ANEXO N° 02
FORMATO TERMINOS DE REFERENCIA PARA SERVICIOS EN GENERAL
(TDR SERVICIOS EN GENERAL)

ÓRGANO Y/O UNIDAD ORGÁNICA:	OFICINA DE TECNOLOGIAS DE INFORMACION
ACTIVIDAD DEL POI:	Implementación de controles, normas, procedimientos en el marco del Sistema de Gestión de Seguridad de Información. (RO.CO. TI.01)
DENOMINACIÓN DE LA CONTRATACIÓN:	Servicio de Implementación Controles de Ciberseguridad

1. FINALIDAD PÚBLICA

Garantizar la integridad, confidencialidad y disponibilidad de los sistemas de información y activos críticos del CONCYTEC, mediante la implementación de controles de ciberseguridad orientados a la mitigación de vulnerabilidades identificadas, en concordancia con el Sistema de Gestión de Seguridad de la Información y estándares internacionales como ISO 27001:2022.

2. OBJETIVO DE LA CONTRATACIÓN

Contratar el servicio especializado para la implementación de controles de ciberseguridad, orientado a la remediación de vulnerabilidades identificadas y priorizadas, a fin de reducir los riesgos de seguridad de la información en los activos críticos del CONCYTEC

3. ALCANCES Y DESCRIPCIÓN DE SERVICIO

El servicio comprende la remediación de veintisiete (27) vulnerabilidades identificadas en el Plan de Remediación de la Entidad, las cuales afectan a treinta y siete (37) activos de información, según detalle:

VULNERABILIDAD IDENTIFICADA	ACTIVOS AFECTADOS
Múltiples vulnerabilidades por Versión obsoleta de Servidor Apache	2
File Upload	3
Path Traversal o Directorio traversal	7
Path Traversal en phpMyAdmin	2
SQL injection	2
XSS - Cross Site Scripting	3
Uso de Sistema Operativo obsoleto	1
Ejecución de código remoto por versión de Wordpress Elementor	1
Fijación de sesiòn osCommerce 'oscid'	1
Denegación de servicios	3
Samba - Múltiples vulnerabilidades Críticas - RCE, EternalBlue, exploits disponibles - CVE-2017-7494, CVE-2017-7494, CVE-2020-1472, Ghost por servicio SMB en Domain Controller / RPC expuestos	1
VNC Exposición con credenciales con usuario "concytecdc" - CVE-2019-15689, CVE-2020-25712	1
SSH con Múltiples vulnerabilidades RCE con Exploits - CVE-2024-6387	1

LDAP de AD expuesto sin restricciones	1
BlueKeep RDP Exposure	1
Kerberos Exposure - Kerberoasting, Golden Ticket	1
HTTP Verb Tampering	1
WinRM Exposure	1
VMware Authentication Daemon - CVE-2021-21974	1
VMware ESXi 8.0.2 Sin Parches - Múltiples CVE 2023-2024	1
Slowloris DoS - denegación de servicio - CVE-2007-6750	1
Inyección (SQLi, XSS)	1

DESCRIPCIÓN DEL SERVICIO

ÍTEM	CANTIDAD	DESCRIPCIÓN DEL SERVICIO
1	**1**	Servicio de Implementación Controles de Ciberseguridad

- La modalidad de trabajo será remoto (las reuniones de trabajo y presentación de resultados en línea se realizará mediante teleconferencias y usando medios seguros para transferencia de información) y presencial de acuerdo las necesidades de seguridad requeridas por el CONCYTEC, quien establecerá el día y la hora
- La ejecución del servicio no debe causar daño alguno en el funcionamiento de los sistemas o en el desempeño de la red de la institución.
- El postor en coordinación con el personal del CONCYTEC, elaborarán los cronogramas para las sesiones de requerirse con el personal de a Oficina de Tecnologías de Información.
- El postor deberá indicar las herramientas, equipos y/o productos que utilizará durante la ejecución de la evaluación de seguridad y pruebas de penetración, en caso se utilice herramientas gratuitas, el postor las entregará a la institución.
- El postor deberá cumplir con la Política de Seguridad de la Información del CONCYTEC.

