



Ministerio
de Transportes
y Comunicaciones

Viceministerio
de Transportes

Proviás Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

TÉRMINOS DE REFERENCIA

"SERVICIO DE IMPLEMENTACIÓN Y FORTALECIMIENTO DE LA SEGURIDAD TECNOLÓGICA DE PROVIAS NACIONAL"

1. ÁREA USUARIA QUE REQUIERE EL SERVICIO

Área de Infraestructura Tecnológica y Seguridad Informática de la Oficina de Tecnologías de la Información de PROVIAS NACIONAL

2. DENOMINACION DE LA CONTRATACIÓN

SERVICIO DE IMPLEMENTACIÓN Y FORTALECIMIENTO DE LA SEGURIDAD TECNOLÓGICA DE PROVIAS NACIONAL

3. OBJETO DE LA CONTRATACION

Contratar un servicio especializado para afianzar la gestión de la seguridad de las Tecnologías de la Información en Proviás Nacional, con el propósito de asegurar la confidencialidad, integridad y disponibilidad de los activos de información institucionales. El servicio incluirá la mejora de controles orientados a la prevención, detección y respuesta ante incidentes de Ciberseguridad, así como el establecimiento de mecanismos de monitoreo continuo y optimización de las medidas de protección en la infraestructura tecnológica.

4. FINALIDAD PÚBLICA

Afianzar el Programa de Seguridad de Tecnologías de la Información de Proviás Nacional, con el fin de resguardar la confidencialidad, integridad y disponibilidad de la información institucional. Esta intervención permitirá implementar controles y medidas de seguridad en plataformas y servidores tecnológicos, contribuyendo a la mejora de la gestión institucional, la continuidad de las operaciones y la protección de los procesos administrativos y técnicos asociados a la infraestructura vial nacional.

Meta POI: 1147 – 0047173 | GESTIÓN DEL PROGRAMA

5. DESCRIPCION DEL SERVICIO

La presente contratación tiene por finalidad brindar un servicio especializado de implementación y fortalecimiento de la seguridad tecnológica de Proviás Nacional, orientado a mejorar la protección de la infraestructura tecnológica, los sistemas de información y los servicios institucionales frente a amenazas y vulnerabilidades que puedan comprometer la confidencialidad, integridad y disponibilidad de la información. Para ello, el servicio comprende la optimización de controles y soluciones de seguridad, la ejecución de actividades de monitoreo, evaluación y gestión de riesgos, la atención de incidentes de seguridad, el fortalecimiento de las plataformas tecnológicas existentes, la aplicación de buenas prácticas de Ciberseguridad, con el propósito de incrementar la resiliencia de la infraestructura tecnológica, reducir la exposición a riesgos y contribuir a garantizar la continuidad operativa de los servicios tecnológicos de la entidad.

5.1. ACTIVIDADES

Para tal efecto, el personal propuesto deberá desarrollar las siguientes actividades:

- Ser miembro de comité de selección según la necesidad del área usuaria en el ámbito de la especialización del personal propuesto.

Desarrollo de la actividad 01

- Optimizar la configuración y operación de la plataforma Wazuh para mejorar la recopilación, correlación y análisis de eventos de seguridad, incrementando la

eficiencia del monitoreo y la generación de alertas.

- Fortalecer el monitoreo continuo de eventos de seguridad mediante la incorporación de nuevas fuentes de registro y la mejora de los mecanismos de supervisión de los activos tecnológicos.
- Actualizar y optimizar las reglas de correlación existentes para mejorar la detección de amenazas, reducir falsos positivos e incrementar la precisión de las alertas generadas.
- Informe detallado de análisis de incidentes de Ciberseguridad generados en plataformas Wazuh, LUMU y XDR, incluyendo alcance, clasificación por severidad y acciones de respuesta.
- Realizar el apoyo en las operaciones de TI en sitio cuando se lo requiera, desarrollo y programación de job, así como tareas que se le designe y debe de realizar el registro de todas las actividades indicadas en los puntos anteriores.

Desarrollo de la actividad 02

- Realizar evaluaciones periódicas de vulnerabilidades sobre la infraestructura tecnológica para identificar debilidades de seguridad y riesgos que puedan afectar los servicios institucionales.
- Clasificar y priorizar las vulnerabilidades identificadas de acuerdo con su nivel de criticidad, impacto y riesgo para facilitar su atención y remediación.
- Realizar el monitoreo continuo de eventos e incidentes de seguridad para identificar oportunamente actividades sospechosas y posibles amenazas sobre la infraestructura tecnológica.
- Informe detallado de análisis de incidentes de Ciberseguridad generados en plataformas Wazuh, LUMU y XDR, incluyendo alcance, clasificación por severidad y acciones de respuesta.
- Realizar el apoyo en las operaciones de TI en sitio cuando se lo requiera, desarrollo y programación de job, así como tareas que se le designe y debe de realizar el registro de todas las actividades indicadas en los puntos anteriores.

