en Ingeniería de Sistemas, Informática, Software, Computación o afines.
EXPERIENCIA	Experiencia mínima de dos (02) años en: - Gestión de plataformas de ciberseguridad (EDR, SIEM, IDS/IPS). - Implementación de soluciones de simulación de ataques o pruebas de penetración.
CAPACITACIÓN Y/O CERTIFICACIONES	Ciberseguridad (al menos una): - CEH (Certified Ethical Hacker) - OSCP (Offensive Security Certified Professional) - CompTIA Security+ - MITRE ATT&CK Defender (MAD) - Capacitación formal en simulación de ataques o pruebas de penetración (mínimo 40 horas)
FUNCIONES	- Liderar la implementación de la plataforma de emulación de ataques. - Configurar librerías y scripts mapeados al MITRE ATT&CK. - Ejecutar pruebas de validación y mantenimiento. - Atender incidentes y requerimientos de soporte técnico. - Elaborar informes mensuales del servicio. - Coordinar con la OTIC y áreas responsables las actividades del servicio.

Nota: El contratista deberá presentar el CV documentado del personal propuesto, adjuntando los documentos que acrediten el cumplimiento de los requisitos de formación académica, experiencia y capacitaciones/certificaciones. La Entidad se reserva el derecho de verificar la documentación presentada.

5.5. Normas obligatorias y/o voluntarias:

- Ley N° 32069, Ley General de Contrataciones Públicas y su Reglamento aprobado mediante Decreto Supremo N° 009-2025-EF.
- Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento.

- Norma Técnica Peruana NTP-ISO/IEC 27001: Sistemas de Gestión de Seguridad de la Información (referencial).
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición".

6. MODALIDAD DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en de forma periódica en cuotas mensuales, cuyo porcentaje de pago serán en partes iguales en función al monto del contrato

7. PLAZO DE PRESTACIÓN

Plazo de ejecución:

El servicio tendrá una duración de 1095 días calendarios (equivalente a 03 años), computados a partir del día siguiente de firmado el Acta de Inicio.

Plazo de implementación:

El plazo para la ejecución de la implementación del proyecto, será de hasta quince (15) días calendarios contados desde el día siguiente de la firma del contrato y/u orden de servicio, donde al término de la implementación se firmará el Acta de Inicio

Entregable de implementación:

De hasta cinco (05) días calendarios para presentar el entregable final de implementación; contados desde el día siguiente de finalizado la implementación del proyecto.

7.1. Entregables:

N°	ENTREGABLE	PLAZO
7.1.1.	Informe final de implementación, incluyendo acta final de implementación, configuraciones y pruebas de operatividad (actividades en general definidos en el plan de trabajo).	Hasta los quince (15) días calendarios contados desde el día siguiente de la firma del contrato y/u orden de servicio
7.1.2.	Informes Mensuales del Servicio (36 informes): Correspondiente al soporte y mantenimientos definidos en el numeral 5.2.1 y 5.2.2	Dentro de los diez (10) primeros días calendario del siguiente periodo de la prestación de servicio en ejecución

8. LUGAR DE LA PRESTACIÓN

En la Sede Central de la SUNAFIL, ubicada en Av. Salaverry 655 - 4to. Piso, Jesús María, Lima, adecuándose a los horarios requeridos y ambientes establecidos por la entidad.

9. GASTOS POR DESPLAZAMIENTO

Los gastos por desplazamiento del personal del contratista para atención presencial en las instalaciones de la SUNAFIL serán asumidos por el contratista.

10. CONFORMIDAD DE SERVICIO

Conformidad del Servicio de Implementación:

La conformidad será emitida por la Oficina de Tecnologías de la Información y Comunicaciones, dentro de un plazo máximo de siete (07) días calendarios de producida la recepción de los entregables finales de la Implementación del Servicio. (Ver 7.1.1).

Conformidad de la Prestación del Servicio:

La conformidad será emitida por la Oficina de Tecnologías de la Información y Comunicaciones, dentro de un plazo máximo de siete (07) días calendarios de producida la recepción de los informes mensuales emitidos por el Contratista. (Ver 7.1.2).

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF.

De existir observaciones, la Entidad las comunica al contratista, indicando claramente el sentido de estas, otorgándole un plazo para subsanar de cinco (05) días hábiles. Si pese al plazo otorgado, el contratista no cumpliese a cabalidad con la subsanación, la Entidad puede otorgar al contratista periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso la Entidad no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

11. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en de **forma periódica en cuotas mensuales**, cuyo porcentaje de pago serán en partes iguales en función al monto del contrato y/u orden de servicio, previa conformidad de la Oficina de Tecnologías de la Información y Comunicaciones, para lo cual el contratista presentará

mensualmente un informe del servicio integral dentro de los diez (10) primeros días calendario del siguiente periodo de la prestación de servicio en ejecución.

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 Tecnologías de la Información y Comunicaciones emitiendo la conformidad de la prestación efectuada, previa entrega, por parte del contratista, de un informe mensual del servicio integral, el cual debe ser entregado dentro de los diez (10) primero días calendarios del siguiente periodo de la prestación de servicio en ejecución.
- Comprobante de pago.
- Entregables de acuerdo al detalle señalado en el numeral 6.1.2 de los términos de referencia.

Los documentos se entregarán en mesa de partes virtual de SUNAFIL sito en URL https://aplicativosweb6.sunafil.gob.pe/si.mesaVirtual/ o Mesa de Partes Presencia ubicada en Av. Salaverry 655 – 4to piso, Jesús María, Lima, en el horario de 8:3 am a 16:30 horas. Asimismo, los entregables serán necesarios para la conformidad técnica.

