## FORMATO Nº 13

## ACTA DE APERTURA ELECTRONICA DE OFERTAS, EVALUACIÓN DE LAS OFERTAS Y CALIFICACIÓN: SERVICIOS EN GENERAL

| 1 | NÚMERO DE ACTA | 006-2025-CS/CP-002-2025-CR |
|---|---|---|

**2 SOBRE LA INFORMACIÓN GENERAL**

En Lima, a los 09 días del mes de abril del año 2025, se reunieron los miembros del comité de selección designados mediante FORMATO 04 N° 002-2025-DGA-CR, encargado de la preparación, conducción y realización del procedimiento de selección del Concurso Público Nº002-2025-CR-1, cuyo objeto de convocatoria es el SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPUBLICA, a fin de efectuar la APERTURA ELECTRONICA DE OFERTAS, ADMISIÓN, EVALUACIÓN DE LAS OFERTAS presentadas y CALIFICACIÓN de la oferta correspondiente según orden de prelación.

**3 SOBRE EL QUORUM Y LOS MIEMBROS PARTICIPANTES DE LA SESIÓN (DE CORRESPONDER)**

El quorum necesario que exige la normativa de contrataciones del Estado, se logró con la presencia de los siguientes miembros:

| | | | | | |
|---|---|---|---|---|---|
| Presidente | JHON IRVIN CISNEROS CARPIO | Titular | X | Dependencia: | Departamento de Abastecimiento - Dirección General de Administración. |
| | | Suplente | | | |
| Primer Miembro | ANA ISIDORA TRONCOS SAMANIEGO | Titular | X | Dependencia: | Departamento de Abastecimiento - Dirección General de Administración. |
| | | Suplente | | | |
| Segundo Miembro | WILFREDO ELÍAS RIVERA LÁZARO | Titular | X | Dependencia: | Area de Infraestructura Tecnológica - Departamento de Tecnologías de la Información |
| | | Suplente | | | |

**4 DETALLE DE LOS PARTICIPANTES**

De acuerdo con el cronograma establecido en las bases, se registraron a través del SEACE como participantes los siguientes proveedores:

| Nº | Nombre o razón social del participante | RUC |
|---|---|---|
| 1 | MIRAVAL OLIVAS WALTER HUBER | 10074572141 |
| 2 | JAPAN COMPUTER SERVICE S.A.C. | 20113277964 |
| 3 | ADVANCED SECURITY GROUP S.A. | 20470111594 |
| 4 | INNOVARE E-BUSINESS S.A.C. | 20475805101 |
| 5 | KONFIDI TECHNOLOGIES S.A. | 20513909463 |
| 6 | THINK NETWORKS PERU S.A.C. | 20524531861 |
| 7 | IB TECHNOLOGY GROUP S.A.C.-IB TECH GROUP S.A.C. | 20537328445 |
| 8 | MICRO SOLUTIONS TI S.A. | 20544303709 |
| 9 | ATIXWORLD SYSTEMS S.A.C. | 20556897256 |
| 10 | 3G IT CONSULTING S.A.C. | 20600050738 |
| 11 | CONSULTORES Y EJECUTORES PASEJUN S.A.C. | 20600084721 |
| 12 | INNOVA TECNOLOGIA CORP S.A.C. | 20601100593 |
| 13 | ALLSAFE CORPORATION E.I.R.L. | 20601252989 |
| 14 | DNP NETWORK S.A.C. | 20603369221 |
| 15 | GRUPO R & S SOCIEDAD COMERCIAL DE RESPONSABILIDAD LIMITADA | 20605353674 |
| 16 | CYBER SECURITY ENTERPRISE S.A.C. | 20606052112 |
| 17 | COMERCIO E INVERSIONES ANCCAS S.A.C. | 20607396516 |
| 18 | BGS PERU CO. LTD. E.I.R.L. | 20607821608 |
| 19 | HARDSECUR E.I.R.L. | 20609755751 |
| 20 | BUSINESS INSIGHTS S.A.C. | 20613591126 |
| 21 | PASSWORD CONSULTING SERVICES SAS | 99000035820 |

**Nota:** De conformidad con el literal B del numeral 11.2.2.2 de la Directiva N°003-2020-OSCE/CD - DISPOSICIONES APLICABLES PARA EL ACCESO Y REGISTRO DE INFORMACIÓN EN EL SISTEMA ELECTRÓNICO DE CONTRATACIONES DEL ESTADO - SEACE: "El SEACE restringe el registro de aquellos proveedores que no cuentan con inscripción vigente en el RNP, que su registro no corresponda al objeto del procedimiento, o se encuentre suspendido o inhabilitado para contratar con el Estado."

**5 DETALLE DE LOS POSTORES**

En el día y horario señalado en las bases, los siguientes postores presentaron su oferta de manera electrónica a través del SEACE:

| Nº | Nombre o razón social del postor | Estado de la propuesta | Fecha de presentación | Hora de presentación |
|---|---|---|---|---|
| 1 | INNOVA TECNOLOGIA CORP S.A.C. | Enviado | 24/03/2025 | 19:58:56 |

**Nota:** De conformidad con el literal C del numeral 11.2.2.3 de la Directiva N°003-2020-OSCE/CD - DISPOSICIONES APLICABLES PARA EL ACCESO Y REGISTRO DE INFORMACIÓN EN EL SISTEMA ELECTRÓNICO DE CONTRATACIONES DEL ESTADO - SEACE: "El SEACE restringe el registro de la oferta de aquellos participantes, incluyendo a los consorcios y sus integrantes, que no cuentan con inscripción vigente en el RNP, que su registro no corresponda al objeto del procedimiento, o se encuentre suspendido o inhabilitado para contratar con el Estado."

## FORMATO Nº 13

## ACTA DE APERTURA ELECTRONICA DE OFERTAS, EVALUACIÓN DE LAS OFERTAS Y CALIFICACIÓN: SERVICIOS EN GENERAL

**6 ADMISIÓN DE LAS OFERTAS**

Acto seguido, se procede con la descarga y apertura electronica de las ofertas de los mencionados postores, y con la revisión de las mismas, a fin de verificar la presentación de los documentos requeridos y determinar si las ofertas responden a las características y/o requisitos y condiciones del requerimiento previstos en las bases.

Se procedió a verificar que las ofertas cumplan con la acreditación de la documentación solicitada en el numeral 2.2.1.1 del capítulo II de la sección específica de las bases integradas del procedimiento de selección, de conformidad a lo establecido en el numeral 73.2 del Art. 73° del Reglamento de la LCE. El detalle de admisión de ofertas se encuentra en el **Anexo N°1** que forma parte de la presente Acta.

**7 DETALLE DE LAS OFERTAS QUE NO FUERON ADMITIDAS**

De acuerdo con la revisión efectuada, las siguientes ofertas no se admiten, por lo que no se les aplicará los factores de evaluación:

| Nº | Nombre o razón social | Consignar las razones para su no admisión |
|---|---|---|
| --- | --- | --- |

**8 DETALLE DE LAS OFERTAS QUE FUERON ADMITIDAS Y QUE PASAN A EVALUACIÓN**

De acuerdo con la revisión efectuada, las siguientes ofertas fueron admitidas por lo que se procederá con su evaluación:

| Nº | Nombre o razón social del postor | Item(s) a los que postula |
|---|---|---|
| 1 | INNOVA TECNOLOGIA CORP S.A.C. | 1 |

**9 EVALUACIÓN DE LAS OFERTAS**

**9.1 DETALLE DEL PRECIO DE LA OFERTA**

| Nº | Nombre o razón social del postor | Precio de su oferta | % del valor estimado |
|---|---|---|---|
| 1 | INNOVA TECNOLOGIA CORP S.A.C. | S/ 2,498,000.00 | 68.44% |

**9.2 DETALLE DE LA EVALUACIÓN DE LAS OFERTAS EN CONCORDANCIA CON LOS FACTORES DE EVALUACIÓN ESTABLECIDOS EN LAS BASES DEL PROCEDIMIENTO DE SELECCIÓN**

La evaluación de las ofertas se detalla en el cuadro de Evaluación de Ofertas, según **Anexo N° 02** que forma parte de la presente Acta.