5.2. PROCEDIMIENTOS

Para la correcta ejecución del servicio, se deberán considerar los siguientes procedimientos:

- Realizar el levantamiento de información y la revisión del estado de las plataformas de seguridad tecnológica, con la finalidad de identificar oportunidades de mejora y definir las acciones a implementar.
- Ejecutar las actividades de optimización, configuración y fortalecimiento de las plataformas de seguridad, de acuerdo con las mejores prácticas y las recomendaciones de los fabricantes.
- Realizar el monitoreo continuo de las plataformas de seguridad, analizando los eventos, alertas e incidentes detectados para su evaluación y atención oportuna.
- Ejecutar evaluaciones de vulnerabilidades sobre la infraestructura tecnológica definida por la Entidad, registrando, clasificando y priorizando los hallazgos identificados.
- Brindar apoyo técnico especializado en la atención de incidentes de Ciberseguridad, incluyendo actividades de análisis y seguimiento cuando sea requerido por la Entidad.
- Registrar las actividades ejecutadas, configuraciones realizadas, incidentes atendidos y acciones implementadas, manteniendo la documentación técnica debidamente actualizada.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Viceministerio
de Transportes

Provias Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

- Mantener estricta confidencialidad sobre la información, configuraciones, registros y demás activos tecnológicos a los que tenga acceso durante la ejecución del servicio.

5.3. RECURSOS Y FACILIDADES A SER PROVISTO POR LA ENTIDAD

- La entidad proveerá un escritorio de trabajo y equipo de cómputo en la sede central de ser necesario para el desarrollo de sus actividades.
- La entidad brindará los materiales necesarios para completar lo solicitado en los Términos de Referencia.
- Provías Nacional proporcionará correo electrónico, accesos a los sistemas administrativos necesarios para la ejecución de las actividades del servicio, un usuario y clave temporal, en tanto dure el servicio, y coordinará su retiro al finalizar el mismo.

5.4. RECURSOS Y FACILIDADES A SER PROVISTO POR PROVEEDOR

- Deberá contar con un servicio de comunicación (celular) con acceso a datos móviles, el cual deberá estar activo y disponible durante toda la vigencia del contrato.
- Deberá estar disponible para trasladarse a la oficina central cuando sea requerido, brindando apoyo en cualquier momento que se solicite.

6. PERFIL DEL POSTOR

6.1 Del Postor

Capacidad Legal:

No corresponde.

Capacidad técnica:

No corresponde.

Experiencia:

Para el caso de la experiencia del postor se considerará servicios iguales y/o similares objeto de la contratación en monto facturado mínimo de 01 vez el valor ofertado según la complejidad de la contratación.

Se consideran servicios similares: Servicios especializado de infraestructura y soluciones tecnológicas y/o servicio de soporte técnico de solución de seguridad para protección de la infraestructura tecnológica y/o servicio de implementación y robustecimiento de la seguridad tecnológica y/o servicio de mejora del programa de seguridad informática para plataformas y servidores de TI.

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 constancia 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. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados, para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.



a. Del Personal Propuesto

Capacidad Legal:

No corresponde.

Capacidad Técnica y profesional

- Título Profesional en: en ingeniería de sistemas y/o ingeniería de software y/o Ingeniería electrónica y/o ingeniería de computación y sistemas y/o ingeniería informática y/o ingeniería de telecomunicaciones y/o ingeniería de redes o licenciado sistemas de información y/o Ciencias de la computación y/o sistemas.
- Curso y/o diplomado y/o Seminario en: Fundamentos de Ciberseguridad y/o diplomado en: Administración del Datacenter y/o talleres de instalación y/o configuración y administración de sistemas operativos de red como Windows Server y/o Linux y/o Herramientas y técnicas de detección de Ciberamenazas.
- Certificación y/o talleres de redes inalámbricas o Wireless Networking y/o talleres de seguridad de redes y/o curso de capacitación FCP administrador y/o en innovación e integración tecnológica.

Nota. La capacidad técnica y profesional se acreditará mediante copia simple de la documentación correspondiente. La formación académica se acreditará con el título profesional, constancia o certificado emitido por la universidad o centro de estudios de procedencia; mientras que las capacitaciones se acreditarán con constancias o certificados de estudios, cursos y/o talleres emitidos por un centro de estudios o institución certificadora. En caso de títulos o grados académicos obtenidos en el extranjero, deberá presentarse, adicionalmente, copia simple del documento de revalidación o reconocimiento emitido por la SUNEDU, según corresponda.

