

ADQUISICIÓN DE UNA DE UNA SOLUCIÓN INTEGRAL DE FORTALECIMIENTO DE LA CIBERSEGURIDAD

1. FINALIDAD PÚBLICA DE LA CONTRATACIÓN

Fortalecer la protección de la integridad, disponibilidad y confidencialidad de la información institucional y apoyar la continuidad de los servicios públicos digitales del Gobierno Regional de Ucayali. Esta finalidad se encuentra alineada con el marco nacional de seguridad digital y con la implementación de controles de seguridad de la información en entidades públicas.

2. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

El Gobierno Regional de Ucayali requiere la adquisición de una solución integral de fortalecimiento de la ciberseguridad del Centro de Datos del Gobierno Regional de Ucayali mediante diagnóstico, evaluación de riesgos y propuestas de pruebas de seguridad controladas, con la finalidad de identificar vulnerabilidades, analizar el estado situacional de la infraestructura tecnológica y proponer medidas de mejora que fortalezcan la confidencialidad, integridad y disponibilidad de la información, permitiendo además contar con informes técnicos y recomendaciones útiles para la toma de decisiones y la protección de los servicios digitales de la entidad.

3. CONDICIONES DE CONTRATACIÓN

a) MODALIDAD DE PAGO

El contrato se rige por la modalidad de pago Suma Alzada de conformidad con el artículo 130 del Reglamento.

b) FORMA DE PAGO

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.

La entidad contratante paga las contraprestaciones pactadas a favor del contratista dentro de los diez días hábiles siguientes de otorgada la conformidad por parte del área usuaria, y es prorrogable, previa justificación de la demora, por cinco días hábiles.

La entidad contratante realiza el pago de la contraprestación pactada a favor del contratista en pago único.

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

- Documento de recepción y verificación del bien.
- Documento en el que conste la conformidad de la prestación efectuada suscrita por el servidor responsable de la Oficina de Tecnologías de la Información.
- Comprobante de pago.

c) SISTEMA DE ENTREGA

NO APLICA.

d) PLAZO DE ENTREGA

La solución deberá ser entregada en un plazo máximo de treinta (30) días calendario, contados a partir del día siguiente de la notificación de la orden de compra o documento contractual correspondiente.

e) LUGAR DE ENTREGA DE LOS BIENES



Lugar: Almacén del GOREU, ubicado en Jr. Mariscal Cáceres N.º 795 – Ex Cárcel, en el horario de 8.00 AM hasta las 5.00 PM.

f) ADELANTOS

NO APLICA.

g) PENALIDADES

PENALIDAD POR MORA:

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. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{Monto de la contratación o ítem}}{F \times \text{Plazo en días}}$$

Donde F tiene los siguientes valores:

Para bienes y servicios: $F = 0.40$

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 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, conforme al numeral 120.4 del artículo 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

Las penalidades se deducen de los pagos a cuenta, pagos parciales o del pago final, según corresponda; o si fuera necesario, se cobra del monto resultante de la ejecución de la garantía de fiel cumplimiento.

Cuando se llegue a cubrir el monto máximo de la aplicación de la penalidad por mora y otras penalidades, de ser el caso, LA ENTIDAD CONTRATANTE puede resolver el contrato por incumplimiento.

OTRAS PENALIDADES:

NO APLICA.

h) SUBCONTRATACIÓN

Se encuentra prohibida la subcontratación de las prestaciones objeto del contrato.

i) FÓRMULAS DE REAJUSTES

No Aplica.

j) SOLUCIÓN DE CONTROVERSIAS CONTRACTUALES



Toda controversia que surja entre las partes sobre la validez, nulidad, interpretación, ejecución, terminación o eficacia del contrato se resuelven mediante conciliación, conforme al Artículo 81 de la ley N°32069-Ley General de Contrataciones Públicas y 330 del Decreto Supremo N°099-2025-EF-Reglamento de la Ley General de Contrataciones Públicas.

k) REQUISITOS DEL PROVEEDOR

El proveedor deberá cumplir los siguientes requisitos y acreditarlos al momento de formalizar el contrato y/o orden de compra:

- Persona jurídica y/o natural
- Registro Nacional de Proveedores-RNP, habilitado en bienes.
- Registro único de contribuyente-RUC, activo y habido.
- Declaración jurada de cumplimiento y de no estar impedido para contratar con el Estado.

Capacidad Técnica y Experiencia

El postor deberá acreditar experiencia en ventas o contrataciones vinculadas a soluciones o prestaciones iguales o similares al objeto de la convocatoria, por un monto acumulado de S/ 80,000.00 durante los tres años anteriores a la fecha de presentación de ofertas.

