"SERVICIO DE ASESORÍA DE AUDITORIA DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN EN LA CMAC MAYNAS S.A"

TERMINOS DE REFERENCIA

1. OBJETO DEL PROCESO

Contratar a un profesional o empresa especializada, con experiencia comprobada en Auditoría de Ciberseguridad y Auditoría de Seguridad de la Información en entidades del sistema financiero, para brindar el servicio profesional a la Gerencia de Auditoría Interna de la CMAC Maynas S.A., denominado "Servicio de Auditoría de Gestión de Ciberseguridad y Auditoría de Seguridad de la Información", de conformidad con la normativa SBS vigente y normas aplicables.

El servicio se desarrollará bajo la modalidad de apoyo técnico especializado a la Gerencia de Auditoría Interna (co-sourcing), en el marco del Plan Anual de Auditoría aprobado por el Directorio.

2. ESPECIFICACIONES Y OBJETIVO DEL SERVICIO

Evaluar de manera independiente el cumplimiento de la Resolución SBS N.° 11699-2008 – Reglamento de Auditoría Interna (Artículo 6, literal "d"), normas concordantes y complementarias, así como la eficacia del sistema de control interno y la gestión de riesgos no financieros de naturaleza tecnológica, utilizando como marco de referencia COBIT 2019.

La evaluación tendrá especial énfasis en los riesgos no financieros asociados a ciberseguridad, seguridad de la información, continuidad del negocio y gestión de bases de datos.

3. ALCANCE DE LA EVALUACIÓN

El período a evaluar será la información concerniente del 01.ENE.2025 hasta el 28.FEB.2026

La responsabilidad por la planificación, supervisión, conclusiones e informe final de Auditoría será indelegable y permanecerá en la Gerencia de Auditoría Interna.

Gerente de Auditoría Interna VºBº Carlos Alberto Mori Chávez CMAC MAYNAS S.A.

3.1. Auditoría de Ciberseguridad:

El servicio comprenderá lo siguiente:

- Evaluar el cumplimiento de la Resolución SBS Nº 504-2021 y sus modificatorias, en lo relacionado con la Ciberseguridad.
- Evaluar la gestión de amenazas y vulnerabilidades, incluyendo:
  - Procesos de identificación, análisis y tratamiento.
  - Gestión de parches y remediación.
- Revisar incidentes de ciberseguridad reportados en el periodo evaluado y la eficacia de la respuesta.
- Evaluar la efectividad del monitoreo de seguridad, incluyendo SOC, SIEM u otras herramientas implementadas.
- Evaluar la implementación y seguimiento de recomendaciones derivadas de auditorías anteriores.
- Identificar debilidades de control que pueden impactar la confidencialidad, integridad y disponibilidad de la información.
- Evaluar el nivel de madurez de ciberseguridad de la institución, utilizando marcos de referencia NIST CSF, ISO/IEC 27001.
- Elaborar un plan de mejora de capacidades de ciberseguridad, priorizando acciones para cerrar brechas.

3.2. El servicio de Auditoría de Seguridad de la Información comprenderá, lo siguiente:

El servicio comprenderá lo siguiente:

- Evaluar el cumplimiento de la Resolución SBS Nº 504-2021 en materia de Seguridad de la Información.
- Evaluar el marco normativo.
- Revisar la gestión de accesos lógicos y segregación de funciones.
- Evaluar la metodología de gestión de riesgos de seguridad de la información.
- Evaluar el seguimiento de planes de acción derivados de auditorías previas.

3.3. Actividad Complementaria

- Retroalimentación general de hasta 04 horas académicas en Gestión de Ciberseguridad y Seguridad de la Información al personal de Gerencia de Auditoría Interna, la cual se realizará luego de la emisión del informe final de auditoría.
- Transferencia de conocimiento metodológico general al personal de la Gerencia de Auditoría Interna, sin participación en la ejecución, elaboración ni aprobación de informes de Auditoría Interna.