**10 PUNTAJE DE LAS OFERTAS DE LOS POSTORES**

**10.1**

| NOMBRE O RAZON SOCIAL DEL POSTOR | INNOVA TECNOLOGIA CORP S.A.C. |
|---|---|
| FACTORES | PUNTAJES |
| PRECIO | 100.00 |
| PUNTAJE TOTAL DE FACTORES | 100.00 puntos |

**11 RESULTADOS DE LA EVALUACIÓN**

De acuerdo a la evaluación realizada, el orden de prelación es el siguiente:

| Nº DE ORDEN DE PRELACIÓN | NOMBRE O RAZÓN SOCIAL DEL POSTOR | PUNTAJE TOTAL |
|---|---|---|
| 1 | INNOVA TECNOLOGIA CORP S.A.C. | 100.00 |

**12 CALIFICACIÓN**

Luego de culminada la evaluación, el COMITÉ DE SELECCIÓN determinó si existen postores, de acuerdo al orden de prelación, que cumplan con los requisitos de calificación detallados en las bases:

**12.1**

| NOMBRE O RAZON SOCIAL DEL POSTOR Nº 1 | | | INNOVA TECNOLOGIA CORP S.A.C. | |
|---|---|---|---|---|
| REQUISITOS DE CALIFICACIÓN | | | CUMPLE | NO CUMPLE |
| B | CAPACIDAD TÉCNICA Y PROFESIONAL | | X | |
| | B.3 CALIFICACIONES DEL PERSONAL CLAVE | | X | |
| | | B.3.1 FORMACIÓN ACADÉMICA | x | |
| | | B.3.2 CAPACITACIÓN | x | |
| | B.4 EXPERIENCIA DEL PERSONAL CLAVE | | X | |
| C | EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD | | X | |
| RESULTADO DE LA CALIFICACIÓN | | | CALIFICADO | |

**12.2 DETALLE DE LA CALIFICACIÓN DE LAS OFERTAS**

La calificación de las ofertas se detalla en el cuadro de Calificación, según **Anexo N°03** que forma parte de la presente Acta.

## FORMATO Nº 13

## ACTA DE APERTURA ELECTRONICA DE OFERTAS, EVALUACIÓN DE LAS OFERTAS Y CALIFICACIÓN: SERVICIOS EN GENERAL

**13 RESULTADOS DE LA CALIFICACIÓN**

De acuerdo a la calificación realizada, el postor que ocupa el **primer lugar** en el orden de prelación cumple con los requisitos de calificación establecidos en las bases. Por lo tanto, el postor ganador de la buena pro es el siguiente:

| Nº | NOMBRE O RAZÓN SOCIAL DEL POSTOR GANADOR |
|---|---|
| 1 | INNOVA TECNOLOGIA CORP S.A.C. |

**14 ACUERDO ADOPTADO**

Los integrantes del COMITÉ DE SELECCIÓN, por UNANIMIDAD, dan por aprobados los resultados de la evaluación de las ofertas y calificación, de acuerdo con el análisis efectuado y los cuadros de Evaluación de Ofertas y Calificación adjuntos que forman parte del Acta.

**15**

| ANA ISIDORA TRONCOS SAMANIEGO | JHON IRVIN CISNEROS CARPIO | WILFREDO ELÍAS RIVERA LÁZARO |
|---|---|---|
| PRIMER MIEMBRO DE COMITÉ SELECCIÓN | PRESIDENTE DEL COMITÉ DE SELECCIÓN | SEGUNDO MIEMBRO DEL COMITÉ DE SELECCIÓN |

**NOMBRES Y FIRMAS DE LOS INTEGRANTES DEL COMITÉ DE SELECCIÓN O DEL ÓRGANO ENCARGADO DE LAS CONTRATACIONES**

# ANEXO N° 1
## ADMISIÓN DE OFERTAS

Se procedió a verificar que las ofertas cumplan con la acreditación de la documentación solicitada en el numeral 2.2.1.1 del capítulo II de la sección específica de las bases integradas del procedimiento de selección y de conformidad a lo establecido en el numeral 73.2 del Art. 73° del Reglamento de la LCE.

De la verificación de la documentación para la admisión de la oferta presentada por los postores, se señala lo siguiente:

| Nº | DOCUMENTO | 1<br>INNOVA TECNOLOGIA CORP S.A.C.<br>RUC N° 20601100593 |
|---|---|---|
| a) | Declaración jurada de datos del postor. (Anexo Nº 1) | CUMPLE |
| b) | Documento que acredite la representación de quien suscribe la oferta. | CUMPLE |
| c) | Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. (Anexo Nº 2). | CUMPLE |
| d) | Declaración jurada de cumplimiento de los Términos de Referencia contenidas en el numeral 3.1 del Capítulo III de la presente sección. (Anexo Nº 3) | CUMPLE |
| e) | Catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales y/o capturas de pantalla de las plataformas en funcionamiento, para acreditar el cumplimiento de los siguientes componentes:<br><br>Compatibilidad con sistemas operativos especificados, integración con fuentes de datos de seguridad (firewalls, antivirus, correo, directorio activo, componentes de red), autenticación de dos factores (2FA), protocolos de comunicación segura, aislamiento del agente (sin conexiones entrantes ni control remoto), coadministración basada en roles (propietario, visualizador, resolutor de incidentes), capacidades avanzadas de detección y respuesta (SOAR) integradas con MITRE ATT&CK, reducción de la superficie de ataque mediante pruebas de penetración y priorización de vulnerabilidades, monitoreo 24x7 de eventos de seguridad con alertas en tiempo real, respuesta automatizada a incidentes (aislamiento de hosts comprometidos, remediación de amenazas), certificaciones internacionales (ISO/IEC 27001, 27017, 27018, CSA STAR, SOC 3), generación de reportes (inventario, vulnerabilidades, eventos detectados), modalidad SaaS desde un SOC Data Center certificado, capacidad de análisis predictivo mediante Cyber Threat Intelligence (dark web, día 0/1 día), cumplimiento de normativas internacionales (ISO, NIST, STIG). | CUMPLE (*) |
| f) | Declaración jurada de plazo de entrega. (Anexo Nº 4). | CUMPLE |
| g) | Promesa de consorcio con firmas legalizadas. (Anexo Nº 5) | NO CORRESPONDE |
| h) | El precio de la oferta en Soles. (Anexo N° 6). | CUMPLE |
| **RESULTADO** | | **ADMITIDA** |

**(*) Acciones realizadas por el comité de selección:**

Mediante correo electrónico de fecha 25 de marzo de 2025, el comité de selección, en merito a lo establecido en el numeral 46.4 del artículo 46 del Reglamento de la Ley de Contrataciones del Estado, el cual precisa lo siguiente: *"Durante el desempeño de su encargo,* ***el comité de selección está facultado para solicitar el apoyo que requiera de las dependencias o áreas pertinentes de la Entidad****, las que están obligadas a brindarlo bajo responsabilidad."*, solicita al Área de Infraestructura Tecnológica del Departamento de Tecnologías de la Información, en su calidad de área técnica, apoyo en la revisión técnica de la oferta presentada por el postor: **INNOVA TECNOLOGIA CORP S.A.C.**, en lo respecta al cumplimiento del literal e) del numeral 2.2.1.1 de la Sección Especifica de las bases integradas. Asimismo, se precisó que, a pesar de que la presentación del documento técnico para acreditar el cumplimiento de la primera viñeta del numeral 7.1 de los términos de referencia, no es un documento obligatorio para la admisión de la oferta, dicho documento forma parte de la oferta del postor y deberá ser verificado también, de tal forma que no se identifiquen incongruencias, contradicciones u ambigüedades con los términos de referencia en ambas verificaciones.

Con correo electrónico de fecha 02 de abril del 2025, el Área de Infraestructura Tecnológica del Departamento de Tecnologías de la Información comunica el resultado de la verificación técnica de la oferta del postor **INNOVA TECNOLOGIA CORP S.A.C.,** donde se indica que la oferta del mencionado postor cumple con acreditar los requisitos solicitados en las bases integradas y los términos de referencia. De acuerdo al siguiente detalle:

Respecto a la documentación presentada para acreditar el cumplimiento del literal e) del numeral 2.2.1.1 de la Sección Especifica de las bases integradas del CONCURSO PÚBLICO N°002-2025-CR y, al numeral 7.5 de los términos de referencia

