Anexo N°02

Términos de Referencia

Órgano y/o Unidad Orgánica:	Oficina de Tecnologías de la información y comunicaciones
Actividad del POI:	C0046 – Implementación de Gobierno Digital
Denominación de la Contratación:	Servicios Especializados en Ciberseguridad Integral para Plataformas Web, Sistemas Internos y Gestión de la Seguridad de la Información
Principio de Contratación	Valor por Dinero

I. FINALIDAD PÚBLICA

Garantizar la seguridad, integridad y disponibilidad de los sistemas web (sitios web y APIs) y los sistemas internos de la institución ante posibles amenazas cibernéticas como phishing, exploits, Cross-Site Scripting y ransomware, asegurando la continuidad operativa y la protección de la información sensible, lo que incluye la implementación de medidas robustas para la **protección de los activos digitales** de la institución."

II. OBJETIVO DE LA CONTRATACIÓN

Contratar un especialista en ciberseguridad para realizar evaluaciones de vulnerabilidades, pruebas de penetración e implementar medidas de seguridad preventivas y reactivas en los servidores web, sitios web, APIs y sistemas internos de la institución.

Objetivos Específicos

- Realizar evaluaciones de vulnerabilidades y pruebas de penetración exhaustivas en los 2 servidores web de producción y 1 de desarrollo, con los 14 sitios web (ASP Nativo, ASP .Net 9, Joomla), las Web APIs .Net 9 y la plataforma de pagos en línea.
- Analizar las vulnerabilidades de los sistemas internos y la configuración de seguridad de la infraestructura de red (firewalls Fortinet, segmentación de red).
- Implementar medidas de seguridad correctivas y preventivas basadas en los resultados de las evaluaciones.
- Desarrollar un plan básico de respuesta a incidentes de seguridad adaptado a la infraestructura existente.
- **Transferir conocimiento y capacitar al personal técnico en las herramientas y técnicas utilizadas durante las evaluaciones y en los fundamentos de la respuesta a incidentes.**
- **Fortalecer las Capacidades de Gestión de Seguridad de la Información y Monitoreo Continuo,** lo que incluye implementar o reforzar medidas de seguridad clave para la protección integral de los activos digitales, incluyendo el establecimiento de bases para un Sistema de Gestión de Seguridad de la Información (SGSI), la consideración de equipos de respuesta a incidentes (CSIRT), la implementación de herramientas para el monitoreo constante de intrusiones, y la optimización de procesos de respaldo y recuperación de datos críticos

III. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

3.1 Descripción del servicio a contratar

El servicio principal a contratar es la provisión de Servicios Especializados en Ciberseguridad, que incluyen la evaluación de vulnerabilidades, pruebas de penetración, implementación de medidas de seguridad, desarrollo de un plan de respuesta a incidentes, y capacitación, según se detalla en los alcances del servicio.

3.2 Actividades

El especialista en ciberseguridad deberá llevar a cabo las siguientes actividades:

3.2.1. Evaluación de Vulnerabilidades y Pruebas de Penetración:

- Realizar pruebas de caja negra, caja blanca y caja gris en los servidores web.
- Evaluar las vulnerabilidades de los 14 sitios web (identificando posibles ataques como inyecciones SQL, XSS, CSRF, etc.).
- Analizar la seguridad de las Web APIs .Net 9 (autenticación, autorización, inyecciones, etc.).
- Evaluar la seguridad de la plataforma de pagos en línea (siguiendo las mejores prácticas y estándares de la industria).
- Analizar la configuración de seguridad de los firewalls Fortinet y la segmentación de red.
- Evaluar la seguridad de los sistemas internos (identificando posibles puntos débiles).
- Generar informes detallados de las vulnerabilidades encontradas, incluyendo su criticidad, impacto potencial y recomendaciones de mitigación.
- Analizar la seguridad de los servidores de archivos, servidores de correo, servidores de bases de datos y las aplicaciones transaccionales.
- Generar informes detallados de las vulnerabilidades encontradas, incluyendo su criticidad, impacto potencial y recomendaciones de mitigación.

