TÉRMINOS DE REFERENCIA

SERVICIO PARA MEJORAMIENTO DE LA SEGURIDAD DIGITAL IMPLEMENTANDO PROCEDIMIENTOS DE DETECCIÓN DE AMENAZAS Y VULNERABILIDADES.

1. NOMBRE DEL SERVICIO:

SERVICIO PARA MEJORAMIENTO DE LA SEGURIDAD DIGITAL IMPLEMENTANDO PROCEDIMIENTOS DE DETECCIÓN DE AMENAZAS Y VULNERABILIDADES.

2. ANTECEDENTES:

La revolución digital está transformando profundamente la forma en la que vivimos, cómo nos comunicamos, las sociedades y, sin duda, la forma en la que prestamos el servicio público. El despliegue digital y su aprovechamiento compromete a todos los ciudadanos, al Estado, al sector privado, a la academia y a la sociedad civil. Sin embargo, es obligación del Estado garantizar la viabilidad de la digitalización del país desde la conectividad, la educación, la economía, la seguridad y el gobierno digital.

Como país existen aún fuertes brechas que superar respecto a los indicadores internacionales, por lo que la transformación digital requiere de un sólido liderazgo al interior de las entidades públicas. Es en ese marco que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, ha desplegado grandes esfuerzos para encaminar este proceso en el Estado hacia un mejor servicio a los ciudadanos:

Líder Digital: Se estableció el rol del líder digital como un miembro de la Alta Dirección de las entidades públicas. El líder dirige la estrategia de gobierno digital en las entidades con un claro enfoque en la atención de las necesidades del ciudadano. El Perú se ha convertido en el primer país de la Alianza del Pacífico en establecer el rol del líder digital al interior del Estado siguiendo las recomendaciones de la OCDE.	**Plataforma Digital para la Declaración Jurada de Intereses:** Se estableció una plataforma digital para que los funcionarios del Poder Ejecutivo declaren sus intereses en un entorno digital identificándose y firmando digitalmente con su DNI electrónico **como muestra clave de transparencia y gobierno abierto.**
Comités de Gobierno Digital: Se establece un único colegiado al interior de las entidades públicas que incorpora como miembros principales a los servidores responsables de la atención al ciudadano y la gestión de talento para dirigir una transformación digital orientada a nuestros ciudadanos. El Perú es el primer país de la Alianza del Pacífico en establecer este modelo de gobernanza para el gobierno digital.	**Promulgación de la Ley de Gobierno Digital:** El **Perú se constituye en uno de los primeros países en promulgar una Ley de Gobierno Digital** con pilares centrados en identidad digital, interoperabilidad, arquitectura digital, datos, seguridad digital y servicios digitales que implican una orientación integral de los proyectos de tecnologías digitales hacia los ciudadanos y que aseguran el despliegue de las tecnologías digitales como base de la economía digital en el país y de un Estado Digital más transparente, eficiente, confiable, productivo y cercano con el ciudadano.
Seguridad Digital: Se estableció la orientación de la seguridad digital del Estado como un entorno de confianza en el mundo digital para los ciudadanos. El Perú es el segundo país de la Alianza del Pacífico, después de Colombia, en orientar la seguridad digital hacia ciudadanos.	**Promulgación del Decreto Supremo 118-2018-PCM** que declara de interés nacional el desarrollo de gobierno digital, la innovación y la economía digital con enfoque territorial y crea el Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo que convoca a las entidades responsables de los ámbitos fundamentales de la digitalización del Estado.

Plataforma Digital Única GOB.PE del Estado para Orientación al Ciudadano: Se estableció una única plataforma para orientar a los ciudadanos con un sólido trabajo en equipo y un esfuerzo extraordinario de todos los Ministerios. El Perú es el primer país de la Alianza del Pacífico que ha desplegado una Plataforma Única GOB.PE y el 3er. país en el mundo luego de www.gob.uk (Reino Unido) y www.gob.mx (México).	**Perú lidera el cumplimiento del Mandato 3 de la Declaración de Cali firmada por los Presidentes de Alianza del Pacífico** que promueve **el reconocimiento transfronterizo de firmas digitales** el cual impacta directamente en la seguridad y agilidad jurídica de las acciones internacionales, en el comercio internacional, en el cumplimiento de tratados de libre comercio, en la facilitación del intercambio comercial con bloques de países como APEC, Unión Europea entre otros, elevando la competitividad de los países miembros.