| N° | Requisito | Solicitado | Cumplimiento | Pagina/Sustento | URL/Evidencia de Sustento |
|---|---|---|---|---|---|
| 1 | Compatibilidad con sistemas operativos especificados | • La plataforma deberá soportar mínimamente las siguientes plataformas de sistemas operativos Windows Server 2012 R2 (32-bit / 64-bit), Windows Server 2016 / 2019 (32-bit / 64-bit), Windows Server 2022 (32-bit / 64-bit), Centos 7 and greater, Red Hat 8 and 9. | CUMPLE | 1 de 33<br>2 de 33 | (SUSTENTO N°1)<br>URL: https://www.rocketcyber.com/faqs/ |
| 2 | Integración con fuentes de datos de segurdad (firewalls, antivirus, correo, directorio activo, componentes de red) | • La plataforma debe integrar capacidades de SIEM Less para el monitoreo y correlacionamiento de eventos de seguridad de hosts, firewalls, antivirus, directorio activo, correo electrónico y/o componentes de red, incorporando la detección de infracciones basadas en las técnicas de Mitre Attack, la actividad y los servicios de la red, las herramientas sospechosas y la detección de archivos maliciosos para brindar una solución de seguridad integral. | CUMPLE | 2 de 33 a la<br>7 de 33 | (SUSTENTO N°2A):<br>URL: https://www.rocketcyber.com/products/managed-soc/<br>(SUSTENTO N°2B):<br>URL: https://www.rocketcyber.com/appstore/ |
| 3 | Autenticación de dos factores (2FA) | • La plataforma debe admitir la autenticación de dos factores (2FA) para salvaguardar el acceso a la consola. | CUMPLE | 7 de 33 a la<br>8 de 33 | (SUSTENTO N°3):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/account/securing-your-account-with-two-factor-authentication-2fa.html |
| 4 | Protocolos de comunicación segura | • La plataforma debe garantizar la seguridad de las comunicaciones usando el protocolo TLS v1.2 | CUMPLE | 8 de 33 a la<br>9 de 33 | (SUSTENTO N°4):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/rocketcyber-managed-soc-agent-architecture-and-capabilities.htm |
| 5 | Aislamiento del agente (sin conexiones entrantes ni control remoto) | • La plataforma debe contar con capacidades de respuesta ante ataques en curso, aislando dispositivos en la red que tengan instalado un agente, el aislamiento del host se realizará como consecuencia de un análisis y/o activación automática de un playbook de respuesta a incidentes para evitar la propagación de código malicioso al impedir que una máquina vulnerada se comunique con otros dispositivos de red en internet o la red del cliente. La máquina aislada mantendrá la conectividad con la plataforma correspondiente y permitirá que el Data Center SOC o equipo responsable en la institución reconecten el dispositivo. | CUMPLE | 9 de 33 a la<br>10 de 33 | (SUSTENTO N°5):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/managed-soc-incident-response.htm |
| 6 | Coadministración basada en roles (propietario, visualizador, resolutor de incidentes) | • La plataforma debe presentarse como un sistema integrado tipo SOAR integrando tecnologías y plataformas requendas que se gobiernen desde una sola consola de orquestación automatizada con acceso basado en roles que permita la COADMINISTRACIÓN por parte del equipo del Congreso de la Republica. | CUMPLE | 11 de 33 a la<br>12 de 33 | (SUSTENTO N°6A):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/getting_started-with-rocketcyber.htm<br>(SUSTENTO N°6B):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/roles-and-access-permissions-in-rocketcyber.html |

| | | | | | |
|---|---|---|---|---|---|
| 7 | Capacidades avanzadas de detección y respuesta (SOAR) integradas con MITRE ATT&CK | • La plataforma de Cyber SOC debe integrar a través del agente capacidades de detección avanzada de infracciones reconociendo tácticas, técnicas y procedimientos (TTP) del adversario de acuerdo con el marco MITRE ATT&CK. | CUMPLE | 12 de 33 a la 14 de 33 | (SUSTENTO N°7A):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/overview/rocketcyber-native-capabilities.html?Highlight=ADVANCED%20BREACH%20DETECTION<br>(SUSTENTO N°7B):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/getting_started-with-rocketcyber.htm<br>(SUSTENTO N°7C):<br>URL: https://www.microsoft.com/es-mx/security/business/security-101/what-is-a-security-operations-center-soc |
| 8 | Reducción de la superficie de ataque mediante pruebas de penetración y priorización de vulnerabilidades | • La solución propuesta para este escenario tiene por objetivo añadir capacidades de prevención proactiva contra ataques cibernéticos a la plataforma de Cyber SOC delegada a través de la reducción proactiva y continua de la superficie de ataque externa e interna en la entidad. | CUMPLE | 14 de 33 a la 17 de 33 | (SUSTENTO N°8A):<br>URL: https://www.vonahi.io/<br>(SUSTENTO N°8B):<br>URL: https://www.secpod.com/risk-prioritization-real/ |
| 9 | Monitoreo 24x7 de eventos de seguridad con alertas en tiempo real | • La plataforma base tipo SOAR debe permitir la integración con la infraestructura de TI y seguridad existente, logrando que la plataforma administrada por el equipo de analistas de SOC del fabricante identifique rápidamente actividades maliciosas y sospechosas en los principales vectores de amenazas críticas: endpoint, red y nube, para brindar una defensa avanzada contra ciberamenazas las 24 horas, los 7 días de la semana durante el tiempo que dure la suscripción. | CUMPLE | 17 de 33 a la 19 de 33 | (SUSTENTO N°9):<br>URL: https://www.rocketcyber.com/products/managed-soc/ |
| 10 | Respuesta automatizada a incidentes (aislamiento de hosts comprometidos, remediación de amenazas) | La plataforma debe contar con capacidades de respuesta y remediación a través del agente, logrando ejecutar la eliminación de archivos, eliminación de claves y valores del registro, terminación de procesos, desinstalación de software, parada de servicios, eliminación de tareas programadas. | CUMPLE | 19 de 33 a la 21 de 33 | (SUSTENTO N°10):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/managed-soc-incident-response.htm |
| 11 | Certificaciones internacionales (ISO/IEC 27001, 27017, 27018, CSA STAR, SOC 3) | • La plataforma de Cyber SOC delegada debe ser provista en modalidad de Software as a Service (SaaS) desde un SOC Data Center que cuente con infraestructura certificada en conformidad con al menos dos (02) de las siguientes normas ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM v4.0. | CUMPLE | 21 de 33 a la 23 de 33 | (SUSTENTO N°11A):<br>URL: https://www.kaseya.com/download/13530/?tmstv=16835766<br>2 (SUSTENTO N°11B):<br>URL: https://www.kaseya.com/trust-center/earning-your-trust/<br>(SUSTENTO N°11C):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/rocketcyber-managed-soc-agent-architecture-and-capabilities.htm<br>(SUSTENTO N°11D):<br>URL: https://aws.amazon.com/es/compliance/iso-certified/ |

| | | | | | |
|---|---|---|---|---|---|
| 12 | Generación de reportes (inventario, vulnerabilidades, eventos detectados) | • La plataforma debe permitir crear reportes bajo demanda y programarlos para su envío automático al correo electrónico.<br>• La plataforma debe permitir la creación de informes de inventario e informes ejecutivos hasta con una antigüedad de noventa (90) días. | CUMPLE | 23 de 33 a la 27 de 33 | (SUSTENTO N°12A):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/overview/reporting-overview.html?Highlight=report<br>(SUSTENTO N°12B):<br>URL: https://docs.secpod.com/docs/how-to-create-a-custom-report-in-sanernow/<br>(SUSTENTO N°12C):<br>URL: https://www.secpod.com/saner-posture-anomaly/<br>(SUSTENTO N°12D):<br>URL: https://www.secpod.com/risk-based-vulnerability-management/ |
| 13 | Modalidad SaaS desde un SOC Data Center certificado | • La plataforma deberá ser presentada en modalidad de Software as a Service (SaaS) sin requerir de infraestructura física adicional para su normal desempeño.<br>• La plataforma de Cyber SOC delegada debe ser provista en modalidad de Software as a Service (SaaS) desde un SOC Data Center que cuente con infraestructura certificada en conformidad con al menos dos (02) de las siguientes normas ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM v4.0. | CUMPLE | 27 de 33 a la 28 de 33 | (SUSTENTO N°13A):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/rocketcyber-managed-soc-agent-architecture-and-capabilities.htm<br>(SUSTENTO N°13B):<br>URL: https://aws.amazon.com/es/compliance/iso-certified/ |
| 14 | Capacidad de análisis predictivo mediante Cyber Threat Intelligence (dark web, día 0/1 día) | • La plataforma de Cyber SOC deben incluir funciones de búsqueda a través de sistemas de cacería de amenazas avanzadas y feeds de búsqueda de inteligencia de amenazas automatizadas | CUMPLE | 28 de 33 a la 32 de 33 | (SUSTENTO N°14A):<br>URL: https://outpost24.com/products/cyber-threat-intelligence/<br>(SUSTENTO N°14B):<br>URL: https://outpost24.com/wp-content/uploads/2023/10/Outpost24_ThreatCompass_2023.pdf<br>(SUSTENTO N°14C):<br>URL: https://docs.secpod.com/docs/sanercvem-patch-management-user-guide/ |
| 15 | Cumplimiento de normativas internacionales (ISO, NIST, STIG) | • La plataforma deberá implementar una gestión avanzada de vulnerabilidades, configuraciones alineadas a cumplimiento normativo como ISO y NIST además los activos en busca de anomalías. | CUMPLE | 29 de 33 a la 32 de 33 | (SUSTENTO N°15):<br>URL: https://docs.secpod.com/docs/overview-of-sanercvem-advanced-vulnerability-management/ |

Respecto a la documentación presentada para acreditar el cumplimiento de la primera viñeta del numeral 7.1 de los términos de referencia

| N° | Requisito | Solicitado | Cumplimiento | Pagina/Sustento | URL/Evidencia de Sustento |
|---|---|---|---|---|---|
| 1 | El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoria de tipo SOC 2 para los productos de detección y respuesta ofertados. | • La plataforma deberá soportar mínimamente las siguientes plataformas de sistemas operativos Windows Server 2012 R2 (32-bit / 64-bit), Windows Server 2016 / 2019 (32-bit / 64-bit), Windows Server 2022 (32-bit / 64-bit), Centos 7 and greater, Red Hat 8 and 9. | CUMPLE | Páginas 046-057 (Documento: Traducción Certificada TC N.° 0777-2025) | Informe del Auditor de Servicio Independiente sobre la Descripción de la Gestión del Sistema - SOC 2 Tipo 2 de Kaseya US, LLC para el periodo del 1 de junio de 2023 al 31 de mayo de 2024 |
| 2 | El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoria de tipo SOC 3 para los productos de detección y respuesta ofertados. | • La plataforma debe integrar capacidades de SIEM Less para el monitoreo y correlacionamiento de eventos de seguridad de hosts, firewalls, antivirus, directorio activo, correo electrónico y/o componentes de red, incorporando la detección de infracciones basadas en las técnicas de Mitre Attack, la actividad y los servicios de la red, las herramientas sospechosas y la detección de archivos maliciosos para brindar una solución de seguridad integral. | CUMPLE | Páginas 058-063 (Documento: Traducción Certificada TC N.° 0779-2025) | Informe del Auditor de Servicio Independiente sobre la Descripción de la Gerencia del Sistema - SOC 3 de Kaseya US, LLC para el periodo del 1 de junio de 2023 al 31 de mayo de 2024 |

En ese sentido, de la revisión integral de los documentos presentados por el postor **INNOVA TECNOLOGIA CORP S.A.C.,** para acreditar lo requerido en el numeral 2.2.1.1 Documentos para la admisión de la oferta, de la Sección Especifica de las bases integradas, y del resultado de la revisión técnica realizada por el Área de Infraestructura Tecnológica del Departamento de Tecnologías de la Información, se da por **ADMITIDA** la oferta del postor mencionado.