3.2.2. Implementación de Medidas de Seguridad:

- Proponer e implementar medidas de seguridad correctivas y preventivas basadas en los hallazgos de las evaluaciones.
- Asistir en la configuración de herramientas de seguridad (ej. WAFs, sistemas de detección de intrusiones, etc., si aplica).
- Revisar y fortalecer las políticas de seguridad existentes.

3.2.3. Respuesta a Incidentes:

- Desarrollar un plan básico de respuesta a incidentes adaptado a la infraestructura actual.
- Definir roles y responsabilidades en caso de incidentes.
- Establecer procedimientos básicos de contención, erradicación y recuperación.

3.2.4. Capacitación y Transferencia de Conocimiento:

- Realizar sesiones de capacitación al personal de OTI sobre las herramientas y metodologías utilizadas en las evaluaciones de vulnerabilidades y pruebas de penetración, dichas capacitaciones serán avaladas por un certificado o constancia.
- Capacitar al personal de OTI en los fundamentos de la respuesta a incidentes y los procedimientos básicos definidos.
- Documentar las configuraciones de seguridad implementadas y los procedimientos de respuesta a incidentes.

3.2.5. Fortalecimiento de la Gestión y Monitoreo de Seguridad de Activos Digitales:

- **Implementación y/o Asesoría en Sistema de Gestión de Seguridad de la Información (SGSI):** Proponer y asistir en las fases iniciales de la implementación de un SGSI basado en estándares reconocidos (como ISO 27001), enfocándose en la identificación, evaluación y tratamiento de riesgos de seguridad de la información.

- **Formación de Equipos de Respuesta a Incidentes (CSIRT):** Asesorar en la conceptualización y/o formación de un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) interno, incluyendo la definición de roles, responsabilidades y procedimientos iniciales.

- **Implementación de Herramientas y Procesos de Vigilancia Continua:**

  - **Programación y Ejecución de Auditorías y Pruebas Anuales:** Complementar las evaluaciones de vulnerabilidades y pruebas de penetración iniciales con una propuesta de programación para auditorías y pruebas anuales recurrentes, con el fin de asegurar la identificación continua de brechas y puntos débiles en la infraestructura.

  - **Adopción de Soluciones de Seguridad y Monitoreo (SIEM):** Asesorar en la adopción de soluciones avanzadas contra códigos maliciosos (anti-malware, EDR) y en la implementación y configuración de herramientas SIEM (Security Information and Event Management) para el monitoreo continuo de eventos de seguridad, detección temprana de actividades sospechosas e intentos de intrusión.

  - ***Gestión de Copias de Seguridad y Recuperación ante Desastres:*** *Revisar y optimizar los procedimientos existentes para la realización de copias de seguridad regulares de datos críticos, y asegurar la disponibilidad y prueba de los procedimientos de recuperación ante desastres en caso de un incidente de seguridad mayor.*

- **Plan de trabajo**

  No Aplica

- **Seguros**

  No Aplica

- **Prestaciones accesorias a la prestación principal**

  No Aplica

- **Lugar y plazo de prestación del servicio**
  - **Lugar**

    El desarrollo del servicio se llevará a cabo en, Jr. Bolívar N.º 538-Centro Histórico de Trujillo, en la provincia de Trujillo, Región La Libertad y/o en forma remota previa coordinación con el área usuaria para elaboración del informe.

3.3 Plazo

Plazo de 60 días calendario (a partir del día siguiente de la suscripción del contrato o de la recepción de la Orden de Servicio)

IV. RECURSOS A SER PROVISTOS POR EL CONTRATISTA

4.1 Equipamiento

A. Equipamiento estratégico
No Aplica

B. Otro equipamiento
No Aplica

4.2 Infraestructura estratégica

El Proveedor debe contar con la infraestructura y herramientas adecuadas para la prestación de servicios especializados en ciberseguridad, incluyendo, pero no limitándose a:

