FORMATO N° 02 – TÉRMINOS DE REFERENCIA PARA SERVICIOS EN GENERAL (CONTRATOS MENORES)

1. **ÁREA USUARIA**: **OAD - RECURSOS HUMANOS**

2. **ACTIVIDAD DEL POI/ACCIÓN ESTRATÉGICA PEI**:
   Gestión Administrativa / AEI.04.02 Programas de fortalecimiento de capacidades desarrollados para el talento humano de la UNI.

3. **CUADRO MULTIANUAL DE NECESIDADES:**

   a. Programado ( ) b. No Programado (x)

Código	Descripción
35.20.0001.7839	CURSO DE DETECCION, INTELIGENCIA Y ORQUESTACION DE EVENTOS DE CIBERSEGURIDAD CON WAZUH

Firmado digitalmente por ROMERO VILCAPOMA Patricia FAU 20514761826 soft
Motivo: Doy V° B°
Fecha: 05.07.2025 10:57:51 -05:00

4. **DENOMINACIÓN DE LA CONTRATACIÓN**):
   Curso: Detección, Inteligencia y Orquestación de eventos de ciberseguridad con Wazuh

5. **FINALIDAD PÚBLICA:**
   Contribuir a la mejora de las capacidades institucionales en materia de seguridad de la información y ciberseguridad a través del fortalecimiento de conocimientos técnicos especializados del personal responsable de la gestión de eventos e incidentes de seguridad, en el marco del cumplimiento de los lineamientos de gobierno digital, seguridad digital, protección de datos personales y continuidad del negocio, y la Política Nacional de Transformación Digital.

6. **OBJETIVO DE LA CONTRATACIÓN:**
   Contratar el servicio de capacitación especializada para el desarrollo del curso denominado: "Detección, Inteligencia y Orquestación de Eventos de Ciberseguridad con Wazuh", orientado al fortalecimiento de competencias técnicas avanzadas para diseñar, implementar y administrar arquitecturas SIEM-XDR avanzadas usando Wazuh para automatizar flujos de ingestión de datos, correlación de eventos e inteligencia de amenazas de ciberseguridad; así como en el monitoreo, correlación, automatización de respuesta y threat hunting mediante el uso e integración de herramientas open source.

7. **INDICAR SI ES ACTIVIDAD Y/O PROYECTO**

   a. Actividad (x) b. Proyecto de Investigación ( ) c. Proyecto de Inversión ( )

   En caso sea un "Proyecto de inversión", señalar el código CUI:

Firmado digitalmente por SANTILLAN RAMOS Oscar Ramiro FAU 20514761826 soft
Motivo: Doy V° B°
Fecha: 07.07.2025 14:40:42 -05:00

8. REGISTRO DE ÍTEM CUBSO:

Nro. CUBSO	Descripción del CUBSO	Descripción adicional	Cantidad	Unidad de medida	Moneda	Lugar
86101709 00385443	Curso de ciberseguridad	Orquestación y Automatización de la ciberseguridad con Wazuh	01	Servicio	soles	Región: Lima Provincia: Lima Distrito: San Borja

9. MODALIDADES DE PAGO:

a. Suma alzada (X) b. Precios unitarios ( ) c. Esquema mixto ( ) d. Tarifas ( )
e. En base a porcentajes ( ) f. En base a un honorario fijo y una comisión ( )
g. Pago por consumo ( )

10. DESCRIPCIÓN DEL SERVICIO:

10.1 Alcances del Servicio:

- Nivel: Avanzado
- Cantidad de participantes: 03 servidores civiles del INICTEL-UNI
- Modalidad: Virtual; clase en vivo en la plataforma virtual proporcionada por el contratista.
- Duración: 40 horas académicas
- Inicio: A coordinar
- Horario: a coordinar
- Temario: basado en la última versión disponible de Wazuh.

Módulo 1: Arquitectura y Fundamentos Avanzados de Wazuh
Sesión 1 – Diseño de arquitecturas XDR con Wazuh
- Repaso profundo de arquitectura distribuida Wazuh
- Escalabilidad, HA, multicliente
- Pipeline de eventos en profundidad
- Seguridad y cifrado de la comunicación

Sesión 2 – Afinamiento de detección y normalización
- Tuning de remoted, analysisd, decoders personalizados
- Uso avanzado de reglas CDB y listas negras/blancas
- Detección de evasiones: timestomping, obfuscación de procesos, LOLBins

Módulo 2: Inteligencia de Amenazas y Correlación Contextual
Sesión 3 – Integración avanzada con MISP
- Instalación y configuración de MISP
- Automatización con PyMISP
- Sincronización de eventos y atributos
- Correlación cruzada de IOCs en tiempo real

Sesión 4 – OpenCTI, STIX y feeds TAXII
- Introducción a OpenCTI + Wazuh
- Enriquecimiento de alertas con contexto
- Configuración de feeds STIX/TAXII (CIRCL, InfectedHosts, etc.)