Actividades a desarrollar

El servicio debe solucionar las vulnerabilidades de ciberseguridad identificados y priorizadas del sus Plan de Remediación priorizados según cuadro indicado

ETAPA I: EJECUCIÓN DE LA REMEDIACIÓN: Aplicación de parches (Patching), endurecimiento de sistemas (Hardening), configuración de reglas en WAF/IPS y segmentación de red.

Objetivo Principal: Esta fase consiste en la aplicación directa de soluciones técnicas:
- Análisis técnico de vulnerabilidades priorizadas
- Aplicación de parches (patch management)
- Hardening de sistemas
- Implementación de controles compensatorios (WAF, IPS)
- Gestión de accesos (MFA, privilegios)
- Segmentación de red

Actividades mínimas que debe de realizar el contratista para el cumplimiento de la finalidad publica de la presente contratacion:

- Realizar un análisis exhaustivo de las vulnerabilidades priorizadas del cuadro presentado
- Revisar los Planes de Remedición y las acciones para mitigar los riesgos en cada vulnerabilidad y sobre los activos afectados.
- Realizar las reuniones de coordinación para identificar los permisos necesarios y los aspectos de seguridad necesaria para el desarrollo del servicio.,
- Realizar la Gestión de Parches (Patching): Aplicar parches de seguridad a sistemas operativos, aplicaciones, firmware y bases de datos, priorizando los críticos.
- Realizar el fortalecimiento de las Configuraciones (Hardening): Ajustar las configuraciones de seguridad por defecto, desactivar servicios innecesarios y eliminar cuentas predeterminadas.
- Implementación de Controles Compensatorios: De las Vulnerabilidades que han sido identificada por la OTI que será comunicado, entre otros establecer las reglas de WAF (Web Application Firewall) o IPS (Intrusion Prevention System) para proteger el sistema e implementaras en coordinación con la OTI en estos casos.
- Segmentación de Red: Aislar sistemas vulnerables o sensibles para limitar el movimiento lateral de un atacante previamente comunicado a la OTI si se pudiera presentar alguna situación de riesgo durante el servicio.
- Gestión de Identidades y Accesos: Implementar o reforzar la autenticación multifactor (MFA) y revisar los privilegios de usuario en las vulnerabilidades alguna de la vulnerabilidad identificada del cuadro lo requiera.
- Elaborar el Informe de Avance de la implementación de los controles y resolución de vulnerabilidades.

ETAPA II: VALIDACIÓN Y MEJORA CONTINUA: Verificación post-remediación mediante un nuevo análisis (Re-Testing) para confirmar la efectividad de los controles.

Objetivo principal: Una vez aplicadas las correcciones, se debe verificar su efectividad

- Re-testing de vulnerabilidades
- Validación de mitigación
- Generación de evidencias

Actividades mínimas que debe de realizar el contratista para el cumplimiento de la finalidad publica de la presente contratacion:

- **Verificación Post-Remediación:** Realizar nuevos análisis de todas las vulnerabilidades para confirmar que la mitigación fue efectiva y realizar el Informe de los resultados con las evidencias.
- **Elaboración de la Documentación:** Registrar todas las acciones tomadas para auditoría y cumplimiento normativo (como ISO 27001).
- **Fortalecimiento Capacidades:** Charla de seguridad para evitar que errores humanos reintroduzcan vulnerabilidades
- **Realizar el Informe Final de la Remediación de las Vulnerabilidades y presentación.**

Reglamentos técnicos, normas metrológicas y/o sanitarias

El Marco de Seguridad Cibernética (CSF) del NIST (Instituto Nacional de Estándares y Tecnología) debe estar alineado a los manuales de seguridad OSSTMM (Open Source Security Testing Methodology Manual) y OWASP Testing Guide version vigente.

4. REQUISITOS DEL PROVEEDOR Y/O PERSONAL PROPUESTO

Perfil del postor:

El postor deberá contar con los siguientes requerimientos como mínimo:

a) Persona Natural o Jurídica
b) Contar con RNP vigente

Experiencia del postor:

El postor deberá acreditar experiencia mínima de cinco (05) servicios ejecutados en seguridad de la información y/o ciberseguridad y/o análisis de vulnerabilidades y/o pruebas de penetración, en entidades públicas o privadas.