1. **Herramientas de Evaluación de Vulnerabilidades:** Software y plataformas para escaneo de vulnerabilidades en aplicaciones web, APIs y sistemas.
2. **Herramientas de Pruebas de Penetración:** Kits de herramientas y metodologías para la ejecución de pruebas de intrusión controladas.
3. **Acceso a Bases de Datos de Vulnerabilidades:** Acceso a bases de datos actualizadas de vulnerabilidades y exploits conocidos.
4. **Recursos Computacionales Suficientes:** Hardware y software robustos para el procesamiento y análisis de grandes volúmenes de datos de seguridad.
5. **Conectividad Segura:** Medios seguros para el acceso remoto, si aplica, y la transmisión de información sensible.
6. **Medios para la Generación de Informes:** Herramientas para la elaboración de informes técnicos y ejecutivos detallados.
7. **Capacidad de Almacenamiento Seguro:** Espacio de almacenamiento seguro para la información recopilada y generada durante el servicio, cumpliendo con estándares de confidencialidad.
8. **Herramientas SIEM y de Análisis Profundo:** Plataformas de Gestión de Información y Eventos de Seguridad (SIEM) para la recolección, correlación y análisis en tiempo real de logs y eventos de seguridad, así como herramientas para análisis forense, análisis de comportamiento y detección avanzada de amenazas.

4.3 Personal

El contratista será responsable de asignar el personal técnico y profesional idóneo para la ejecución del servicio, asegurando que cuente con la experiencia, formación académica y competencias necesarias para cumplir con las actividades establecidas.

El personal deberá ser suficiente y encontrarse disponible durante toda la vigencia del servicio, conforme al cronograma de trabajo. Cualquier cambio en el equipo de trabajo deberá ser comunicado previamente a la Entidad y autorizado por esta.

A. Personal clave (Especialista Principal en Ciberseguridad)

i. Actividades

- Supervisión y ejecución de las Evaluaciones de Vulnerabilidades y Pruebas de Penetración.
- Liderazgo en la Implementación de Medidas de Seguridad.
- Diseño y desarrollo del Plan Básico de Respuesta a Incidentes.
- Dirección de las sesiones de Capacitación y Transferencia de Conocimiento.
- Elaboración y presentación de todos los Entregables.

ii. Perfil

Profesional Ingeniero de Sistemas, Informático o a fines al servicio brindado, con **capacitaciones y experiencia certificada en ciberseguridad** (ej. certificaciones CEH, OSCP, CompTIA Security+, u otras relevantes) y **experiencia mínima de cinco (05) años en servicios similares** de evaluación de vulnerabilidades y pruebas de penetración en entornos web, APIs y de infraestructura de red.

Del Proveedor

- El Proveedor no deberá estar impedido, temporal o permanentemente, para contratar con el Estado Peruano. Tampoco deberá tener sanción vigente aplicada por el OSCE.
- Persona jurídica o persona natural que se encuentre activo y habido en el registro de la SUNAT.
- El proveedor deberá de contar con el Registro Nacional de Proveedores (RNP) vigente, a fin de poder contratar con el Estado.
- El proveedor podrá ser una persona jurídica o natural con experiencia demostrable en el rubro de ciberseguridad.
- El proveedor deberá demostrar **experiencia mínima de tres (03) servicios similares** al objeto de contratación, específicamente en la provisión de servicios de **evaluaciones de vulnerabilidades y pruebas de penetración en entornos web y de red.**

V. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

5.1 Otras obligaciones

5.1.1 Otras obligaciones del contratista

El proveedor deberá presentar a las de Oficina de Logística y Control Patrimonial, Oficina de Tecnologías de la información y comunicaciones y Soporte Técnico, un informe digital detallando los siguiente:

a) Informe de Evaluación de Vulnerabilidades y Pruebas de Penetración (Servidores Web, Sitios Web, APIs y Plataforma de Pagos):

- Un documento detallado por cada componente evaluado (servidores, sitios web, APIs, plataforma de pagos).