# ANEXO N°2

## EVALUACIÓN DE OFERTAS

El Comité de Selección, procedió a determinar el puntaje, según los factores de evaluación enunciados en el capítulo IV de las bases integradas, siendo para ello el único factor de evaluación el **Precio** con un puntaje máximo de **100 puntos**.

| FACTOR DE EVALUACIÓN | | PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN |
|---|---|---|
| A. | **PRECIO** | |
| | Evaluación:<br><br>Se evaluará considerando el precio ofertado por el postor.<br><br>Acreditación:<br><br>Se acreditará mediante el documento que contiene el precio de la oferta **(Anexo N° 6)**. | La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula:<br><br>$Pi = \frac{Om \times PMP}{Oi}$<br><br>**i** = Oferta<br>**Pi** = Puntaje de la oferta a evaluar<br>**Oi** = Precio i<br>**Om** = Precio de la oferta más baja<br>**PMP** = Puntaje máximo del precio<br><br>**100 puntos** |

| POSTORES ADMITIDOS | FACTORES DE EVALUACIÓN | | PUNTAJE TOTAL | ORDEN DE PRELACIÓN | % DE LA OFERTA RESPECTO AL VALOR ESTIMADO |
|---|---|---|---|---|---|
| | A.PRECIO | | | | |
| | Monto | Puntaje | | | |
| INNOVA TECNOLOGIA CORP S.A.C. | S/ 2,498,000.00 | 100.00 | 100.00 | 1 | 68.44% |

| | |
|---|---|
| **Valor Estimado** | **S/ 3,650,000.00** |
| **Precio de Oferta mas baja** | S/ 2,498,000.00 |

Luego de la evaluación realizada, queda el siguiente orden de prelación:

| Nº DE ORDEN DE PRELACIÓN | NOMBRE O RAZÓN SOCIAL DEL POSTOR | PRECIO DE LA OFERTA | PUNTAJE TOTAL | % RESPECTO AL V.E. |
|---|---|---|---|---|
| 1 | INNOVA TECNOLOGIA CORP S.A.C. | S/ 2,498,000.00 | 100.00 | 68.44% |

# ANEXO N°3
## CALIFICACIÓN DE OFERTAS

En cumplimiento de lo establecido en el Capítulo III – punto 3.2 "Calificación de Ofertas", el Comité de Selección realiza la calificación de la oferta de los postores que obtuvieron el primer y segundo lugar en el orden de prelación, conforme a lo establecido en los numerales 75.1 y 75.2 del artículo 75 del Reglamento. La oferta del postor que no cumpla con los requisitos de calificación es descalificada.

Si alguno de los dos (2) postores no cumple con los requisitos de calificación, el comité de selección verifica los requisitos se calificación de los postores admitidos, según el orden de prelación obtenido en la evaluación, hasta identificar dos (2) postores que cumplan con los requisitos de calificación; salvo que, de la revisión de las ofertas, solo se pueda identificar una (1) que cumpla con tales requisitos.

Verificación de los requisitos de calificación del postor que obtuvo el **primer** lugar y único en el orden de prelación:

| REQUISITOS DE CALIFICACIÓN | INNOVA TECNOLOGIA CORP S.A.C. |
|---|---|
| **ORDEN DE PRELACIÓN** | **1** |
| **B. CAPACIDAD TÉCNICA Y PROFESIONAL** | |
| **B.3 CALIFICACIONES DEL PERSONAL CLAVE** | **PERSONAL CLAVE PROPUESTO**<br>• **Jefe de Proyectos:** Alan Marino Llancachahua Córdova<br>• **Operador de Servicio:** Eduardo Raúl Gonzales Bustamante |
| **B.3.1 FORMACIÓN ACADÉMICA**<br><br>Requisitos:<br>Ingeniero titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Ingeniería Informática del personal clave requerido como **Jefe de Proyectos**.<br><br>Técnico profesional Titulado y/o Titulo o Bachiller profesional en ingeniería, en redes y comunicaciones y/o telecomunicaciones y/o sistemas y/o informática[1] del personal clave requerido como **Operador de Servicio**.<br><br>Acreditación:<br><br>El Título será verificado por el comité de selección 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/* o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: *https://titulosinstitutos.minedu.gob.pe/*, según corresponda. | **FORMACIÓN ACADEMICA**<br><br>**CUMPLE: Si**<br>**Jefe de Proyectos:** Título Profesional de Ingeniero de Computación y Sistemas expedido por la Universidad San Martin de Porres – **Cumple(*)**<br>**Operador de Servicio:** Título Profesional Técnico en Redes y Comunicaciones expedido por el Instituto de Educación Superior Tecnológico Privado "CIBERTEC" – **Cumple** |

[1] Ajuste realizado en merito a la absolución de la Consulta N°24

| | |
|---|---|
| En caso el Título no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida. | |
| **B.3.2 CAPACITACIÓN**<br><br>Requisitos:<br>Mínimo de ocho (08) horas lectivas, en participación en curso o taller "Gestión de Ciber Crisis" del personal clave requerido como **Jefe de Proyectos**.<br><br>Mínimo de ocho (08) horas lectivas, en participación en curso o taller "Gestión de Ciber Crisis" del personal clave requerido como **Operador de Servicio**.<br><br>Acreditación:<br>Se acreditará con copia simple de constancias o certificados, según corresponda. | **CAPACITACIÓN**<br><br>**CUMPLE: Si**<br>**Jefe de Proyectos:** Certificado de participación en el Taller "Gestión de Cibercrisis" por ocho (08) horas lectivas emitido por la asociación internacional ISACA – **Cumple**.<br>**Operador de Servicio:** Certificado de participación en el Taller "Gestión de Cibercrisis" por ocho (08) horas lectivas emitido por la asociación internacional ISACA – **Cumple**. |
| **B.4 EXPERIENCIA DEL PERSONAL CLAVE** | |
| Requisitos:<br>Experiencia no menor de tres (03) años como jefe o gestor de proyectos de soluciones de Ciberseguridad. del personal clave requerido como **Jefe de Proyectos**.<br><br>Experiencia no menor de tres (03) años como especialista en soluciones de Ciberseguridad, del personal clave requerido como **Operador de Servicio**.<br><br>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.<br><br>Acreditación:<br>La experiencia del personal clave 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 del personal propuesto. | **EXPERIENCIA DEL PERSONAL CLAVE**<br><br>**CUMPLE: Si**<br>**Jefe de Proyectos:** Acredita contar con más de tres (03) años de experiencia en las actividades requeridas – **Cumple**.<br>Certificado de trabajo emitido por INNOVA TECNOLOGIA CORP S.A.C. de fecha 24.03.2025, en donde se detalla que el personal realizó actividades en soluciones de ciberseguridad, en el cargo de Jefe de Proyectos.<br><br>**Operador de Servicio:** Acredita contar con más de tres (03) años de experiencia en las actividades requeridas – **Cumple**.<br>Certificado de trabajo emitido por INNOVA TECNOLOGIA CORP S.A.C. de fecha 24.03.2025, en donde se detalla que el personal realizó actividades en soluciones de ciberseguridad, en el cargo de Especialista. |
| **C. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD** | |
| Requisitos:<br>El postor debe acreditar un monto facturado acumulado equivalente a **S/ 1'500,000.00 (Un Millón Quinientos Mil con 00/100 Soles)**, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.<br><br>Se consideran servicios similares a los siguientes: **servicios de soluciones y/o implementación de soluciones de seguridad y ciberseguridad (antivirus y/o antispam y/o XDR y/o EDR), soluciones de monitoreo, automatización y respuesta ante incidentes de seguridad informática y/o soluciones de respaldo y restauración de información para entornos físicos o virtualizados y/o servicio de hackeo ético y/o servicio de ethical hacking y/o servicio de ejecución de ethical hacking y/o servicio para el análisis de vulnerabilidades y/o servicio de análisis de vulnerabilidades y/o servicio de pruebas de penetración y/o servicio para el análisis de ciberseguridad.** | **SI CUMPLE**<br>Postor acredita el monto facturado mínimo solicitado en las bases. |

| | |
|---|---|
| Acreditación:<br><br>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 voucher 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, correspondientes a un máximo de veinte (20) contrataciones.<br>(...) | |
| **RESULTADO** | **CALIFICADA** |

**(*) Acciones realizadas por el comité de selección:**

Mediante correo electrónico de fecha 04 de abril de 2025, el comité de selección, en merito a lo establecido en el numeral 46.4 del artículo 46 del Reglamento de la Ley de Contrataciones del Estado, la cual precisa lo siguiente: *"Durante el desempeño de su encargo, **el comité de selección está facultado para solicitar el apoyo que requiera de las dependencias o áreas pertinentes de la Entidad**, las que están obligadas a brindarlo bajo responsabilidad."*, solicita al Área de Infraestructura Tecnológica del Departamento de Tecnologías de la Información, en su calidad de área técnica, su apoyo en la revisión técnica de la oferta presentada por el postor: **INNOVA TECNOLOGIA CORP S.A.C.**, en lo respecta al cumplimiento de la Formación Académica del personal clave Jefe de Proyectos requerido en el numeral 3.2 Requisitos de Calificación de la Sección Especifica de las Bases Integradas.

