

## TÉRMINOS DE REFERENCIA

# Contratación de un/a consultor/a para Análisis y Remediación de Ciberseguridad en el marco del Programa para la Transformación Digital de mipyme (5294/OC-UR)

### 1. Antecedentes y justificación

La Agencia Nacional de Desarrollo es una Persona Pública no Estatal que tiene por misión impulsar la competitividad y contribuir al desarrollo sostenible de las pequeñas empresas y personas emprendedoras, en todo el territorio nacional, a través de la articulación con actores públicos y privados.

El Gobierno de Uruguay, a través de la ANDE y con el apoyo del Banco Interamericano de Desarrollo (BID), está implementando el Programa de Transformación Digital de MIPYME (5294/OC-UR) denominado “Modo Digital” con el objetivo general de aumentar el crecimiento económico y la eficiencia de las mipymes uruguayas a partir de la adopción de tecnologías digitales.

Los objetivos específicos son: (i) aumentar el conocimiento y el uso de soluciones digitales por las mipyme; e (ii) incrementar la oferta de productos y servicios digitales para la mipyme y fortalecer las capacidades de facilitación para la TD de las mipymes.

### 2. Objetivos de la consultoría

Los objetivos generales de esta consultoría se centran en llevar a cabo un análisis exhaustivo de la infraestructura tecnológica y los sistemas de información de la organización en dos etapas clave. La primera etapa consiste en identificar vulnerabilidades, evaluar riesgos y posibles brechas de seguridad, con el fin de recomendar medidas correctivas que fortalezcan la seguridad. La segunda etapa, cuya realización estará sujeta a un estudio de viabilidad, se enfoca en implementar las acciones de remediación necesarias para corregir las vulnerabilidades detectadas y asegurar la protección integral de los activos digitales, garantizando la continuidad operativa y la seguridad de los datos y operaciones.

### 3. Actividades clave

#### 3.1 Primera Etapa: Análisis y Recomendaciones

- Recopilar información relevante sobre la infraestructura tecnológica, sistemas de información, políticas de seguridad, y procedimientos actuales.
- Realizar pruebas de penetración (pentesting), análisis de vulnerabilidades y escaneos de seguridad en los sistemas y redes.
- Evaluar los riesgos asociados a las vulnerabilidades identificadas, considerando el impacto potencial y la probabilidad de ocurrencia.

- Verificar el cumplimiento con normas y estándares de seguridad relevantes, como ISO/IEC 27001, etc.
- Documentar todas las vulnerabilidades, riesgos y brechas de seguridad identificadas, junto con el análisis de su impacto.
- Diseñar un plan detallado para la implementación de las medidas correctivas, incluyendo cronograma, recursos necesarios, y responsables.

### **3.2 Segunda Etapa: Remediación (Sujeta a Viabilidad)**

- Ejecutar las acciones correctivas y de mejora en la infraestructura, sistemas, y procesos según lo planificado en la primera etapa.
- Realizar pruebas posteriores a la implementación para verificar la efectividad de las medidas y asegurarse de que las vulnerabilidades hayan sido corregidas.
- Actualizar la documentación de seguridad para reflejar los cambios y mejoras implementadas.
- Preparar un informe que detalle las acciones realizadas, los resultados obtenidos y cualquier recomendación adicional.

## **4. Condiciones de la contratación**

El/la consultor/a prestará sus servicios profesionales reportando al área de Tecnologías de la Información (TI). Se prevé una modalidad remota sin perjuicio de mantener las reuniones presenciales que tanto ANDE como el área de TI entiendan necesarias o convenientes a los efectos del desarrollo de la presente consultoría, las que serán llevadas adelante en las oficinas de ANDE.

Quien resulte seleccionado/a para realizar la consultoría para ANDE, para poder cobrar los respectivos honorarios, deberá acreditar estar al día con sus obligaciones tributarias (certificados comunes de BPS y DGI y CJPPU vigentes). En caso de no corresponder afiliación a CJPPU, deberá acreditar tal circunstancia.