- Resumen ejecutivo con los hallazgos más críticos y recomendaciones de alto nivel.
- Descripción de las metodologías y herramientas utilizadas durante las pruebas.
- Listado exhaustivo de las vulnerabilidades encontradas, clasificadas por criticidad (alta, media, baja).
- Descripción técnica de cada vulnerabilidad, incluyendo su ubicación, impacto potencial y pasos para su reproducción (si aplica).
- Recomendaciones específicas y priorizadas para la mitigación de cada vulnerabilidad, incluyendo posibles soluciones técnicas y configuraciones.
- Evidencia de las vulnerabilidades encontradas (capturas de pantalla, logs, etc., según sea apropiado y sensible).

b) Informe de Análisis de Seguridad de Infraestructura de Red:

- Un documento que detalle el análisis de la configuración de los firewalls Fortinet y la segmentación de red

- Identificación de posibles debilidades en la configuración de las reglas de firewall, políticas de acceso y segmentación de la red.
- Recomendaciones para fortalecer la seguridad perimetral y la segmentación interna.

c) Plan Básico de Respuesta a Incidentes:

- Un documento que describa los procedimientos básicos a seguir en caso de incidentes de seguridad.
- Definición de roles y responsabilidades del equipo técnico ante un incidente.
- Pasos generales para la detección, contención, erradicación, recuperación y lecciones aprendidas de un incidente.
- Lista de contactos importantes en caso de emergencia cibernética.

d) Documentación de Medidas de Seguridad Implementadas (si aplica):

- En caso de que el especialista asista en la implementación de medidas de seguridad, se deberá entregar documentación sobre las configuraciones realizadas, las políticas implementadas y las herramientas de seguridad configuradas.

e) Material de Capacitación:

- Presentaciones, guías o manuales utilizados durante las sesiones de capacitación al personal técnico, las cuales deben ser muy claras y entendibles.
- El Contenido de la capacitación deberá cubrir las herramientas y metodologías de pentesting utilizadas y los fundamentos de la respuesta a incidentes.

f) Informe de Transferencia de Conocimiento y Capacitación:

- Un resumen de las sesiones de capacitación realizadas, incluyendo los temas cubiertos, la asistencia del personal técnico y las recomendaciones para futuras capacitaciones

g) Presentación de Resultados Finales:

- Ser realizará una presentación ejecutiva que resuma los hallazgos principales, las recomendaciones clave y el plan de acción propuesto.

h) Informe de Propuesta/Avance SGSI y CSIRT (si aplica):

- Documento que detalle la propuesta o los avances realizados en la implementación de un SGSI y/o la formación de un CSIRT, incluyendo la definición de alcance, políticas iniciales o recomendaciones de estructura.

i) Informe de Soluciones y Procesos de Monitoreo:

- Documento que describa las soluciones implementadas o las recomendaciones para la adopción de herramientas anti-malware y SIEM, incluyendo su configuración, los procesos de monitoreo definidos y los procedimientos de alerta y respuesta temprana.

j) Informe sobre Copias de Seguridad y Recuperación ante Desastres:

- Un reporte que evalúe el estado actual de las copias de seguridad y los procedimientos de recuperación, incluyendo recomendaciones para su optimización y prueba.

k) Inventario Actualizado y Resultados de Pruebas PIDE (TLP:RED):

- El proveedor deberá remitir un inventario actualizado de todos los aplicativos que consumen servicios web a través de la Plataforma de Interoperabilidad del Estado (PIDE), así como los resultados de las pruebas de evaluación de vulnerabilidades específicas para estos aplicativos, acompañados de las evidencias de las acciones realizadas. Esta información deberá ser enviada de forma segura bajo el protocolo TLP:RED.

EL PROVEEDOR será responsable directo de la ejecución de todas las actividades contratadas, ya sea de manera personal o a través del personal a su cargo. Deberá cumplir con los plazos establecidos, mantener comunicación constante con el área usuaria y garantizar la calidad de los servicios prestados. Asimismo, deberá entregar los entregables comprometidos, de acuerdo con los términos y condiciones establecidos en el contrato.