Con correo electrónico de fecha 04 de abril del 2025, el Área de Infraestructura Tecnológica del Departamento de Tecnologías de la Información comunica el resultado de la verificación técnica de la oferta del postor **INNOVA TECNOLOGIA CORP S.A.C.**, indicando lo siguiente:

*"Luego de analizar lo indicado respecto a la formación académica del personal propuesto como Jefe de Proyectos, quien cuenta con el título de "Ingeniero de Computación y Sistemas", y contrastándola con lo requerido en las bases integradas que solicitan "Ingeniero titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Ingeniería Informática", considero lo siguiente:*

*La evaluación de equivalencias entre denominaciones de títulos profesionales requiere un análisis interpretativo que debe realizarse considerando el perfil profesional y las competencias desarrolladas en la carrera, no limitándose únicamente a la denominación literal.*

*Es importante señalar que, corresponde al Comité de Selección en estricto uso de sus facultades y autonomía determinar si la formación académica ofertada cumple con lo requerido en las bases integradas, teniendo en cuenta que en el Perú existe variedad en las denominaciones de carreras profesionales con competencias y campos de acción similares o equivalentes.*

*Desde el punto de vista técnico, se observa que la carrera de "Ingeniería de Computación y Sistemas" integra conocimientos tanto de computación como de sistemas, abarcando áreas como desarrollo de sistemas, sistemas de información, sistemas computacionales y gestión de TI, las cuales son concordantes con el perfil requerido. Sin embargo, corresponde al Comité de Selección, en ejercicio de sus funciones y conforme a lo establecido en la normativa de contrataciones, evaluar y determinar si la formación ofertada cumple con los requisitos establecidos en las bases, considerando la amplitud y diversidad de denominaciones académicas existentes en el país." (el subrayado es propio)*

Tomando como referencia la Resolución N°529-2022-TCE-S1, en donde el Tribunal de Contrataciones del Estado realiza un análisis respecto a la determinación de una formación académica equivalente respecto a la solicitada en las Bases Integradas, el comité de selección revisó el portal web del Colegio de Ingenieros del Perú[2], a fin de verificar en el Capítulo de ingeniería Industrial, Sistemas y Transportes, si los profesionales de la especialidad de Ingeniería de Computación y Sistemas, son considerados como Ingenieros de Sistemas ante el Colegio de Ingenieros del Perú.

De la revisión del portal web del Colegio de Ingenieros del Perú, se verifica que la Ingeniería de Computación y Sistemas, se encuentra incluido en el Capítulo de Ingeniería Industrial, Sistemas y Transportes, al ser sub especialidad perteneciente a dicho capítulo. Por tanto, se deprende que, para efectos de su colegiatura, los profesionales en Ingeniería de Computación y Sistemas se incluyen dentro del Capítulo que incorpora, entre otras carreras de ingeniería, a los ingenieros de sistemas.

Al respecto, resulta necesario citar lo analizado por el Tribunal de Contrataciones del Estado en la resolución referida en párrafos precedentes, con la finalidad de exponer el criterio sobre la verificación realizada por el comité de selección: *"(...) el Colegio de Ingenieros del Perú – Consejo Departamental de Lima también ha señalado que la especialidad de "Ingeniería de Sistemas Empresariales", es una sub especialidad perteneciente al Capítulo de Ingeniería Industrial, Sistemas y Transportes, por contener dicha sub especialidad cursos afines entre las carreras profesionales de dicho Capítulo, descartando de ese modo, la posibilidad de que la carrera de "Ingeniería de Sistemas Empresariales" corresponda a una profesión distinta a la de Ingeniería de Sistemas, por cuanto comparte cursos afines. Por lo que se entiende que aquellos cursos que resultasen diferentes están orientados a la especialidad empresarial, lo cual no implica que el profesional no pueda colegiarse en el Capítulo que integran los ingenieros de sistemas. Es decir, en el caso en concreto, estamos frente a un profesional en Ingeniería de Sistemas, pero orientado a la especialidad empresarial."*

Por consiguiente, si en las bases integradas se solicitó acreditar el Titulo en la profesión de Ingeniería de Sistemas, este colegiado considera que se acreditó correctamente la formación académica del personal clave requerido como Jefe de Proyectos, toda vez que, la carrera profesional de Ingeniería de Computación y Sistemas, es una sub especialidad perteneciente al Capítulo de Ingeniería Industrial, Sistemas y Transportes, que incorpora a los ingenieros de sistemas.

Finalmente, es menester mencionar que, el Comité de Selección ha realizado una evaluación integral de las ofertas recibidas, verificando todos y cada uno de los documentos obrantes en las mismas, siempre y cuando no signifique subrogarse o asumir la voluntad de los postores al realizar interpretaciones y/o suposiciones que pudieran favorecer (o perjudicar) la condición de éstos, ya que ello implicaría vulnerar los principios de transparencia e igualdad de trato, descritos en la normativa de contrataciones del Estado.

[2] https://cdlima.org.pe/ciist/#1672790108880-aeaf24ca-d0c2

# Capítulo de Ingeniería Industrial, de Sistemas & Transporte

## Junta Directiva

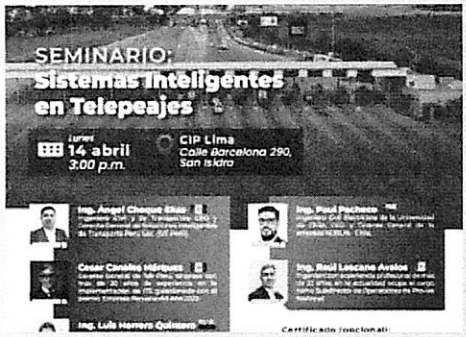
## Especialidades

- Ing. De sistemas empresariales
- Ing. En computación informática
- Ing. Sistemas de información
- Ing. Industrial y gestión empresarial
- Ing. Civil de industrias
- Ing. En computación
- Ing. Agroindustrial
- Ing. De alimentos
- Ing. En sistema automatización de producción de información y control
- Ing. De informática y sistemas
- Ing. De computación y sistemas
- Ing. Industrial y sistemas
- Ing. En informática y de sistemas
- Ing. Industrial y comercial

## Informes de Gestión

El Capítulo de Ingeniería Industrial, de Sistemas y Transporte congrega a los profesionales de estas dos carreras, así como a otras de campos afines, como ingeniería de industrias alimentarias, agroindustria e ingeniería de transportes. Sus objetivos son los de aportar al mejoramiento y optimización de los procesos industriales, la aplicación de mejores herramientas de gestión, métodos y sistemas, así como lograr una mejor producción y distribución.

## Próximos eventos

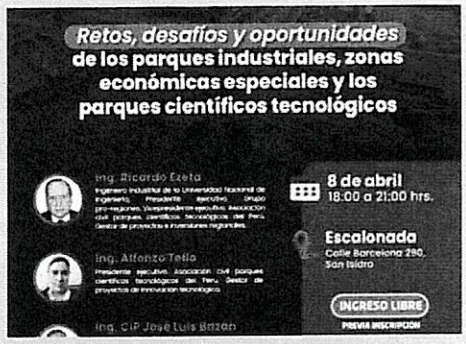



Seminario «Sistemas Inteligentes en Telepeajes» / Lunes 14 de abril – 3:00 p.m.

7 DE ABRIL DE 2025


Conferencia «El Antepuerto del Callao: Una solución estratégica para la congestión portuaria» / Miércoles 16 de abril – 6:00 p.m.

3 DE ABRIL DE 2025




Conferencia «Retos, desafíos y oportunidades de los parques industriales, zonas económicas especiales y los parques [illegible] Martes [illegible] abril – 6:00

Hola deseo comunicarme con ustedes

COLEGIO DE INGENIEROS DEL PERÚ

# CONSEJO DEPARTAMENTAL LIMA

El Consejo Departamental de Lima (CD Lima – CIP) es uno de los órganos principales y agrupa al mayor número de ingenieros colegiados de distintas especialidades conformando un total de 19 capítulos de ingeniería.