12. FÓRMULA DE REAJUSTE

No aplica fórmula de reajuste para el presente servicio.

13. PENALIDADES APLICABLES

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, de conformidad con el artículo 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF:

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

Donde F = 0.40

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato, componente o ítem que debió ejecutarse o, en caso de que estos involucren entregables cuantificables en monto y plazo, al monto y plazo del entregable que fuera materia de retraso.

El monto máximo de la penalidad aplicable no puede exceder el diez por ciento (10%) del monto total contratado. La Entidad tiene el derecho a exigir, además de la penalidad, el cumplimiento de la obligación.

OTRAS PENALIDADES:

La entidad aplicará penalidades por incumplimiento en la presentación tardía de los entregables del servicio y demora en solución de averías, de acuerdo al siguiente detalle

N°	Supuestos de aplicación de penalidad	Penalidad	Procedimiento
1	Por demora en la presentación de los entregables mensuales, de acuerdo a los plazos establecidos en los términos de referencia.	1% UIT por cada día de retraso	Informe técnico de la OTIC.
2	Tiempo de resolución de una avería muy crítica	0.3% UIT por cada hora de retraso	Informe técnico de la OTIC.
3	Tiempo de resolución de una avería critica	0.2% UIT por cada hora de retraso	Informe técnico de la OTIC.
4	Tiempo de resolución de una incidencia o requerimiento normal	0.1% UIT por cada hora de retraso	Informe técnico de la OTIC.

La suma de la aplicación de las penalidades por mora y otras penalidades no debe exceder el 10% del monto vigente del contrato.

14. CONFIDENCIALIDAD

El contratista deberá guardar confidencialidad sobre los aspectos relacionados a la prestación, no encontrándose autorizado por la Entidad para la divulgación de información. Las obras, creaciones intelectuales, científicas, entre otros, que se hayan realizado en el cumplimiento de las obligaciones del presente contrato, son de propiedad de la Entidad.

En cualquier caso, los derechos de autor y demás derechos de cualquier naturaleza sobre cualquier material producido bajo las estipulaciones del presente contrato son cedidos a la Entidad en forma exclusiva.

El contratista no podrá divulgar, revelar, entregar o poner a disposición de terceros, dentro o fuera de la SUNAFIL, salvo autorización expresa de la Entidad, la información proporcionada por ésta para la prestación del servicio y, en general, toda información a la que tenga acceso o la que pudiera producir con ocasión del servicio que presta, durante y después de concluida la vigencia del presente contrato.

15. RESPONSABILIDAD POR VICIOS OCULTOS

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

16. PROPIEDAD INTELECTUAL

El proveedor acepta expresamente que los derechos patrimoniales de propiedad intelectual sobre los productos y documentación generados que se entreguen al amparo del presente servicio son de propiedad única y exclusiva de la SUNAFIL para todos sus efectos, por ende, no puede por ninguna razón ser usado en otros servicios y/o por cualquier otro medio de difusión toda vez que el servicio fuera adquirido por la SUNAFIL.

17. GARANTÍAS

Según el artículo 61 de la Ley N° 32069, Ley General de Contrataciones Públicas, el cumplimiento de las obligaciones de los contratistas debe ser garantizado a través de los mecanismos establecidos en la presente ley, a fin de cubrir el adelanto de pago, y el fiel cumplimiento del contrato, así como el fiel cumplimiento de las prestaciones accesorias.

18. CLÁUSULA ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción del presente contrato y/o notificación de la orden de servicio, el contratista declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la Entidad.

Asimismo, el contratista se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, el contratista se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la Entidad, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito.

Adicionalmente, el contratista se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con la Entidad.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a la Entidad el derecho de resolver total o parcialmente el contrato.

19. SOLUCIÓN DE CONTROVERSIAS

De conformidad con lo establecido en el artículo 81 de la Ley N° 32069, Ley General de Contrataciones Públicas; y en concordancia con lo previsto en el artículo 330 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF; las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante CONCILIACIÓN, como mecanismo de la solución de controversias. Cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente.

20. RESOLUCIÓN DE CONTRATO POR INCUMPLIMIENTO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas; esto es:

- Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
- Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
- Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
- Por incumplimiento de la cláusula anticorrupción.
- Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
- Configuración de la condición de terminación anticipada establecida en el contrato, de acuerdo con los supuestos que se establezcan en el reglamento para su aplicación.

De encontrarse en alguno de los supuestos de resolución del contrato, las partes proceden de acuerdo con lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

21. CLÁUSULA DE CUMPLIMIENTO

Son causales de resolución de contrato la presentación de información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de Prevención y Mitigación del Conflicto de intereses en el acceso y salida de personal del servicio público - Ley 31564. Asimismo, en caso se incumpla con los impedimentos

señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

22. GESTIÓN DE RIESGOS

Las partes realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

23. SANCIONES

El Tribunal de Contrataciones Públicas sanciona a los participantes, postores, proveedores, y subcontratistas, cuando incurran en las infracciones señaladas en el párrafo 87.1 del artículo 87 de la Ley N° 32069, Ley General de Contrataciones Públicas, sin perjuicio de las responsabilidades civiles o penales a que hubiera lugar.

Las sanciones por imponer pueden ser:

a) Multa.

b) Inhabilitación temporal.

c) Inhabilitación permanente.

La multa o inhabilitación que se impongan no eximen de la obligación de cumplir con los contratos ya perfeccionados a la fecha en que la sanción queda firme.

24. ANEXOS

No aplica

Víctor Freddy Espinoza Córdova

Firmado digitalmente por Víctor Freddy Espinoza Córdova
Fecha: 2026.05.11 11:20:00 -05'00'