Para la prestación del servicio, el contratista debe de asignar el siguiente personal:

a) Experiencia del Personal Clave

Especialista en Seguridad de la Información

- Grado académico mínimo de bachiller de las carreras profesionales de ingeniería informática y/o ingeniería de sistemas y/o ingeniería computación y/o ingeniería electrónica y/o ingeniera de telecomunicaciones.
- Experiencia especifica mínima de dos (2) años en servicios vinculados a especialista y/o consultor y/o analista y/o profesional y/o asesor y/o apoyo y/o administrador de servicios de Seguridad de la Información y/o Ciberseguridad y/o Análisis de Vulnerabilidades y/o Hacking Ético y/o Pruebas de penetración (Pentesting) y/o Gestión de Riesgos de TI e ISO27001 ejecutados en instituciones públicas o privadas.

Certificaciones:

Como mínimo un (01) certificado oficial VIGENTE, en cualquiera de las siguientes certificaciones de seguridad:

- LPT Master (Licensed Penetration Tester - Master)
- CPENT (Certified Penetration Testing Professional)
- ECSA (Council Certified Security Analyst)
- CEH (Certified Ethical Hacker)
- CEH Practical (Certified Ethical Hacker)
- GPEN (GIAC Penetration Tester)
- GWAPT (Web Application Penetration Tester)
- CPTE (Certified Penetration Testing Engineer)
- CPEH (Certified Professional Ethical Hacker)
- CRTP (Certified Red Team Professional)
- CRTO (Certified Red Team Operator)
- OSCE (Offensive Security Certified Expert)
- OSCP (Offensive Security Certified Professional)
- OSWE (Offensive Security Web Expert).
- CSWAE (Certified Web Secure Application Engineer).
- eJPT (eLearn Junior Penetration Testing)
- eWPT (eLearn Web Penetration Testing)
- eWPTX (eLearn Web Application Penetration Tester eXtreme)
- eCPPT (Certified Professional Penetration Tester)

- ISO 27001 Foundation (I27001)
- ISO 22301 – Continuidad del Negocio
- ISO 31000 – Gestión de Riesgos
- LCSPC – Lead Cybersecurity Professional Certified
- CSFPC – Cybersecurity Foundation Professional Certified
- CRISC – Certified in Risk and Information Systems Control
- CRMA – Certified Risk Management Assurance
- CISM – Certified Information Security Manager
- CBCP – Certified Business Continuity Professional
- CRMP – Certified Risk Management Professional

5. LUGAR Y PLAZO DE PRETACION DEL SERVICIO

Lugar de prestación del servicio: El servicio se realizará de manera remota y en caso se requiera la presencia del postor se realizará a través de sesiones de trabajo previamente coordinadas con la Oficina de Tecnologías de la Información, en Av. Del Aire 485 – San Borja.

Plazo de prestación del servicio: La prestación del servicio se debe de realizar en cuarenta y cinco (45) días calendario, contados a partir del día siguiente de notificada la orden de servicio.

6. ENTREGABLES

La presente contratacion cuenta con tres (3) entregables, según el siguiente detalle:

Etapa	Entregables	Descripción	Plazo de entrega
Etapa I	**Primer entregable**	• Plan del Desarrollo servicio, Cronograma y metodología	A los 5 días calendario contados a partir del día siguiente de notificada la orden de servicio.
	Segundo entregable	• Informe de avance (Etapa I) • Evidencias de remediación (logs, capturas, reportes)	A los 20 días calendario contados a partir del día siguiente de notificada la orden de servicio.
Etapa II	**Tercer entregable**	• Documentación Técnica actualizada de las vulnerabilidades • Informe del Re Testing, Resultados de re-testing y documentación de controles implementados • Diapositivas del entrenamiento practico en ciberseguridad y de la Charla de Seguridad	A los 45 días calendario contados a partir del día siguiente de notificada la orden de servicio.

Sin perjuicio de otras obligaciones a su cargo, el contratista deberá entregar una versión digital final, datos procesados y estadísticas de monitoreo sin ninguna medida tecnológica efectiva ni sistema de autotutela, sin contraseña ni restricción, de acuerdo con los lineamientos establecidos por el Consejo Nacional de Ciencia, Tecnología e Innovación

(CONCYTEC) en relación con el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto.

Los informes y recomendaciones entregados al CONCYTEC deben encontrarse en español, a excepción de los reportes que puedan ser emitidos directamente por las herramientas utilizadas, los cuales servirán como anexos a los informes presentados.