Follow Us

## Accesos directos:

**Acerca del CDLIMA**

**Bolsa de Trabajo**

**Centro de Convenciones – CD LIMA**

**Directorio Telefónico CIP CDLima**

**Busqueda**

**Colegiación**

**Certificados**

**Formas de Pago**

**Tribunal de Ética**

**Bolsa de Trabajo**

## Libro de reclamaciones


## Nuestras políticas

**Política del Sistema Integrado de Gestión**

**Política de privacidad, protección y tratamiento de datos personales**

Detalles de contacto:

(+01) 202-5000

informes@ciplima.org.pe

**Calle Barcelona 240**
**San Isidro – Lima (Perú)**

Lunes a Viernes de 08:00 a 20:00 Horas

**Jhon Irvin Cisneros Carpio**

**De:** John Blademir Anaya Veramendi
**Enviado el:** viernes, 4 de abril de 2025 15:15
**Para:** Jhon Irvin Cisneros Carpio; TI - Eduardo Celso Prieto Hernández
**CC:** Ana Isidora Troncos Samaniego; Wilfredo Rivera Lazaro
**Asunto:** RE: SOLICITO APOYO EN VERIFICACIÓN TÉCNICA - CP N°002-2025-CR - SERVICIO DE SUSCRIPCIÓN PARA PLATAFORMA SIEM Y CYBER SOC

Estimados miembros del Comité de Selección,

En atención a su solicitud de apoyo para la revisión técnica de la formación académica del personal clave propuesto como Jefe de Proyectos en el CONCURSO PÚBLICO N°002-2025-CR, me permito indicar lo siguiente:

Luego de analizar lo indicado respecto a la formación académica del personal propuesto como Jefe de Proyectos, quien cuenta con el título de "Ingeniero de Computación y Sistemas", y contrastándola con lo requerido en las bases integradas que solicitan "Ingeniero titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Ingeniería Informática", considero lo siguiente:

La evaluación de equivalencias entre denominaciones de títulos profesionales requiere un análisis interpretativo que debe realizarse considerando el perfil profesional y las competencias desarrolladas en la carrera, no limitándose únicamente a la denominación literal.

Es importante señalar que, corresponde al Comité de Selección en estricto uso de sus facultades y autonomía determinar si la formación académica ofertada cumple con lo requerido en las bases integradas, teniendo en cuenta que en el Perú existe variedad en las denominaciones de carreras profesionales con competencias y campos de acción similares o equivalentes.

Desde el punto de vista técnico, se observa que la carrera de "Ingeniería de Computación y Sistemas" integra conocimientos tanto de computación como de sistemas, abarcando áreas como desarrollo de sistemas, sistemas de información, sistemas computacionales y gestión de TI, las cuales son concordantes con el perfil requerido. Sin embargo, corresponde al **Comité de Selección, en ejercicio de sus funciones y conforme a lo establecido en la normativa de contrataciones**, evaluar y determinar si la formación ofertada cumple con los requisitos establecidos en las bases, considerando la amplitud y diversidad de denominaciones académicas existentes en el país.

En ese sentido, la presente opinión se limita únicamente a brindar un alcance técnico respecto a la naturaleza de la carrera revisada, sin emitir juicio sobre la validez o cumplimiento de lo estipulado en las bases integradas, aspecto que queda bajo criterio exclusivo del Comité de Selección.

Quedo a su disposición para cualquier aclaración adicional.

Atentamente,

PERÚ
CONGRESO de la REPÚBLICA

John Blademir Anaya Veramendi
**Jefe del Área de Infraestructura Tecnológica**
(511) 311-7777
7564
(511) 997422117
janaya@congreso.gob.pe



---

**De:** Jhon Irvin Cisneros Carpio <jcisneros@congreso.gob.pe>
**Enviado:** viernes, 4 de abril de 2025 11:15
**Para:** John Blademir Anaya Veramendi <janaya@congreso.gob.pe>; TI - Eduardo Celso Prieto Hernández <eprieto@congreso.gob.pe>
**Cc:** Ana Isidora Troncos Samaniego <atroncos@congreso.gob.pe>; Wilfredo Rivera Lazaro <wrivera@congreso.gob.pe>
**Asunto:** SOLICITO APOYO EN VERIFICACIÓN TÉCNICA - CP N°002-2025-CR - SERVICIO DE SUSCRIPCIÓN PARA PLATAFORMA SIEM Y CYBER SOC

Estimados,
**EDUARDO CELSO PRIETO HERNÁNDEZ**
Jefe del Departamento de Tecnología de la Información

**JOHN BLADEMIR ANAYA VERAMENDI**
Jefe del Área de Infraestructura Tecnológica

Buenos días, es grato dirigirme a ustedes, en representación del Comité de Selección del **CONCURSO PÚBLICO N°002-2025-CR,** para el **SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA**, para solicitar su apoyo en la revisión, en lo respecta al aspecto técnico, de una oferta presentada en el procedimiento de selección, la cual se encuentra en etapa de calificación de ofertas. Esta solicitud se realiza en merito a lo establecido en el numeral 46.4 del artículo 46 del Reglamento de la Ley de Contrataciones del Estado, la cual precisa lo siguiente: *"Durante el desempeño de su encargo, **el comité de selección está facultado para solicitar el apoyo que requiera de las dependencias o áreas pertinentes de la Entidad**, las que están obligadas a brindarlo bajo responsabilidad."*

Al respecto, de acuerdo al numeral 3.2 de la Sección Especifica de las bases integradas del CONCURSO PÚBLICO N°002-2025-CR, se solicita al postor, acreditar dentro de su oferta la siguiente formación académica para el personal clave propuesto como jefe de Proyectos:

| | |
|---|---|
| **B.3** | **CALIFICACIONES DEL PERSONAL CLAVE** |
| **B.3.1** | **FORMACIÓN ACADÉMICA** |
| | Requisitos:<br>Jefe de Proyectos:<br><br>○ Ingeniero titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Ingeniería Informática. Con colegiatura vigente al realizar el servicio. |

Sobre eso, en la oferta presentada se ha propuesto un personal clave con una formación académica relacionada a lo requerido por en las bases integradas y el requerimiento, lo cual se adjunta al presente correo electrónico.

En ese sentido, agradeceremos su apoyo con la revisión del punto mencionado de la oferta del postor, en el plazo máximo de un (01) día hábil contabilizados del día siguiente de recibida la presente solicitud, remitiendo para dicho

caso, el sustento correspondiente de la revisión técnica respecto a la formación académica del personal clave requerido en las bases y la ofertada por el postor.

Atentamente,

PERÚ
CONGRESO de la REPÚBLICA

**Jhon I. Cisneros Carpio**
Especialista en Contrataciones Públicas
Área de Programación y Gestión de Adquisiciones
Departamento de Abastecimiento
311-7777 anexo 6680
jcisneros@congreso.gob.pe

## Jhon Irvin Cisneros Carpio

**De:** John Blademir Anaya Veramendi
**Enviado el:** miércoles, 2 de abril de 2025 11:41
**Para:** Jhon Irvin Cisneros Carpio; TI - Eduardo Celso Prieto Hernández
**CC:** Wilfredo Rivera Lazaro; Analiz del Milagro Tantalean Colan; Ana Isidora Troncos Samaniego
**Asunto:** RE: SOLICITO APOYO EN VERIFICACIÓN OFERTAS - CP N°002-2025-CR - SERVICIO DE SUSCRIPCIÓN PARA PLATAFORMA SIEM Y CYBER SOC
**Datos adjuntos:** Validación OFERTASCIBER SOC[R].pdf

Estimados miembros del Comité de Selección,

Reciban un cordial saludo.

En atención a lo solicitado en el correo electrónico precedente, y conforme a lo dispuesto en el numeral 46.4 del Reglamento de la Ley de Contrataciones del Estado, se **remite la Verificación de Cumplimiento** correspondiente a la revisión técnica de la oferta presentada por el postor en el marco del **Concurso Público N.º 002-2025-CR**, referido al servicio de suscripción para una plataforma de correlacionador de eventos (SIEM) y Cyber SOC delegada tipo SOAR.

Se adjunta la verificación de los documentos presentados en relación con lo requerido en el numeral 7.1 y numeral 7.5 literal e) del numeral 2.2.1.1 de las Bases, así como la revisión adicional del documento técnico presentado voluntariamente por el postor, el cual permitió verificar técnicamente el cumplimiento de los términos de referencia.

Quedamos atentos ante cualquier consulta adicional.

Atte.