Experiencia

Experiencia laboral de tres (03) años en el sector público y/o privado, brindando servicios de: Administrador de servidores y/o Analista de Ciberseguridad y/o Especialista de TI y/o Analista en infraestructura y/o redes y/o Seguridad y/o administrador de red y/o soporte técnico de redes en Entidades Públicas o Privadas en Entidades Públicas o Privadas en el área de tecnologías de la información de los cuales Dos (02) años debe ser en la gestión pública.

Nota: La experiencia del personal propuesto 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.

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

7. ENTREGABLES

N°	Entregable	Plazo de Entrega
Primer Entregable	El proveedor deberá presentar un (01) informe consolidado, el cual deberá incluir como mínimo lo siguiente: • Optimizar la configuración y operación de la plataforma Wazuh para mejorar la recopilación, correlación y análisis de eventos de seguridad, incrementando la eficiencia del monitoreo y la generación de alertas.	Hasta los (30) treinta días calendario de iniciado el Servicio.

**PERÚ****Ministerio
de Transportes
y Comunicaciones****Viceministerio
de Transportes****Provias Nacional**

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

	- Fortalecer el monitoreo continuo de eventos de seguridad mediante la incorporación de nuevas fuentes de registro y la mejora de los mecanismos de supervisión de los activos tecnológicos. - Actualizar y optimizar las reglas de correlación existentes para mejorar la detección de amenazas, reducir falsos positivos e incrementar la precisión de las alertas generadas. - Informe detallado de análisis de incidentes de Ciberseguridad generados en plataformas Wazuh, LUMU y XDR, incluyendo alcance, clasificación por severidad y acciones de respuesta. - Realizar el apoyo en las operaciones de TI en sitio cuando se lo requiera, desarrollo y programación de job, así como tareas que se le designe y debe de realizar el registro de todas las actividades indicadas en los puntos anteriores.	
Segundo Entregable	El proveedor deberá presentar un (01) informe consolidado, el cual deberá incluir como mínimo lo siguiente: - Realizar evaluaciones periódicas de vulnerabilidades sobre la infraestructura tecnológica para identificar debilidades de seguridad y riesgos que puedan afectar los servicios institucionales. - Clasificar y priorizar las vulnerabilidades identificadas de acuerdo con su nivel de criticidad, impacto y riesgo para facilitar su atención y remediación. - Realizar el monitoreo continuo de eventos e incidentes de seguridad para identificar oportunamente actividades sospechosas y posibles amenazas sobre la infraestructura tecnológica. - Informe detallado de análisis de incidentes de Ciberseguridad generados en plataformas Wazuh, LUMU y XDR, incluyendo alcance, clasificación por severidad y acciones de respuesta. - Realizar el apoyo en las operaciones de TI en sitio cuando se lo requiera, desarrollo y programación de job, así como tareas que se le designe y debe de realizar el registro de todas las actividades indicadas en los puntos anteriores.	Hasta los (60) sesenta días calendario de iniciado el Servicio.

8. PLAZO DE EJECUCIÓN DEL SERVICIO

El Plazo de desarrollo del servicio es de hasta sesenta (60) días calendarios, el cual inicia desde el día siguiente de confirmada la orden de servicio y culmina con la emisión de la conformidad de la última prestación.

De corresponder, se debe adjuntar la Declaración Jurada de Intereses, oportunidad Inicio/Cese.

9. LUGAR DE EJECUCIÓN DEL SERVICIO

El servicio se ejecutará en la Oficina de Tecnologías de la Información de Provias Nacional ubicado en Jr. Zorritos 1203 Cercado de Lima.



10. CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad del servicio será emitida dentro de un plazo que no excederá de siete (07) días calendario de recibido el entregable por el área de Infraestructura Tecnológica y Seguridad Informática de la Oficina de Tecnologías de la Información.

El Responsable del Área Usuaria que solicita la prestación deberá emitir la conformidad del servicio. En caso de requerir la evaluación técnica previa, deberá adjuntar copia de dicho informe.

11. MODALIDAD DE PAGO

Suma Alzada

12. FORMA DE PAGO Y PENALIDAD

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

Entregable	Porcentaje	Plazo de entrega
01	50 %	El procedimiento de pago se ejecutará dentro del plazo de Diez (10) días hábiles siguientes de otorgada la conformidad del primer entregable.
02	50 %	El procedimiento de pago se ejecutará dentro del plazo de Diez (10) días hábiles siguientes de otorgada la conformidad del segundo entregable

Se debe precisar que el pago se efectuará después de realizada la prestación y otorgada la conformidad, dentro del plazo de diez (10) días hábiles de otorgada la conformidad de la prestación.