Así también, como parte de los avances en materia de transformación digital, el Perú y el Banco Interamericano de Desarrollo (BID) suscribieron el 12 de septiembre de 2018 el Contrato de Préstamo N°PE4399/OC-PE el mismo que permitirá garantizar la interoperabilidad entre las entidades públicas para simplificar los trámites más demandados por los ciudadanos, establecer un sólido Centro de Seguridad Digital en el Estado, construir una identidad y una carpeta digital para los ciudadanos, ampliar la Plataforma GOB.PE, establecer una sólida estrategia de datos para la toma de decisiones en el Estado y digitalizar los servicios públicos más importantes para el ciudadano.

El Proyecto tiene un monto de inversión de US$ 64.9 millones, siendo el monto del préstamo de US$ 50 millones y la contrapartida nacional de US$ 14.6 millones. Siendo los objetivos específicos: Los objetivos específicos son: (i) simplificación, estandarización y mejora regulatoria; (ii) mejora y ampliación de las capacidades de interoperabilidad de las entidades del Estado; (iii) mejora de la gestión en la atención a ciudadanos y empresas; y (iv) mejora de las condiciones para la planificación y coordinación de los servicios.

3. BASE NORMATIVA DEL PROYECTO

- Constitución Política del Perú
- Ley Nª 29158, Ley Orgánica del Poder Ejecutivo.
- Decreto Legislativo N° 1246, que aprueba diversas medidas de simplificación administrativa.
- Decreto Legislativo N° 1310, que aprueba medidas de adicionales de simplificación administrativa.
- **Decreto Legislativo 1412, Ley de Gobierno Digital**
- **Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital.**
- **Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.**
- Decreto Supremo N° 022-2017-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
- Decreto Supremo N° 033-2018-PCM, que crea la Plataforma Digital Única del Estado Peruano, Gob.pe, y establece disposiciones adicionales para el desarrollo del Gobierno Digital
- Decreto Supremo N° 118-2018-PCM, por el que declaran de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial.

4. OBJETIVO DE LA CONTRATACIÓN:

4.1. Objetivo General.

Implementar y analizar procedimientos de detección de amenazas y vulnerabilidades y hackeo ético del Centro Nacional de Seguridad Digital, en el marco de lo establecido en el “Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y a las Empresas, a Nivel Nacional”.

4.2. Objetivos Específicos

- Elaborar procedimientos de gestión de riesgos así como detección de amenazas y vulnerabilidades de la seguridad digital en el Centro Nacional de Seguridad Digital y entidades públicas, en coordinación con el equipo de la Subsecretaria de Tecnologías Digitales.
- Detectar e identificar riesgos, amenazas y vulnerabilidades de la seguridad digital en entidades públicas.
- Capacitar sobre gestión de riesgos así como en prevención y protección de amenazas y vulnerabilidades de la seguridad digital en entidades públicas.

La contratación se encuentra programada en el POA del "Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y a las Empresas, a Nivel Nacional" según el siguiente detalle:

- **Actividad 2.5.1.4.1:** Preparación, diseño y despliegue de los componentes del Centro Nacional de Seguridad Digital
- **Componente 2:** Mejora y ampliación de las capacidades de interoperabilidad de las entidades del Estado.

La contratación contribuye al logro de metas programadas en el "Proyecto de Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y a las Empresas, a Nivel Nacional", específicamente a la meta:

- **Meta**: "1 Centro de ciberseguridad implementado y operando al año 2".

La contribución de la consultoría se realizará a través de la implementación de procedimientos de detección de amenazas y vulnerabilidades, orientado a brindar confianza del entorno digital que permita la creación o mejora de la seguridad digital del Centro Nacional de Seguridad Digital.

5. DETALLE DEL SERVICIO

5.1. Actividades a desarrollar

- Elaborar procedimientos de gestión de riesgos y detección de amenazas y vulnerabilidades de seguridad digital en el Centro Nacional de Seguridad Digital, en coordinación constante con el equipo de la Subsecretaría de Tecnologías Digitales.
- Elaborar informe de detección de riesgos, amenazas y vulnerabilidades de seguridad digital, en coordinación con el equipo de la Subsecretaría de Tecnologías Digitales, en el Centro Nacional de Seguridad Digital.
- Elaborar informe de gestión de riesgos así como prevención y protección de activos digitales como son infraestructura, datos e información y aplicaciones informáticas, en entidades públicas.
- Promover y realizar acciones de capacitación y transferencia de conocimientos sobre gestión de riesgos, prevención y protección de activos digitales en entidades públicas.
- Analizar y generar informes periódicos de hacking ético de seguridad digital en entidades públicas.