3.4. Resultados esperados del servicio

Los resultados esperados estarán orientados exclusivamente al fortalecimiento del proceso de auditoría interna, sin involucrar funciones de gestión u operación, e incluirán lo siguiente:

- Identificación y evaluación de riesgos tecnológicos y de seguridad.
- Evaluación del cumplimiento normativo y del sistema de control interno de TI.
- Emisión de recomendaciones orientadas a la mejora del control interno y mitigación de riesgos.

El alcance se limita a la evaluación, sin involucrar la operación directa de sistemas criticos ni la gestión de activos que afecten la continuidad del negocio, siendo su finalidad fortalecer el proceso de Auditoría Interna.

4. ENTREGABLES

a) Plan de Trabajo aprobado (dentro de 3 días hábiles de la firma del contrato)
   - Contendrá cronograma, alcance detallado, metodología de auditoria y responsables de cada actividad.
b) Informe Técnico preliminar (dentro de 20 días hábiles)
c) Informe Técnico Final detallado de hallazgos con nivel de criticidad. (dentro de 30 días hábiles)
d) Matriz de Riesgos identificados con nivel de criticidad.
e) Evidencias técnicas y papeles de trabajo.
   - Documentación soporte de pruebas, verificaciones, Logs, capturas y análisis utilizados para la auditoria.
f) Recomendaciones priorizadas.
   - Acciones correctivas y preventivas, con indicación de prioridad, responsables y plazo sugerido de implementación.
g) Sesiones de explicación técnica de los resultados a las áreas involucradas incluyendo:
   - Sustento de cada hallazgo
   - Evidencias Técnicas
   - Nivel de riesgo asignado
   - Recomendaciones propuestas.
h) Informe que presenta el nivel de madurez de ciberseguridad, brechas detectadas y plan de mejora con acciones priorizadas y cronograma de implementación.

Asimismo, las sesiones deberán realizarse en coordinación con la Gerencia de Auditoría Interna, quien supervisará y validará las explicaciones brindadas.

El Informe Final consolidado será emitido por la Gerencia de Auditoría Interna, incorporando y validando los resultados del apoyo técnico especializado.

5. PERFIL REQUERIDO

Conforme al Reglamento SBS N.° 11699-2008, el proveedor y el equipo asignado al servicio deberán cumplir con los siguientes requisitos mínimos de idoneidad, experiencia y competencias.

- Formación académica
  a) Profesional universitario titulado en Ingeniería de Sistemas, Informática, Ciberseguridad, Seguridad de la información o disciplinas afines.
- Experiencia profesional
  a) Experiencia mínima de 3 años en auditoria de sistemas, seguridad de la información o ciberseguridad.
  b) Experiencia comprobable en:
     - Evaluación de controles de seguridad de la información y tecnología.
     - Elaboración de informes técnicos de auditoria, con hallazgos, riesgos y recomendaciones.
     - Aplicación de marcos normativos y estándares aplicables a entidades supervisadas (ISO/IEC 27001, NIST CSF, COBIT, PCI-DSS según corresponda).
- Certificaciones Profesionales
  a) CISA (Certified Information System Auditor) o equivalente reconocido internacionalmente.
  b) ISO/IEC 27001 Lead Auditor será requerido cuando la auditoria incluya la revisión del sistema de gestión de seguridad de la información.
- Competencias Técnicas
  a) Conocimiento del marco regulatorio SBS aplicable a TI y ciberseguridad, incluyendo Resolución SBS 504-2021 y Reglamento SBS 11699-2008.
  b) Capacidad para realizar evaluaciones técnicas y de control, revisión de Logs, gestión de vulnerabilidades y pruebas de cumplimiento.
  c) Capacidad para evaluar madurez de ciberseguridad y seguridad de la información, y para elaborar planes de mejora de capacidades.
- Independencia y ética profesional
  a) El auditor debe ser independiente y no presentar conflictos de interés con la entidad auditada.
  b) La responsabilidad por la planificación, supervisión, conclusiones e informe final es indelegable, de acuerdo con el Reglamento SBS 11699-2008.
- Para el caso de empresa deberá contar en su equipo de trabajo con personal que cuente con dicho requisito y experiencia. (deseable línea arriba).
- Experiencia: En evaluaciones similares en Auditoria de la Gestión de Ciberseguridad y Gestión de Seguridad de la Información (indispensable).
- Conocimiento comprobado en:
  - COBIT 2019
  - Gestión de riesgos no financieros
  - Ciberseguridad y seguridad de la información
  - Continuidad del negocio (BCP/DRP)
- Para el caso de empresa, deberá contar con un equipo que cumpla con los requisitos señalados.