- Caso práctico: correlación de campaña de APT con reglas Sigma + OpenCTI

Módulo 3: Reglas Basadas en TTPs y Técnicas de Red Team
Sesión 5 – Reglas de detección basadas en MITRE ATT&CK
- Cobertura táctica y técnica
- Creación de reglas Wazuh alineadas a ATT&CK
- Simulación de técnicas ofensivas (LOLBins, UAC bypass, etc.)

Sesión 6 – Detección de actividad maliciosa compleja
- Uso combinado de Sysmon, Osquery y Falco
- Ingeniería inversa de alertas
- Detección de beaconing, process hollowing y fileless malware

Módulo 4: Threat Hunting Guiado por Hipótesis
Sesión 7 – Metodología de hunting
- Hipótesis, modelos de detección y marcos de análisis
- MITRE D3FEND, análisis de ataque, y casos reales

Sesión 8 – Ejecución práctica de hunts
- Hunts de persistencia, movimiento lateral y exfiltración
- Uso de Wazuh + Sigma + Kibana para búsquedas avanzadas

Módulo 5: Orquestación y Automatización de Respuesta
Sesión 9 – TheHive y Cortex para respuesta automatizada
- Ingesta automática de alertas de Wazuh
- Analyzers y responders
- Priorización y enriquecimiento automático

Sesión 10 – Casos prácticos de SOAR
- Playbooks para ransomware, C2, escalamiento de privilegios
- Integración de herramientas de análisis (VirusTotal, AbuseIPDB, MISP)

Módulo 6: Detección en la Nube, CI/CD y Contenedores
Sesión 11 – CloudTrail, GCP, Azure y Falco
- Integraciones con AWS GuardDuty, GCP SCC, Azure Activity Logs
- Monitorización de actividades sospechosas en la nube
- Correlación de eventos híbridos

Sesión 12 – Integración con DevSecOps y contenedores
- Seguridad en CI/CD: detección en repos, artefactos, pipelines
- Visibilidad y control con Falco, auditd, Wazuh
- Cierre: despliegue completo con hunting, CTI y respuesta

* En la cotización deberán entregar el silabus del curso.

10.2 Plan de Trabajo: No corresponde

10.3 Reglamentos técnicos, normas metrológicas y/o sanitarias:
- Norma Técnica Peruana ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ra. Edición.
- Norma Técnica Peruana ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición
- Norma Técnica Peruana ISO/IEC 27032:2024 Ciberseguridad. Directrices para la seguridad en Internet.

- Norma Técnica Peruana ISO/IEC 27035-3:2024 Tecnología de la información. Gestión de incidentes de seguridad de la información. Parte 3: Directrices para operaciones de respuesta a incidentes de las TIC. 1ª Edición

10.4 Seguros: No corresponde

10.5 Prestaciones accesorias a la prestación principal: No corresponde

10.5.1 Mantenimiento preventivo y/o correctivo
a. Sí ( ) b. No (X)

10.5.2 Soporte técnico de ser el caso:
a. En el sitio ( ) b. Por teléfono ( )
c. En taller de terceros ( ) d. En Línea ( )

10.5.2 Capacitación y/o entrenamiento:
a. Sí ( ) b. No (X)

10.5.3 Otras prestaciones accesorias
a. Sí ( ) b. No (X)

10.6 Garantía:
a. ……. Meses b. .....Año c) durante la ejecución del servicio

10.7 Corresponde a una consultoría:
a. Sí ( ) b. No (X)

11. REQUISITOS DEL PROVEEDOR Y/O PERSONAL:

11.1 Habilitación: No corresponde

11.2 Experiencia del proveedor:

Contar con una experiencia de mínimo con 02 órdenes de servicios y/o compra en el servicio de capacitaciones de cursos en temas ciberseguridad o seguridad de la información para Instituciones Públicas y/o Privadas.

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.