7. LUGAR DE PRESENTACION DE LOS ENTREGABLES

El entregable debe ser presentado, a través de la Mesa de Partes Virtual (*): mesadepartes@concytec.gob.pe Para lo cual, el contratista debe de presentar por mesa de partes del CONCYTEC el entregable, según el siguiente detalle:

Presencial: Horario de atención: lunes a viernes de 8:00 a.m. a 4:15 p.m. Lugar: Av. Del Aire 485-San Borja
Digital: Mesa de Partes Digital - https://servicios.concytec.gob.pe/mesaPartesDigital/, encuentra habilitado durante las 24 horas del día.
La revisión de documentos en la mesa de partes digital se realizará en días hábiles entre las 8:00 a.m. a 4:15 p.m.

En caso del correo mesadepartes@concytec.gob.pe, solo estará habilitado para consultas sobre el estado de las solicitudes remitidas por este canal (mesa de partes), como para ingreso excepcional de algunos documentos que no puedan ser remitidos por los canales oficiales por problemas en el sistema u otros ajenos al administrado, previa verificación de evidencias.

Los casos de inconvenientes con mesa de partes digital pueden escribir adjuntando la evidencia a los siguientes correos mesadeayuda@concytec.gob.pe y mesadepartes@concytec.gob.pe.

8. CONFORMIDAD DEL SERVICIO

La conformidad del servicio estará a cargo del encargado de la Oficina de Tecnologías de Información, previa presentación del entregable presentado por el contratista.

Dicha conformidad se otorgará en un plazo que no exceda de los siete (07) días, contados desde el día siguiente de recibido el entregable.

9. FORMA Y CONDICIÓN DE PAGO

Forma de pago

El pago se efectuará en dos (2) armadas, previa presentación de los entregables y conformidad emitida por el área usuaria; según el siguiente detalle:

Pagos	Forma de pago
Primer Pago	Monto de pago equivalente al 40% del Monto total contratado, previa presentación del primer y segundo entregable, y conformidad emitida por el área usuaria

Segundo Pago	Monto de pago equivalente al 60% del monto total contratado, previa presentación del tercer entregable, y conformidad emitida por el área usuaria.

Condición de pago
El pago se realizará con abono en la cuenta "Código de Cuenta Interbancaria" (CCI) del contratista, como máximo, hasta los diez (10) días calendario posteriores a la emisión de la conformidad del bien respectiva y presentación del comprobante de pago.

Los informes y recomendaciones entregados al CONCYTEC deben encontrarse en español, a excepción de los reportes que puedan ser emitidos directamente por las herramientas utilizadas, los cuales servirán como anexos a los informes presentados.

10. PENALIDADES APLICABLES:

La entidad contratante puede establecer penalidades en el contrato menor. La suma de la aplicación de las penalidades por mora y de otras penalidades no puede exceder el 10% del monto del entregable correspondiente.

Penalidad por mora:
Según el Art. 120 del RLGC, en caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

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

Donde F tiene los siguientes valores:
Para bienes y servicios: F= 0.40

11. CONFIDENCIALIDAD Y PROPIEDAD INTELECTUAL

La información y material producido bajo las especificaciones técnicas de la presente contratacion, tales como escritos, medios magnéticos, digitales, y demás documentación generados por la prestación, pasará a propiedad del CONCYTEC. El/La proveedor deberá mantener la confidencialidad y reserva absoluta en el manejo de la información y documentación a la que se tenga acceso relacionada a la prestación.

12. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del bien ofertado por un plazo no menor de un año, contado a partir de la conformidad otorgada por la Entidad.

13. CLAUSULA DE CUMPLIMIENTO (LEY DE PREVENCION Y MITIGACION DEL CONFLICTO DE INTERESES EN EL ACCESO Y SALIDA DE PERSONAL DEL SERVICIO PUBLICO, LEY N° 31564). (Obligatorio)

Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.

14. MATERIAL DE ORIENTACIÓN PARA DENUNCIAR ACTOS DE CORRUPCIÓN EN LOS PROCESOS DE CONTRATACION (Obligatorio)

En el Consejo Nacional de Ciencia, Tecnología e Innovación, promovemos la ética e integridad de la función pública, por lo que, si conoces de algún acto de corrupción ejercido por un/a servidor/a del CONCYTEC, comunica tu denuncia ingresando de manera virtual a la Plataforma Digital Única de Denuncias del Ciudadano (https://denuncias.servicios.gob.pe/).