PERÚ
CONGRESO de la REPÚBLICA

John Blademir Anaya Veramendi
**Jefe del Área de Infraestructura Tecnológica**
(511) 311-7777
7564
(511) 997422117
janaya@congreso.gob.pe



---

**De:** Jhon Irvin Cisneros Carpio <jcisneros@congreso.gob.pe>
**Enviado:** martes, 25 de marzo de 2025 16:31
**Para:** TI - Eduardo Celso Prieto Hernández <eprieto@congreso.gob.pe>; John Blademir Anaya Veramendi <janaya@congreso.gob.pe>
**Cc:** Wilfredo Rivera Lazaro <wrivera@congreso.gob.pe>; Analiz del Milagro Tantalean Colan <atantalean@congreso.gob.pe>; Ana Isidora Troncos Samaniego <atroncos@congreso.gob.pe>

**Asunto:** SOLICITO APOYO EN VERIFICACIÓN OFERTAS - CP N°002-2025-CR - SERVICIO DE SUSCRIPCIÓN PARA PLATAFORMA SIEM Y CYBER SOC

Estimados,
**EDUARDO CELSO PRIETO HERNÁNDEZ**
Jefe del Departamento de Tecnología de la Información

**JOHN BLADEMIR ANAYA VERAMENDI**
Jefe del Área de Infraestructura Tecnológica

Buenas tardes, es grato dirigirme a ustedes, en representación del Comité de Selección del **CONCURSO PÚBLICO N°002-2025-CR,** para el **SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA**, para solicitar su apoyo en la revisión, en lo respecta al aspecto técnico, de una oferta presentada en el procedimiento de selección. Esta solicitud se realiza en merito a lo establecido en el numeral 46.4 del articulo 46 del Reglamento de la Ley de Contrataciones del Estado, la cual precisa lo siguiente: *"Durante el desempeño de su encargo, **el comité de selección está facultado para solicitar el apoyo que requiera de las dependencias o áreas pertinentes de la Entidad**, las que están obligadas a brindarlo bajo responsabilidad."*

Al respecto, de acuerdo al literal e) del numeral 2.2.1.1 de la Sección Especifica de las bases integradas del CONCURSO PÚBLICO N°002-2025-CR y, al numeral 7.5 de los términos de referencia, se solicita al postor, acreditar dentro de su oferta lo siguiente:

> El Postor dentro de su propuesta, deberá acreditar mediante la presentación de catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales y/o capturas de pantalla de las plataformas en funcionamiento, el cumplimiento de los siguientes componentes:[11]
>
> Compatibilidad con sistemas operativos especificados, integración con fuentes de datos de seguridad (firewalls, antivirus, correo, directorio activo, componentes de red), autenticación de dos factores (2FA), protocolos de comunicación segura, aislamiento del agente (sin conexiones entrantes ni control remoto), coadministración basada en roles (propietario, visualizador, resolutor de incidentes), capacidades avanzadas de detección y respuesta (SOAR) integradas con MITRE ATT&CK, reducción de la superficie de ataque mediante pruebas de penetración y priorización de vulnerabilidades, monitoreo 24x7 de eventos de seguridad con alertas en tiempo real, respuesta automatizada a incidentes (aislamiento de hosts comprometidos, remediación de amenazas), certificaciones internacionales (ISO/IEC 27001, 27017, 27018, CSA STAR, SOC 3), generación de reportes (inventario, vulnerabilidades, eventos detectados), modalidad SaaS desde un SOC Data Center certificado, capacidad de análisis predictivo mediante Cyber Threat Intelligence (dark web, día 0/1 día), cumplimiento de normativas internacionales (ISO, NIST, STIG).

Por lo cual, el postor presento la documentación técnica (capturas de pantallas) adjunta al presente correo electrónico, para acreditar dicho requisito exigido. Asimismo, a pesar de no ser un requisito obligatorio en la presentación de la oferta, el postor presento documento técnico para acreditar el cumplimiento de la primera viñeta del numeral 7.1 de los términos de referencia, por lo que, debido a que dicho documento forma parte de la oferta, este deberá ser verificado también, de tal forma que no se identifiquen incongruencias, contradicciones u ambigüedades con los términos de referencia en ambas verificaciones.

> **7.1. ARQUITECTURA DE LA PLATAFORMA DE DETECCIÓN Y RESPUESTA**
> - El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoría de tipo SOC 2 y SOC 3[2] para los productos de detección y respuesta ofertados.

En ese sentido, agradeceremos su apoyo con la revisión de los puntos mencionados de la oferta del postor, en el plazo máximo de dos (02) días hábiles contabilizados del día siguiente de recibida la presente solicitud.

Atentamente,

PERÚ
CONGRESO de la REPÚBLICA

**Jhon I. Cisneros Carpio**
Especialista en Contrataciones Públicas
Área de Programación y Gestión de Adquisiciones
Departamento de Abastecimiento
311-7777 anexo 6680
jcisneros@congreso.gob.pe

**Verificación de Cumplimiento Oferta:**

**CONCURSO PÚBLICO N°002-2025-CR, para el SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPÚBLICA**

**7.5. PRESENTACION OBLIGATORIA DENTRO DE LA PROPUESTA:**

El Postor dentro de su propuesta, deberá acreditar mediante la presentación de catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales y/o capturas de pantalla de las plataformas en funcionamiento, el cumplimiento de los siguientes componentes:
Compatibilidad con sistemas operativos especificados, integración con fuentes de datos de seguridad (firewalls, antivirus, correo, directorio activo, componentes de red), autenticación de dos factores (2FA), protocolos de comunicación segura, aislamiento del agente (sin conexiones entrantes ni control remoto), coadministración basada en roles (propietario, visualizador, resolutor de incidentes), capacidades avanzadas de detección y respuesta (SOAR) integradas con MITRE ATT&CK, reducción de la superficie de ataque mediante pruebas de penetración y priorización de vulnerabilidades, monitoreo 24x7 de eventos de seguridad con alertas en tiempo real, respuesta automatizada a incidentes (aislamiento de hosts comprometidos, remediación de amenazas), certificaciones internacionales (ISO/IEC 27001, 27017, 27018, CSA STAR, SOC 3), generación de reportes (inventario, vulnerabilidades, eventos detectados), modalidad SaaS desde un SOC Data Center certificado, capacidad de análisis predictivo mediante Cyber Threat Intelligence (dark web, día 0/1 día), cumplimiento de normativas internacionales (ISO, NIST, STIG).

| N° | Requisito | Solicitado | Cumplimiento | Pagina/Sustento | URL/Evidencia de Sustento |
|---|---|---|---|---|---|
| 1 | Compatibilidad con sistemas operativos especificados | • La plataforma deberá soportar mínimamente las siguientes plataformas de sistemas operativos Windows Server 2012 R2 (32-bit / 64-bit), Windows Server 2016 / 2019 (32-bit / 64-bit), Windows Server 2022 (32-bit / 64-bit), Centos 7 and greater, Red Hat 8 and 9. | CUMPLE | 1 de 33<br>2 de 33 | (SUSTENTO N°1)<br>URL: https://www.rocketcyber.com/faqs/ |
| 2 | Integración con fuentes de datos de seguridad (firewalls, antivirus, correo, directorio activo, componentes de red) | • La plataforma debe integrar capacidades de SIEM Less para el monitoreo y correlacionamiento de eventos de seguridad de hosts, firewalls, antivirus, directorio activo, correo electrónico y/o componentes de red, incorporando la detección de infracciones basadas en las técnicas de Mitre Attack, la actividad y los servicios de la red, las herramientas sospechosas y la detección de archivos maliciosos para brindar una solución de seguridad integral. | CUMPLE | 2 de 33 a la<br>7 de 33 | (SUSTENTO N°2A):<br>URL: https://www.rocketcyber.com/products/managed-soc/<br>(SUSTENTO N°2B):<br>URL: https://www.rocketcyber.com/appstore/ |
| 3 | Autenticación de dos factores (2FA) | • La plataforma debe admitir la autenticación de dos factores (2FA) para salvaguardar el acceso a la consola. | CUMPLE | 7 de 33 a la<br>8 de 33 | (SUSTENTO N°3):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/account/securing-your-account-with-two-factor-authentication-2fa.html |
| 4 | Protocolos de comunicación segura | • La plataforma debe garantizar la seguridad de las comunicaciones usando el protocolo TLS v1.2 | CUMPLE | 8 de 33 a la<br>9 de 33 | (SUSTENTO N°4):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/rocketcyber-managed-soc-agent-architecture-and-capabilities.htm |
| 5 | Aislamiento del agente (sin conexiones entrantes ni control remoto) | • La plataforma debe contar con capacidades de respuesta ante ataques en curso, aislando dispositivos en la red que tengan instalado un agente, el aislamiento del host se realizará como consecuencia de un análisis y/o activación automática de un playbook de respuesta a incidentes para evitar la propagación de código malicioso al impedir que una máquina vulnerada se comunique con otros dispositivos de red en internet o la red del cliente. La máquina aislada mantendrá la conectividad con la plataforma correspondiente y permitirá que el Data Center SOC o equipo responsable en la institución reconecten el dispositivo. | CUMPLE | 9 de 33 a la<br>10 de 33 | (SUSTENTO N°5):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/managed-soc-incident-response.htm |
| 6 | Coadministración basada en roles (propietario, visualizador, resolutor de incidentes) | • La plataforma debe presentarse como un sistema integrado tipo SOAR integrando tecnologías y plataformas requeridas que se gobiernen desde una sola consola de orquestación automatizada con acceso basado en roles que permita la COADMINISTRACIÓN por parte del equipo del Congreso de la Republica. | CUMPLE | 11 de 33 a la<br>12 de 33 | (SUSTENTO N°6A):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/getting_started-with-rocketcyber.htm<br>(SUSTENTO N°6B):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/roles-and-access-permissions-in-rocketcyber.html |