Gerente de Auditoría Interna VºBº Carlos Alberto Moñ Chávez CMAC MAYNAS S.A.

6. LUGAR DE EJECUCÓN DEL SERVICIO

En la Sede Principal de la CMAC Maynas S.A. ubicada en la Calle Requena N° 303-307 – Iquitos.

7. PLAZO DE EJECUCIÓN

La asesoría requiere un mínimo de 30 días hábiles (incluye trabajo de campo y elaboración del informe final)

Este trabajo de campo será ejecutado por el personal propuesto para el servicio, no pudiendo ser sustituido bajo ninguna circunstancia, caso contrario, será causal de resolución de contrato por incumplimiento.

8. PRINCIPIOS GENERALES DE LA AUDITORÍA

El postor que se adjudique la Buena Pro, deberá tener en cuenta la importancia y delicada labor que prestará por lo que deberá obligatoriamente a observar las normas de conducta profesional y personal tales como: objetividad, probidad, transparencia, diligencia, reserva, legalidad, ética, respeto, honestidad, presunción de licitud, veracidad, pulcritud y flexibilidad.

9. OBLIGACIÓN DE RESERVA DE INFORMACIÓN

El consultor guardará reserva respecto de las actividades y acciones encomendadas, así como de la información privilegiada que concierne en el ejercicio de su actividad, no revelando en forma oral o escrita, hechos, datos, procedimientos y documentación no autorizada o confidencial de acuerdo a ley.

10. INDEPENDENCIA, ECLUSIÓN Y CONFLICTO DE INTERES

- El proveedor actuará con plena independencia a las áreas auditadas.
- El proveedor deberá declarar no tener conflicto de interés ni haber participado en el desarrollo de los sistemas evaluados.

11. CLAUSULA DE PENALIDADES

11.1. PENALIDAD POR RETRASO EN ENTREGA DE INFORMES

Por cada día calendario de retraso en la entrega de los informes técnicos, matriz de riesgos o evidencias.

- Retraso injustificado en la entrega del informe final: 0.5% del monto contractual por cada día hábil de retraso, hasta un máximo del 10%.
- Incumplimiento del alcance aprobado: resolución del contrato sin pago pendiente.
- Vulneración de la confidencialidad: resolución inmediata del contrato y acciones legales correspondientes.

Gerente de Auditoría Interna VºBº Carlos Alberto Mori Chávez CMAC MAYNAS S.A.

11.2. PENALIDAD POR INCUMPLIMIENTO EN SUSTENTACIÓN TÉCNICA

Si el proveedor:

- No realiza las sesiones de explicación comprometidas, o
- No absuelve observaciones técnicas del plazo establecido.

Se aplicará una penalidad equivalente al:

- 1% del monto contractual por cada incumplimiento.

12. PLAN DE TRABAJO

El postor ganador de la Buena Pro, deberá coordinar con la Gerencia de Auditoria Interna a fin de presentar un Plan de Trabajo, el cual incluya los objetivos y los procedimientos a utilizarse en el desarrollo del Trabajo de Campo.

13. FORMA DE PAGO

- Pago inicial equivalente al 40% del monto adjudicado a la presentación y aprobación del Plan de Trabajo (Plan y Programa de Auditoría) por parte del Área Usuaria.
- Pago final equivalente al 60% del monto adjudicado a la presentación, del informe final del servicio de asesoría brindado por parte del área usuaria.