5.2. Productos esperados

5.2.1. Productos:

Producto 1: ● Procedimientos de gestión de riesgos, amenazas y vulnerabilidades de la seguridad digital, para el Centro Nacional de Seguridad Digital y entidades públicas. a) Procedimientos relativos a direcciones IP Externas y Dominios de Internet. b) Procedimientos relativos a páginas y servicios web, así como seguridad interna de red. c) Procedimientos relativos a redes de comunicación. d) Procedimientos relativos a sistemas de telefonía y telefonía IP. e) Procedimientos relativos a aplicaciones de correo electrónico, mensajería e ingeniería social. ● Detección e informe de riesgos, amenazas y vulnerabilidades de la seguridad digital, en 2 entidades del sector economía y finanzas en Gobiernos Regionales. ● Realización de hacking ético de la seguridad digital en 2 entidades del sector economía y finanzas en Gobiernos Regionales. ● Capacitación sobre gestión de riesgos, amenazas y vulnerabilidades de la seguridad digital de entidades del sector economía y finanzas.
Producto 2: ● Detección e informe de riesgos, amenazas y vulnerabilidades de la seguridad digital, en 4 entidades del sector salud en Gobiernos Regionales. ● Realización de hacking ético de la seguridad digital en 4 entidades del sector salud en Gobiernos Regionales. ● Capacitación sobre gestión de riesgos, amenazas y vulnerabilidades de la seguridad digital de entidades del sector salud.
Producto 3: ● Detección e informe de riesgos, amenazas y vulnerabilidades de la seguridad digital, en 4 Gobiernos Locales – Municipalidad Provincial tipo "**A**". ● Realización de hacking ético de la seguridad digital en 4 Gobiernos Locales – Municipalidad Provincial tipo "**A**". ● Capacitación sobre gestión de riesgos, amenazas y vulnerabilidades de la seguridad digital en Gobiernos Locales – Municipalidad Provincial tipo "**A**".
Producto 4: ● Detección e informe de riesgos, amenazas y vulnerabilidades de la seguridad digital, en 4 entidades del sector transportes y comunicaciones en Gobiernos Regionales. ● Realización de hacking ético de la seguridad digital en 4 entidades del sector transportes y comunicaciones en Gobiernos Regionales. ● Capacitación sobre gestión de riesgos, amenazas y vulnerabilidades de la seguridad digital en entidades del sector transportes y comunicaciones**.**
Producto 5: ● Detección e informe de riesgos, amenazas y vulnerabilidades de la seguridad digital, en 4 Gobiernos Locales – Municipalidad Provincial tipo "**B**". ● Realización de hacking ético de la seguridad digital en 4 Gobiernos Locales – Municipalidad Provincial tipo "**B**". ● Capacitación sobre gestión de riesgos, amenazas y vulnerabilidades de la seguridad digital en Gobiernos Locales – Municipalidad Provincial tipo "**B**"
Producto 6: ● Detección e informe de riesgos, amenazas y vulnerabilidades de la seguridad digital, en 4 entidades del sector educación en Gobiernos Regionales.

● Realización de hacking ético de la seguridad digital en 4 entidades del sector educación en Gobiernos Regionales. ● Capacitación sobre gestión de riesgos, amenazas y vulnerabilidades de la seguridad digital en entidades del sector educación.
Producto 7: ● Detección e informe de riesgos, amenazas y vulnerabilidades de la seguridad digital, en 4 entidades del sector energía y minas en Gobiernos Regionales. ● Realización de hacking ético de la seguridad digital en 4 entidades del sector energía y minas en Gobiernos Regionales. ● Capacitación sobre gestión de riesgos, amenazas y vulnerabilidades de la seguridad digital en entidades del sector energía y minas.