PERÚ
CONGRESO
REPÚBLICA

Firmado digitalmente por:
ANAYA VERAMENDI John
Blademir FAU 20161749126 hard
Motivo: Soy el autor del
documento
Fecha: 02/04/2025 11:35:21-0500

| N° | Requisito | Solicitado | Cumplimiento | Pagina/Sustento | URL/Evidencia de Sustento |
|---|---|---|---|---|---|
| 7 | Capacidades avanzadas de detección y respuesta (SOAR) integradas con MITRE ATT&CK | • La plataforma de Cyber SOC debe integrar a través del agente capacidades de detección avanzada de infracciones reconociendo tácticas, técnicas y procedimientos (TTP) del adversario de acuerdo con el marco MITRE ATT&CK. | CUMPLE | 12 de 33 a la 14 de 33 | (SUSTENTO N°7A):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/overview/rocketcyber-native-capabilities.html?Highlight=ADVANCED%20BREACH%20DETECTION<br>(SUSTENTO N°7B):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/getting_started-with-rocketcyber.htm<br>(SUSTENTO N°7C):<br>URL: https://www.microsoft.com/es-mx/security/business/security-101/what-is-a-security-operations-center-soc |
| 8 | Reducción de la superficie de ataque mediante pruebas de penetración y priorización de vulnerabilidades | • La solución propuesta para este escenario tiene por objetivo añadir capacidades de prevención proactiva contra ataques cibernéticos a la plataforma de Cyber SOC delegada a través de la reducción proactiva y continua de la superficie de ataque externa e interna en la entidad. | CUMPLE | 14 de 33 a la 17 de 33 | (SUSTENTO N°8A):<br>URL: https://www.vonahi.io/<br>(SUSTENTO N°8B):<br>URL: https://www.secpod.com/risk-prioritization-real/ |
| 9 | Monitoreo 24x7 de eventos de seguridad con alertas en tiempo real | • La plataforma base tipo SOAR debe permitir la integración con la infraestructura de TI y seguridad existente, logrando que la plataforma administrada por el equipo de analistas de SOC del fabricante identifique rápidamente actividades maliciosas y sospechosas en los principales vectores de amenazas críticas: endpoint, red y nube, para brindar una defensa avanzada contra ciberamenazas las 24 horas, los 7 días de la semana durante el tiempo que dure la suscripción. | CUMPLE | 17 de 33 a la 19 de 33 | (SUSTENTO N°9):<br>URL: https://www.rocketcyber.com/products/managed-soc/ |
| 10 | Respuesta automatizada a incidentes (aislamiento de hosts comprometidos, remediación de amenazas) | La plataforma debe contar con capacidades de respuesta y remediación a través del agente, logrando ejecutar la eliminación de archivos, eliminación de claves y valores del registro, terminación de procesos, desinstalación de software, parada de servicios, eliminación de tareas programadas. | CUMPLE | 19 de 33 a la 21 de 33 | (SUSTENTO N°10):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/managed-soc-incident-response.htm |
| 11 | Certificaciones internacionales (ISO/IEC 27001, 27017, 27018, CSA STAR, SOC 3) | • La plataforma de Cyber SOC delegada debe ser provista en modalidad de Software as a Service (SaaS) desde un SOC Data Center que cuente con infraestructura certificada en conformidad con al menos dos (02) de las siguientes normas ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM v4.0. | CUMPLE | 21 de 33 a la 23 de 33 | (SUSTENTO N°11A):<br>URL: https://www.kaseya.com/download/13538/?tmsty=16835766<br>2 (SUSTENTO N°11B):<br>URL: https://www.kaseya.com/trust-center/earning-your-trust/<br>(SUSTENTO N°11C):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/rocketcyber-managed-soc-agent-architecture-and-capabilities.htm<br>(SUSTENTO N°11D):<br>URL: https://aws.amazon.com/es/compliance/iso-certified/ |
| 12 | Generación de reportes (inventario, vulnerabilidades, eventos detectados) | • La plataforma debe permitir crear reportes bajo demanda y programarlos para su envío automático al correo electrónico.<br>• La plataforma debe permitir la creación de informes de inventario e informes ejecutivos hasta con una antigüedad de noventa (90) días. | CUMPLE | 23 de 33 a la 27 de 33 | (SUSTENTO N°12A):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/overview/reporting-overview.html?Highlight=report<br>(SUSTENTO N°12B):<br>URL: https://docs.secpod.com/docs/how-to-create-a-custom-report-in-sanernow/<br>(SUSTENTO N°12C):<br>URL: https://www.secpod.com/saner-posture-anomaly/<br>(SUSTENTO N°12D):<br>URL: https://www.secpod.com/risk-based-vulnerability-management/ |

| N° | Requisito | Solicitado | Cumplimiento | Pagina/Sustento | URL/Evidencia de Sustento |
|---|---|---|---|---|---|
| 13 | Modalidad SaaS desde un SOC Data Center certificado | • La plataforma deberá ser presentada en modalidad de Software as a Service (SaaS) sin requerir de infraestructura física adicional para su normal desempeño.<br>• La plataforma de Cyber SOC delegada debe ser provista en modalidad de Software as a Service (SaaS) desde un SOC Data Center que cuente con infraestructura certificada en conformidad con al menos dos (02) de las siguientes normas ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM v4.0. | CUMPLE | 27 de 33 a la 28 de 33 | (SUSTENTO N°13A):<br>URL: https://help.rocketcyber.kaseya.com/help/Content/general/rocketcyber-managed-soc-agent-architecture-and-capabilities.htm<br>(SUSTENTO N°13B):<br>URL: https://aws.amazon.com/es/compliance/iso-certified/ |
| 14 | Capacidad de análisis predictivo mediante Cyber Threat Intelligence (dark web, día 0/1 día) | • La plataforma de Cyber SOC deben incluir funciones de búsqueda a través de sistemas de cacería de amenazas avanzadas y feeds de búsqueda de inteligencia de amenazas automatizadas | CUMPLE | 28 de 33 a la 32 de 33 | (SUSTENTO N°14A):<br>URL: https://outpost24.com/products/cyber-threat-intelligence/<br>(SUSTENTO N°14B):<br>URL: https://outpost24.com/wp-content/uploads/2023/10/Outpost24_ThreatCompass_2023.pdf<br>(SUSTENTO N°14C):<br>URL: https://docs.secpod.com/docs/saner cvem-patch-management-user-guide/ |
| 15 | Cumplimiento de normativas internacionales (ISO, NIST, STIG) | • La plataforma deberá implementar una gestión avanzada de vulnerabilidades, configuraciones alineadas a cumplimiento normativo como ISO y NIST además los activos en busca de anomalías. | CUMPLE | 29 de 33 a la 32 de 33 | (SUSTENTO N°15):<br>URL: https://docs.secpod.com/docs/overview-of-sanercvem-advanced-vulnerability-management/ |

**7.1. ARQUITECTURA DE LA PLATAFORMA DE DETECCIÓN Y RESPUESTA**

• El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoria de tipo SOC 2 y SOC 32 para los productos de detección y respuesta ofertados.

| N° | Requisito | Solicitado | Cumplimiento | Pagina/Sustento | URL/Evidencia de Sustento |
|---|---|---|---|---|---|
| 1 | El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoría de tipo SOC 2 para los productos de detección y respuesta ofertados. | • La plataforma deberá soportar mínimamente las siguientes plataformas de sistemas operativos Windows Server 2012 R2 (32-bit / 64-bit), Windows Server 2016 / 2019 (32-bit / 64-bit), Windows Server 2022 (32-bit / 64-bit), Centos 7 and greater, Red Hat 8 and 9. | CUMPLE | Páginas 046-057 (Documento: Traducción Certificada TC N.° 0777-2025) | Informe del Auditor de Servicio Independiente sobre la Descripción de la Gestión del Sistema - SOC 2 Tipo 2 de Kaseya US, LLC para el periodo del 1 de junio de 2023 al 31 de mayo de 2024 |
| 2 | El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoría de tipo SOC 3 para los productos de detección y respuesta ofertados. | • La plataforma debe integrar capacidades de SIEM Less para el monitoreo y correlacionamiento de eventos de seguridad de hosts, firewalls, antivirus, directorio activo, correo electrónico y/o componentes de red, incorporando la detección de infracciones basadas en las técnicas de Mitre Attack, la actividad y los servicios de la red, las herramientas sospechosas y la detección de archivos maliciosos para brindar una solución de seguridad integral. | CUMPLE | Páginas 058-063 (Documento: Traducción Certificada TC N.° 0779-2025) | Informe del Auditor de Servicio Independiente sobre la Descripción de la Gerencia del Sistema - SOC 3 de Kaseya US, LLC para el periodo del 1 de junio de 2023 al 31 de mayo de 2024 |