5.1.2 Otras obligaciones de la Entidad

La Entidad proporcionará al PROVEEDOR las facilidades razonables necesarias para la correcta ejecución del servicio, tales como el acceso a las instalaciones, información pertinente oportuna, y los medios de coordinación con el área usuaria. Además, designará un responsable de la supervisión del servicio, con quien el PROVEEDOR deberá mantener contacto permanente.

5.2 Adelantos

No Aplica

5.3 Confidencialidad

La información y documentación a la que se tendrá acceso tiene carácter **confidencial**, y está prohibido revelar dicha información a terceros. El contratista deberá cumplir con todas las políticas y estándares establecidos en el servicio en cuanto a la **seguridad de la información**, tanto la información recibida como la generada durante la realización y al concluir las actividades, incluyendo informes y datos recopilados o recibidos, sin importar su origen o medio de almacenamiento. Se recomienda el cumplimiento de estándares como la ISO 27001.

El Proveedor acepta que será responsable de los daños y perjuicios ocasionados como resultado de cualquier acto que atente contra la confidencialidad, ya sea por acción u omisión.

5.3 Propiedad intelectual

Todos los productos, informes, documentos, software, planos, manuales y demás materiales generados como resultado de la prestación del servicio serán de propiedad exclusiva de la Entidad, incluyendo los derechos de autor, patentes u otros derechos de propiedad intelectual. El PROVEEDOR deberá ceder expresamente dichos derechos a favor de la Entidad cuando corresponda.

5.4 Medidas de control durante la ejecución contractual

La Entidad podrá realizar la supervisión o inspección programadas o inopinadas durante la ejecución del servicio, a fin de verificar el cumplimiento de los términos contractuales. Estas acciones serán coordinadas por el área usuaria y ejecutadas por personal técnico designado. El PROVEEDOR deberá colaborar con estas acciones, brindando la información y facilidades necesarias.

5.5 Conformidad de la prestación

La conformidad la brindará la Oficina de Tecnología de la Información y Comunicaciones
en un plazo máximo de 10 días (se computa desde el día siguiente de culminado el servicio)
previa entrega de informe de actividades realizadas, especificadas en el punto 3.2.

5.6 Forma de pago

El pago se realizará después de ejecutada la prestación y otorgada la conformidad, para lo cual deberá presentar: Los **informes y entregables finales** detallados en el punto 5.1.1 específicamente de **a)** a la **k)**.

5.7 Penalidad por Mora

Penalidad por Mora en la ejecución de la prestación:

En caso de retraso injustificado del proveedor en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

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

Donde F tiene los siguientes valores:

- Para bienes, servicios en general: F=0.40.

Tanto el monto como el plazo se refieren, según corresponda, a la ejecución total del servicio o a la obligación parcial, de ser el caso, que fuera materia de retraso.
Se considera justificado el retraso, cuando el proveedor acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable.

Esta calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.

5.8 Otras penalidades aplicables

No Aplica

9 Responsabilidad por vicios ocultos

El PROVEEDOR será responsable por vulnerabilidades, configuraciones erróneas o fallas en las soluciones implementadas que, habiendo estado presentes al momento de la conformidad, se detecten hasta un (01) año después de otorgada dicha conformidad. Asimismo, deberá corregir dichas deficiencias sin costo adicional para la Entidad, incluyendo la actualización de sistemas, parcheo de vulnerabilidades o reimplementación de controles de seguridad.

5.10 CLÁUSULA: GARANTÍAS

5.11 CLÁUSULA GESTIÓN DE RIESGOS

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

5.12 CLÁUSULA RESOLUCIÓN DEL CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas.

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES proceden de acuerdo a lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF

5.13 CLÁUSULA ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción de este contrato, EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación[1] y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

5.14 CLÁUSULA SOLUCIÓN DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación y/o arbitraje, según el acuerdo de las partes.

Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley N° 32069, Ley General de Contrataciones Públicas, y su Reglamento.
El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 84.9 del artículo 84 de la Ley N° 32069, Ley General de Contrataciones Públicas

V° B° Gerencia respectiva	Firma del Responsable del área usuaria