i) *Las entidades públicas de los sectores bajo la administración de los Gobiernos Regionales se les asignará previa evaluación de las prioridades de la Subsecretaría de Tecnologías Digitales.*
ii) *Las Municipalidades Provinciales de tipo **"A"** se asignará según la prioridad establecida por la Subsecretaría de Tecnologías Digitales del siguiente listado:*
https://www.mef.gob.pe/contenidos/presu_publ/migl/municipalidades_pmm_pi/municipalidades_tipoA.pdf
iii) *Las Municipalidades Provinciales de tipo **"B"** se asignará según la prioridad establecida por la Subsecretaría de Tecnologías Digitales del siguiente listado:*
https://www.mef.gob.pe/contenidos/presu_publ/migl/municipalidades_pmm_pi/municipalidades_tipoB.pdf

5.2.2. Presentación:

PRESENTACIÓN DE LOS PRODUCTOS	
PRESENTACIÓN	Vía correo electrónico a: tramitevirtual@promsace.gob.pe con el asunto INFORME DEL PRODUCTO N° X CONSULTOR "Nombre y Apellido" o en la Presidencia de Consejo de Ministros Mesa de partes de la Unidad Ejecutora 018 Mejoramiento de Servicios a los Ciudadanos y Empresas. Calle Tarata 160, segundo piso. Miraflores.
FORMATO PRODUCTO	El producto debe ser enviado al correo electrónico del Coordinador Sectorial 1: tramitevirtual@promsace.gob.pe con el asunto INFORME DEL PRODUCTO N° X CONSULTOR "Nombre y Apellido". El producto debe tener las siguientes características: - Documento en Formato Docx - Documento en Formato PDF (firmado digitalmente o firmado de manera física visado en todas las páginas y debidamente escaneado) - Las páginas deben estar numeradas con el formato página/total de páginas (ej:1/2). - Letra Arial 11, Interlineado 1.15. Margen moderado.
FORMATO ENTREGA	El informe debe ser entregado junto a una carta firmada digitalmente o firmada de manera física debidamente escaneada dirigida a: SEÑORES UNIDAD EJECUTORA PROMSACE PRESIDENCIA DE CONSEJO DE MINISTROS ASUNTO: Entrega del Producto N°x que detalla las acciones desarrolladas en virtud del contrato N°(…) en el marco del Proyecto de "Mejoramiento y Ampliación de los servicios de soporte para la provisión de los Servicios a Ciudadanos y Empresas a Nivel Nacional", implementado mediante contrato de Préstamo N°PE4399/OC-PE

CONTENIDO	I. ANTECEDENTES II. ANÁLISIS DEL CONTEXTO III. REPORTE DE ACCIONES DESARROLLADAS IV. REPORTE DE DOCUMENTOS PRODUCIDOS V. CONCLUSIONES Y RECOMENDACIONES

5.3. Modalidad y lugar de prestación de los servicios:

5.3.1. El lugar de prestación del servicio:

Lima. El consultor podrá prestar indistintamente sus servicios en las oficinas de la Secretaría de Gobierno Digital o en un espacio externo a ella. Esta definición la realizará la Secretaría de Gobierno Digital.

5.3.2. Equipos:

El consultor deberá contar con su propio equipo de cómputo.

5.3.3. Viajes:

Si la Secretaría de Gobierno Digital lo requiere, el consultor también deberá realizar viajes a provincias. Los gastos serán asumidos por el proyecto "Mejoramiento y Ampliación de los Servicios de Soporte para la Provisión de los Servicios a los Ciudadanos y a las Empresas, a Nivel Nacional" implementado mediante Contrato de Préstamo N° PE4399/OC-PE, de acuerdo a la escala correspondiente, previa presentación del plan de viaje.

5.4. Duración del servicio y forma de pago:

5.4.1. Duración del contrato:

El contrato tendrá una duración de hasta 210 días calendario, como máximo, contados a partir del día siguiente de suscrito el contrato.

5.4.2. Costo de la consultoría:

El costo de la consultoría es de S/ 56,000.00 (Cincuenta seis mil y 00/100 soles) el mismo que incluye los impuestos de ley.