11.3 Del personal clave:

11.3.1 Formación académica:

Acreditación: Profesional con una certificación internacional en ciberseguridad, vigente, la cual deberá ser acreditada con el certificado y/o constancia respectiva.

11.3.2 Experiencia Laboral:

Acreditación: experiencia dictando cursos en temas de ciberseguridad o seguridad de la información para el sector público o privado, la cual deberá ser acreditada mínimo con dos (02) certificados y/o constancias de trabajo y/o constancias de prestación de servicios.

11.3.3 Otros: Adjuntar CV documentado del docente.

12. RESPONSABILIDAD POR VICIOS OCULTOS:

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del servicio contratado por un plazo de un año, contado a partir de la conformidad otorgada por el área usuaria.

13. LUGAR Y PLAZO DE EJECUCIÓN DE LA PRESTACIÓN:

a. Lugar: Aula virtual proporcionada por el contratista.
b. Plazo de ejecución del servicio: (en días calendarios): 60 días calendario contabilizado a partir del día siguiente de notificada la orden de servicio.-
c. Plazo para la entrega de los entregables: Siete días calendarios contabilizado a partir del día siguiente de culminado el dictado del curso.

14. RESULTADOS ESPERADOS (ENTREGABLES):
Informe final del curso; conteniendo los certificados, constancia de notas y el acta de asistencia de los participantes.

15. LUGAR DE PRESENTACIÓN DE LOS ENTREGABLES:
Mesa de partes presencial del INICTEL-UNI (Av. San Luis 1771 – San Borja)
Horario de atención de 8:30 – 12:30 pm / 2:00 – 4:00 pm

16. FORMA DE PAGO:
a. Pago Único (X) b. Pagos Parciales ( )

17. FORMULA DE REAJUSTE: No corresponde.

18. CONFORMIDAD DEL SERVICIO:
a. Dependencia que brindará la conformidad técnica: Recursos Humanos.
b. Dependencia que brindará la conformidad de pago: OAD – Recursos Humanos.

19. PENALIDADES POR MORA:

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

Donde F tiene los siguientes valores:
Para bienes y servicios en general 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.

20. OTRAS PENALIDADES: No corresponde.

21. CLÁUSULAS:

21.1. GARANTÍA:

No se requiere la presentación de garantías, de conformidad con lo previsto en el Artículo 139 el Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas.

21.2. ANTICORRUPCIÓN Y ANTISOBORNO:

A la suscripción del 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, 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 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, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios,

asesores o cualquier persona vinculad 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. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiere lugar.

21.3. SOLUCIÓN DE CONTROVERSIAS:

En el caso de contratos menores, las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante CONCILIACION.

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 N° 32069, Ley General de Contrataciones Públicas.

21.4. RESOLUCIÓN DEL CONTRATO POR INCUMPLIMIENTO:

Cualquiera de las partes puede resolver, total o parcialmente, el contrato en los siguientes supuestos:

a) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
b) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
c) 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.
d) Por incumplimiento de la cláusula anticorrupción.
e) Por la presentación de documentación falsa o inexacta durante la interacción con el mercado.

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.

21.5. GESTION DE RIESGOS:

Es un proceso dinámico y abarca las etapas de la contratación pública, el cual comprende las actividades y las acciones proactivas, preventivas y transversales adoptadas por una entidad contratante para identificar los riesgos que esta enfrenta en la contratación de bienes, servicios y obras. Dichas actividades y acciones se realizan sobre la base de la identificación, análisis, valoración, gestión, control y monitoreo de riesgos, que permiten tomar decisiones informadas y aprovechar las oportunidades potenciales derivadas de estos. Las entidades

contratantes realizan la gestión de riesgos a fin de aumentar la probabilidad y el impacto de riesgos positivos y disminuir la probabilidad y el impacto de riesgos negativos, que puedan afectar el cumplimiento de la finalidad pública buscada. En todo momento, la gestión de riesgos debe considerar una mejora en la administración y en el uso de los recursos públicos.

Firmado digitalmente por ROMERO VILCAPOMA Patricia FAU 20514761826 soft
Motivo: Doy V° B°
Fecha: 05.07.2025 10:58:50 -05:00

Firmado digitalmente por TIRADO CASILDO Angela FAU 20514761826 soft
Motivo: Doy V° B°
Fecha: 07.07.2025 14:10:25 -05:00

Fecha: 04 de julio de 2025.

……
Ing. Angela Tirado Casildo
Jefa de la Oficina de Administración