Se consideran bienes o contrataciones similares, entre otros, los siguientes:

Servicio de diagnóstico de ciberseguridad, análisis de riesgos, levantamiento de vulnerabilidades, pruebas de seguridad controladas, ethical hacking, evaluación de exposición de servicios web, implementación o configuración de soluciones de seguridad informática, monitoreo de infraestructura tecnológica, supervisión de servidores físicos o virtuales, gestión de alertas, control de disponibilidad de servicios críticos, así como la venta, provisión o implementación de software, equipos informáticos, herramientas tecnológicas y soluciones vinculadas a infraestructura de Tecnologías de la Información y seguridad electrónica.

Acreditación

La experiencia podrá acreditarse con copia simple de contratos, órdenes de compra, órdenes de servicio, comprobantes de pago cancelados o documentación equivalente que demuestre fehacientemente la contratación y su conformidad, de acuerdo con las reglas del procedimiento de contratación que defina la entidad. La documentación de acreditación debe guardar coherencia con el objeto efectivamente convocado.

Personal Clave

Formación Académica

Profesional Ingeniero de Sistemas Colegiado y Habilitado.

Acreditación

El título profesional requerido debe estar registrado en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria – SUNEDU a través del siguiente link:
<https://enlinea.sunedu.gob.pe/>

Capacitación

- ISO/IEC 27001 (Implementador o Auditor)

Acreditación

Se acreditará con copia simple de constancia, certificado u otros documentos según corresponda.

4. GARANTIAS

No aplica.



5. CLAUSULA ANTICORRUPCION Y ANTISOBORNO

El contratista declara no haber, directa o indirectamente, ofrecido, negociado o efectuado pago o, en general, entregado beneficio o incentivo ilegal en relación al bien a adquirirse. En línea con ello, se compromete a actuar en todo momento con integridad, a abstenerse de ofrecer, dar o prometer, regalo u objeto alguno a cambio de cualquier beneficio, percibido de manera directa o indirecta ;a cualquier miembro del consejo directivo ,funcionarios públicos ,empleados de confianza ,servidores públicos ;así como a terceros que tengan participación directa o indirecta en la determinación de las características técnicas y/o valor referencial o valor estimado, elaboración de documentos del procedimiento de selección ,calificación y evaluación de oferta, y la conformidad de los contratos derivados de dicho procedimiento.

- El contratista se compromete a denunciar, en base de una creencia razonable o de buena fe cualquier intento de soborno, supuesto o real, que tuviera conocimiento.
- Asimismo, 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, integrantes los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas.

6. 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.

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES proceden de acuerdo a 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.

7. ESPECIFICACIONES TÉCNICAS

La solución a adquirir deberá comprender como mínimo los siguientes componentes funcionales y entregables técnicos:

Componentes	Características
Diagnóstico y Configuración de WAF para Servicios Web	• Reunión de inicio con el equipo de la Oficina de Tecnologías de la Información para identificar activos críticos, servicios web expuestos y políticas de ciberseguridad existentes en el Centro de Datos. • Evaluación del estado situacional de las redes de datos y servidores físicos, identificando servicios web que requieren protección adicional complementaria al firewall perimetral existente. • Implementación de WAF (Web Application Firewall) para protección de servicios web internos expuestos (intranet, portales gubernamentales, aplicaciones web del centro de datos) contra inyecciones SQL, XSS, bots y ataques HTTP/HTTPS. • Configuración del WAF para que opere en paralelo o detrás del firewall perimetral existente, sin duplicar el bloqueo de páginas web de internet.
Monitoreo de Infraestructura Interna	• Análisis del estado de servidores, dispositivos de red y servicios del Centro de Datos que no están monitoreados actualmente. • Implementación de plataforma de monitoreo de infraestructura para disponibilidad, capacidad y rendimiento de: ○ Servidores físicos del centro de datos ○ Equipos de red (switches, routers) ○ Servicios críticos (DNS, DHCP, correo, aplicaciones) ○ El propio firewall perimetral existente (monitoreo de su estado, tráfico, alertas) • Configuración de alertas por caída de servicio, uso excesivo de recursos y eventos críticos.