5.4.3. Forma de Pago

Los pagos al consultor/a serán en siete (07) armadas, contra entrega y aprobación de los productos especificados en el punto 5.2.1 del presente documento:

Producto	Plazo de entrega	Monto a pagar
Producto 1	Hasta los treinta (30) días calendario, como máximo, contados a partir del día siguiente de suscrito el contrato	8,000.00
Producto 2	Hasta los sesenta (60) días calendario, como máximo, contados a partir del día siguiente de suscrito el contrato	8,000.00
Producto 3	Hasta los noventa (90) días calendario, como máximo, contados a partir del día siguiente de suscrito el contrato	8,000.00
Producto 4	Hasta los ciento veinte (120) días calendario, como máximo, contados a partir del día siguiente de suscrito el contrato	8,000.00

Producto 5	Hasta los ciento cincuenta (150) días calendario, como máximo, contados a partir del día siguiente de suscrito el contrato	8,000.00
Producto 6	Hasta los ciento ochenta (180) días calendario, como máximo, contados a partir del día siguiente de suscrito el contrato	8,000.00
Producto 7	Hasta los doscientos diez (210) días calendario, como máximo, contados a partir del día siguiente de suscrito el contrato	8,000.00
Total		**56,000.00**

5.5. Supervisión del contrato, revisiones y conformidades:

Previo informe favorable del Subsecretario de Tecnologías Digitales, la conformidad de servicio será emitida por la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros quien correrá traslado de dicha conformidad, al área administrativa de la unidad ejecutora del Proyecto en un plazo no mayor a 5 días.

En caso el producto sea observado por el área usuaria, el consultor/a tiene un plazo máximo de 5 días para subsanar las observaciones, para ello se contabilizará el plazo desde el día siguiente de notificada las observaciones por la unidad ejecutora (PROMSACE).

6. PERFIL PROFESIONAL

El profesional deberá tener el siguiente perfil mínimo:

Tabla 1. Perfil del profesional

Educación	Experiencia General	Experiencia Específica
Bachiller en Ingeniería de Sistemas, o Ingeniería Electrónica, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas y Computación, o Ingeniería de Telecomunicaciones y Redes y/o carreras afines.	Experiencia mínima de cinco (05) años en el sector público o privado.	Experiencia mínima de tres (03) años realizando actividades en; Procedimientos en detección de amenazas y/o Ethical Hacking y/o Penetration Testing y/o Análisis de Vulnerabilidad y/o Informática Forense y/o Seguridades de la información y/o Ciberseguridad y/o desarrollo de aplicaciones sobre software libre y/o afines en el sector público o privado.

1. CRITERIOS DE EVALUACIÓN

A continuación, en la Tabla 2, se presentan los criterios de evaluación del consultor.

Tabla 2. Criterios de evaluación

CRITERIOS DE EVALUACIÓN		
PERFIL	**MÁXIMO**	**100**
FORMACIÓN ACADÉMICA (Máximo 20 puntos)		

Bachiller en Ingeniería de Sistemas, o Ingeniería Electrónica, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas y Computación, o Ingeniería de Telecomunicaciones y Redes y/o carreras afines.	Cumple No Cumple	20 Puntos
Título universitario en Ingeniería de Sistemas, o Ingeniería Electrónica, o Ingeniería Industrial, o Ingeniería Informática, o Ingeniería de Sistemas y Computación, o Ingeniería de Telecomunicaciones y Redes y/o carreras afines.	10	
Cursos y/o Talleres y/o Seminarios y/o Diplomados en temas relacionados a Ethical Hacking y/o Penetration Testing y/o Análisis de Vulnerabilidad y/o Informática Forense y/o Seguridades de la información y/o Ciberseguridad.	10	
EXPERIENCIA GENERAL (Máximo 40 puntos)		
Experiencia mínima de cinco (05) años en el sector público o privado.	Cumple No Cumple	40 Puntos
5 puntos por cada año adicional de experiencia laboral general.	40	
EXPERIENCIA ESPECÍFICA (Máximo 40 puntos)		
Experiencia mínima de tres (03) años realizando actividades en; Procedimientos en detección de amenazas y/o Ethical Hacking y/o Penetration Testing y/o Análisis de Vulnerabilidad y/o Informática Forense y/o Seguridades de la información y/o Ciberseguridad y/o desarrollo de aplicaciones sobre software libre y/o afines en el sector público o privado.	Cumple / No Cumple	40 Puntos
5 puntos por cada año adicional de experiencia específica requerida.	40	
TOTAL PUNTUACIÓN	**100**	**100**

El Comité de Selección evaluará la pertinencia de realizar entrevistas personales en caso amerite.

ENTREVISTA PERSONAL (OPCIONAL)		
Experiencia en temas relacionados al perfil de la contratación. **Se evaluará** capacidad analítica, iniciativa, facilidad de comunicación, liderazgo, trabajo en equipo para la toma de decisiones, orientación al ciudadano.	Cumple No Cumple	