La penalidad por mora se aplica conforme a lo establecido en la Ley y su Reglamento.

En caso de retraso injustificado del Contratista en la ejecución de las prestaciones objeto del contrato, PROVIAS NACIONAL le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

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

Donde F tiene los siguientes valores:

- Para bienes y servicios: $F = 0.40$

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato, componente o ítem que debió ejecutarse o, en caso que estos involucren entregables cuantificables en monto y plazo del entregable que fuera materia de retraso. En el caso de consultoría que contenga más de un componente el monto y plazo corresponde al componente que se ejecuta. En caso no sea posible cuantificar el monto de la prestación materia de retraso, la Entidad puede establecer en los TDR la penalidad a aplicarse.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobada. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad,



Ministerio
de Transportes
y Comunicaciones

Viceministerio
de Transportes

Provías Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso, la calificación del retraso como justificado por parte de la entidad contratante no da lugar al pago de gastos generales ni costos directos de ningún tipo.

13. OTRAS PENALIDADES

No corresponde

14. DISPOSICIONES DE 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.

RIESGO	ACCIONES A REALIZAR	ASIGNACION DEL RIESGO	
		ENTIDAD	CONTRATISTA
Retraso en el plazo de prestación	Considerar plazos adecuados para la prestación	X	
Incumplimiento de obligaciones del contratista	Aplicación de penalidades		X

15. RESOLUCION DE CONTRATO

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.

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

Se podrá resolver contrato también de mutuo acuerdo o disenso, previa opinión del área usuaria.

16. CLAUSULA ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción de este contrato, 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 contratante.

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, 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 contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas



técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

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 CONTRATANTE.

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; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

17. CLAUSULA DE SOLUCIÓN DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante CONCILIACIÓN, según el acuerdo de las partes.

Cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 82 de la Ley General de Contrataciones Públicas.

18. CLÁUSULA DE GARANTÍAS

No corresponde.

19. OBLIGATORIEDAD DE PRESENTAR DECLARACIÓN JURADA DE INTERÉS

Conforme al Artículo N° 02 de la Ley N° 31227 y su reglamento aprobado con Resolución de Contraloría N° 158-2021-CG cuya presentación constituye requisito indispensable para el ejercicio del cargo o función pública y demás situaciones que regula la presente ley, me comprometo a presentar la DJI en los plazos establecidos bajo sanción establecida en la Ley y su Reglamento.

20. LEY DE PREVENCIÓN Y MITIGACIÓN DEL CONFLICTO DE INTERESES EN EL ACCESO Y SALIDA DE PERSONAL DEL SERVICIO PÚBLICO

Son causales de resolución de contrato la presentación con 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. 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.

21. OTRAS CONDICIONES ADICIONALES



PERÚ

Ministerio
de Transportes
y Comunicaciones

Viceministerio
de Transportes

Proviás Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

De presentarse hechos generadores de atraso, el contratista puede solicitar ampliación de plazo dentro de los diez (10) días hábiles siguientes de finalizado el hecho generador del atraso o paralización, solicitud debidamente sustentada y que no es subsanable.

La entidad debe resolver dicha solicitud y notificar su decisión al Prestador del Servicio en un plazo de doce (12) días hábiles, computado desde el día siguiente de su presentación.

El Prestador del Servicio deberá cumplir con la Confidencialidad y Reserva Absoluta en el manejo de información y documentación a la que tenga acceso y que se encuentre relacionada con la prestación del servicio, quedando prohibido revelar dicha información a terceros.

En tal sentido, EL CONTRATISTA deberá dar cumplimiento a todas las políticas y estándares definidos por la Entidad en materia de seguridad de la información. Dicha obligación comprende la Información que se entrega, así como la que se genera durante la ejecución de las prestaciones y la información producida una vez que se haya concluido las prestaciones.

Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos y demás documentos e información compilados o recibidos por el Contratista.

Elaborado Por
ING. DAVID RICALDI ANTARA
Especialista en Infraestructura de TI

Aprobado por
ING. JAEI ROLANDO MORALES CARAHUANCO
Jefe de Infraestructura Tecnológica y Seguridad
Informática (e)

Aprobado por
ING. MARIA ISABEL VASQUEZ ALDAVE
Jefa de la Oficina de Tecnología de la Información