	Implementación de dashboards operativos y ejecutivos con visualización en tiempo real y tendencias históricas.
Plataforma SOC para Detección y Respuesta ante Incidentes	- Análisis de riesgos para vulnerabilidades encontradas en servidores y redes internas, calculando impacto y probabilidad de ocurrencia. - Implementación de plataforma SIEM para recolección centralizada de logs de: - Firewall perimetral existente (logs de tráfico de internet, bloqueos, alertas de seguridad) - Servidores Windows/Linux del centro de datos - Equipos de red internos - Aplicaciones críticas - Configuración de correlación de eventos, detección de amenazas, monitoreo de integridad de archivos (FIM) y alertas de seguridad. - Implementación de sensor IDS/NSM para captura y análisis de tráfico de red interna (LAN), detectando intrusiones, escaneos, ataques laterales y comportamiento anómalo dentro del centro de datos. - Diseño de acciones de mejora (medidas de seguridad, políticas) para fortalecer la seguridad de la red interna y servidores, complementando las políticas ya existentes en el firewall perimetral.
Requisitos técnicos generales de la solución	- Los productos y documentos entregados deberán ser proporcionados en idioma español. - Los informes, matrices, configuraciones y demás productos deberán presentarse en formato digital editable (Word, Excel) y en PDF. - La solución deberá ser compatible e integrable con el firewall perimetral existente, sin requerir su reemplazo. - El proveedor deberá configurar el forward de logs del firewall perimetral existente hacia el SIEM. - Todas las soluciones utilizarán software libre (open source), sin costo de licenciamiento. - No se implementará firewall perimetral (función ya cubierta por el firewall existente). - Para la validación de las especificaciones técnicas, el potencial proveedor deberá adjuntar una ficha técnica del bien que compone su oferta o cotización.

8. ENTREGABLES

N°	Entregable	Descripción	Forma de presentación
1	Documento de arquitectura + Configuración de WAF	Incluye reunión de inicio, identificación de activos críticos y servicios web expuestos, mapeo de integración con firewall perimetral existente, y configuración de WAF para protección de servicios web internos (no bloqueo de páginas web)	Informe digital en PDF y archivo editable, presentado a la Oficina de Tecnologías de la Información.
2	Configuración de Monitoreo de Infraestructura	Incluye evaluación del estado de servidores y redes internas, configuración de plataforma de monitoreo para servidores, equipos de red, servicios críticos y firewall perimetral existente, con alertas y dashboards operativos	Configuración documentada en PDF y archivo editable, presentado a la Oficina de Tecnologías de la Información
3	Configuración de SOC + Manual de	Incluye configuración de SIEM con recepción de logs del firewall	Documento digital en PDF y archivo editable,

	integración + Acta de conformidad	perimetral, sensor IDS/NSM para tráfico interno, matriz de riesgos, acciones de mejora complementarias, manual de administración y procedimiento de integración, y acta que certifica implementación completa e integrada	presentado a la Oficina de Tecnologías de la Información
--	-----------------------------------	---	--

9. GARANTÍA

El proveedor deberá otorgar una garantía mínima de tres (03) meses respecto de la solución entregada y de la consistencia técnica de los productos proporcionados. Durante este periodo, el proveedor deberá atender consultas, ajustes documentarios y soporte técnico derivado directamente de las características del bien ofertado.

10. RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF. La recepción será otorgada por el área de almacén y la conformidad será otorgada por la Oficina de Tecnologías de la Información en el plazo máximo de 7 (siete) días hábiles computados desde el día siguiente de producida la recepción.

En caso de detectarse incumplimiento de las especificaciones técnicas durante la entrega, el proveedor deberá realizar la reposición del bien en un plazo máximo de (1) día hábil, contados a partir de la notificación de la Entidad, sin costo adicional. (presentar declaración jurada)

De existir observaciones, LA ENTIDAD CONTRATANTE las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar el cual no debe ser mayor al 30% del plazo del entregable correspondiente, dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. Si pese al plazo otorgado, EL CONTRATISTA no cumpliera a cabalidad con la subsanación, LA ENTIDAD CONTRATANTE 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 sin considerar los días en los que pudiera incurrir la entidad contratante para efectuar las revisiones y notificar las observaciones correspondientes.

Este procedimiento no resulta aplicable cuando los bienes manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso la entidad contratante 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. 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 las oportunidades y disminuyendo la probabilidad de las amenazas durante la ejecución contractual, considerando la finalidad pública de la contratación.

GOBIERNO REGIONAL DE UCAYALI

Ing. Leo Martín Chumbe Rodríguez
DIRECTOR DE LA OFICINA DE TECNOLOGÍAS
DE LA INFORMACIÓN

Firma y Sello

Responsable del Área Usuaria