* La aprobación y conformidad del servicio estará a cargo de la Gerencia de Auditoría Interna (GAI) de la CMAC Maynas S.A,

ANEXO N° 03

FORMATO DE SOLICITUD DE ADQUISICIONES Y CONTRATACIONES

FORMATO SOLICITUD DE GASTO PRESUPUESTARIO NO PREVISTO 1/							
1. AREA USUARIA	GERENCIA DE AUDITORÍA INTERNA						
2. DOCUMENTO DE APROBACIÓN	PLAN ANUAL DE AUDITORÍA 2026						
3. DESCRIPCIÓN DEL GASTO	CONTRATACIÓN DE SERVICIO DE CONSULTORÍA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD						
4. GASTO PREVISTO EN EL PIA 2/	SÍ	X	NO				
5. GASTO PREVISTO EN EL PAAC 3/	SÍ	X	NO				
6. REQUIERE INCLUSION EN EL PAAC	SÍ		NO	X			
7. VALOR REFERENCIAL	MONEDA	Soles	X	Dólares		Otro:	
	MONTO	S/ 40,000.00					
8. PLAZO DE EJECUCION DEL GASTO 4/	30	(días calendarios)					
9. MODALIDAD DEL PROCESO DE ADQUISICIONES Y CONTRATACIONES							
COMPRAS POR PROCESOS		COMPRAS EXCLUIDAS					
1° NIVEL (MONTOS > 5 UIT) 5/	S/ 40,000.00	COMPRA MENORES A 5 UIT					
2° NIVEL (MONTOS SIGNIFICATIVOS) 6/		COMPRAS DIRECTAS					
10. OBJETIVO DE LA SOLICITUD	Contratar a un profesional o empresa especializada, con experiencia comprobada en Auditoría de Ciberseguridad y Auditoría de Seguridad de la Información en entidades del sistema financiero, para brindar el servicio profesional a la Gerencia de Auditoría Interna de la CMAC Maynas S.A., denominado "Servicio de Auditoría de Ciberseguridad y Auditoría de Gestión de Riesgos de Seguridad de la Información", de conformidad con la normativa SBS vigente y normas aplicables.						
11. BENEFICIO / COSTO	El costo beneficio de la presente consultoría es que contribuirá al cumplimiento de los siguientes objetivos estratégicos: ➢ Optimizar gastos operativos. ➢ Facilitar el acceso a productos y servicios digitales. ➢ Brindar servicio omnicanales. ➢ Facilitar las ofertas personalizadas a clientes, automatizando e integrando marketing, ventas y servicios. Asimismo, la auditora junior recibirá retroalimentación y/o capacitación de la asesoría brindada por la empresa consultora. Por otra parte, se hace referencia al costo promedio incurridos entre los años 2022 al 2024, que asciende a S/ 52,215.00. **Fuente:** Registro de Compras - Información obtenida del SICMAC. Cabe precisar que, para la presente contratación de servicio de consultoría, no se realiza el análisis de punto de equilibrio, VAN y TIR, por no corresponder a proyectos de inversión.						

Gerente de Auditoría Interna
V°B°
Carlos Alberto Mori Chávez
CMAC MAYNAS S.A.

12. NOMBRE, FIRMA Y SELLO DEL RESPONSABLE DEL AREA USUARIA
Carlos Alberto Mori Chávez Gerente de Auditoría Interna

13. APROBACIONES / V°B°:						
LOGÍSTICA	PLANEAMIENTO Y DESARROLLO		GERENCIA CENTRAL		DIRECTORIO	
14. FECHA DE SOLICITUD	DIA		MES		AÑO	2026

Notas:

1/ Gastos no previstos en el Presupuesto Institucional Anual (PIA) y/o Plan Anual de Contrataciones y Adquisiciones (PAAC), por encima de la meta mensual aprobada, sin sustento previo ante el Directorio.

2/ Presupuesto Institucional Anual (PIA), aprobados por la Gerencia Mancomunada y el Directorio.

3/ Plan Anual de Contrataciones y Adquisiciones (PAAC), aprobados por la Gerencia Mancomunada y el Directorio.

4/ Teniendo en cuenta que los presupuestos aprobados se limitan a un ejercicio económico fiscal, los gastos comprometidos que superen el año se afectan al siguiente ejercicio económico.

5/ Compras no representan montos significativos, no requiere la designación de un comité de compras.

6/ Máximo nivel de adquisición o contratación, montos de compras significativos, requiere mayores controles y designación de un comité de compras y mayores formalidades.