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

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.

	• 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: o Firewall perimetral existente (logs de tráfico de internet, bloqueos, alertas de seguridad) o Servidores Windows/Linux del centro de datos o Equipos de red internos o 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,