Ejemplos:

a) Adecuación o manipulación de las especificaciones técnicas, expediente técnico o términos de referencia para favorecer a un proveedor específico.
b) Generación de falsas necesidades con la finalidad de contratar obras, bienes o servicios.
c) Otorgamiento de la buena pro obviando deliberadamente el procedimiento requerido conforme a ley.
d) Permisividad indebida frente a la presentación de documentación incompleta de parte del ganador de la buena pro.
e) Otorgamiento de la buena pro a postores de quienes se sabe han presentado documentación falsa o no vigente.
f) Otorgamiento de la buena pro de (o ejercicio de influencia para el mismo fin) a empresas ligadas a exfuncionarios, de quienes se sabe están incursos en algunos de los impedimentos para contratar con el Estado que prevé la ley.
g) Admisibilidad de postor (o ejercicio de influencia para el mismo fin) ligado a una misma empresa, grupo empresarial, familia o allegado/a, de quien está incurso en alguno de los impedimentos para contratar con el Estado que prevé la ley.
h) Pago indebido por obras, bienes o servicios no entregados o no prestados en su totalidad.
i) Sobrevaloración deliberada de obras, bienes o servicios y su consecuente pago en exceso a los proveedores que las entregan o brindan.
j) Negligencia en el manejo y/o mantenimiento de equipos y/o tecnología que impliquen la afectación de los servicios que brinda la institución.

¿Conoces de alguno de estos actos de corrupción, o de otros que pueden haberse cometido?, COMUNÍCANOS.

Notas:

- La denuncia puede ser anónima.
- Si el denunciante decide identificarse, se garantiza la reserva de su identidad y/o de los testigos que quieran corroborar la denuncia, y puede otorgar una garantía institucional de no perjudicar su posición en la relación contractual establecida con la Entidad o su posición como postor en el proceso de contratación en el que participa o en los que participe en el futuro.
- Es importante documentar la denuncia, pero si no es posible, se recomienda proporcionar información valiosa acerca de donde obtenerla o prestar colaboración con la entidad para dicho fin.
- La interposición de una denuncia no constituye impedimento para gestionar por otras vías que la ley prevé para cuestionar decisiones de la administración o sus agentes (OSCE, Contraloría General de la República, Ministerio Público, etc.).
- La interposición de una denuncia no servirá en ningún caso para paralizar un proceso de contratación del Estado.

15. GARANTÍAS

NO CORRESPONDE.

16. OBLIGACIÓN ANTICORRUPCIÓN Y ANTISOBORNO

El proveedor declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere la Ley

General de Contrataciones de Públicas, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el proveedor se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a estas.

Además, el proveedor se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Finalmente, el proveedor se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

17. SOLUCIÓN DE CONTROVERSIA

En el caso de contratos menores, las partes pactan la conciliación como mecanismo de solución de las controversias.

18. RESOLUCIÓN DE 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 ejecución contractual.
f) Configuración de la condición de terminación anticipada establecida en el contrato, de acuerdo con los supuestos que se establezcan en el reglamento para su aplicación.

19. GESTIÓN DE RIESGOS

NO CORRESPONDE.

20. SANCIONES

El Tribunal de Contrataciones Públicas sanciona a los participantes, postores, proveedores, y subcontratistas, cuando incurran en las infracciones señaladas en el párrafo 87.2 del artículo 87 de la presente ley, sin perjuicio de las responsabilidades civiles o penales a que hubiera lugar.

Las sanciones por imponer pueden ser:

a) Multa.
b) Inhabilitación temporal.
c) Inhabilitación permanente.

La multa o inhabilitación que se impongan no eximen de la obligación de cumplir con los contratos ya perfeccionados a la fecha en que la sanción queda firme.

CONCYTEC Firma Digital
Firmado digitalmente por VASQUEZ MACHICAO Percy FAU 20135727394 soft
Motivo: Soy el autor del documento
Fecha: 22.04.2026 09:40:30 -05:00

Firma y sello del responsable del Área Usuaria