No podrán ser consultores/as las personas que revistan la calidad de beneficiarios/as de cualquier instrumento de ANDE, mientras dure la vinculación contractual con ésta. En caso de que al momento de la postulación sean beneficiarios/as de algún instrumento de ANDE, ya sea en forma directa (persona) o indirecta (calidad de socio/a de empresa beneficiaria), deberán comunicar tal circunstancia, a los efectos de evaluar en qué estado se encuentra la vinculación contractual con ANDE.

## **5. Perfil del Consultor/a**

Dominio comprobable de las metodologías OWASP, NIST, CIS, o ISO/IEC 27001, con experiencia en su aplicación durante los últimos dos años.

Sólida experiencia en redes, sistemas operativos (Windows, Linux), bases de datos relacionales, aplicaciones web y entornos en la nube.

Se requiere poseer alguna de las siguientes certificaciones: CISM (Certified Information Security Manager), CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) o ISO/IEC 27001 Lead Auditor.

Contar con referencias y casos de éxito en proyectos similares realizados para empresas pequeñas-medianas, destacando los resultados y beneficios alcanzados.

## 6. Competencias requeridas

Es esencial que el consultor/a comprenda la arquitectura de software, el desarrollo seguro y sea capaz de analizar riesgos. Además, debe poseer competencias blandas como pensamiento crítico, atención al detalle, comunicación efectiva y ética profesional, garantizando así que pueda identificar vulnerabilidades, evaluar riesgos y comunicar hallazgos de manera clara y concisa, siempre manteniendo la confidencialidad.

## 7. Productos esperados

Producto	Contenido	Propósito
<b>Primera Etapa: Análisis y Recomendaciones</b>		
1. Informe de Revisión y Análisis Inicial	Relevamiento de la infraestructura tecnológica, sistemas de información, políticas de seguridad, y procedimientos actuales.	Establecer un punto de referencia sobre el estado actual de la seguridad en la organización.
2. Informe de Evaluación de Vulnerabilidades y Análisis de Riesgos	Resultados de las pruebas de penetración, análisis de vulnerabilidades, escaneos de seguridad, y evaluación de riesgos.	Proporcionar una visión clara y detallada de los puntos débiles en la seguridad y su impacto potencial.
3. Informe de Recomendaciones de Seguridad	Conjunto de recomendaciones detalladas para mitigar los riesgos y mejorar la seguridad, priorizadas por nivel de criticidad y estimadas en horas de trabajo.	Ofrecer una hoja de ruta para la remediación de las vulnerabilidades y el fortalecimiento de la seguridad.
<b>Segunda Etapa: Remediación (Sujeta a Viabilidad)</b>		
4. Informe de Implementación de Medidas	Ejecutar las acciones necesarias para la remediación de los puntos detectados y acordados en el producto 3.	Corregir todos los puntos acordados con ANDE.
5. Manual de Procedimientos Actualizado	Documentación actualizada que refleje las nuevas políticas, procedimientos y tecnologías implementadas como parte de la remediación.	Asegurar la correcta adopción y mantenimiento de las medidas de seguridad implementadas.
6. Informe Final de Remediación	Resumen completo de las acciones realizadas, incluyendo validaciones posteriores a la implementación y recomendaciones adicionales.	Proporcionar una visión consolidada del plan ejecutado y sus resultados, dejando una base para futuras auditorías.

## 8. Plazo

La consultoría tiene una duración prevista de 30 días para la primera etapa y en caso de abordar la segunda se prevé 90 días adicionales.

## 9. Cronograma de Entregas

Producto	Plazo previsto de entrega
<b>Primera Etapa: Análisis y Recomendaciones</b>	
Producto 1	10 días desde la firma del contrato.
Producto 2	15 días desde la entrega del producto 1.
Producto 3	5 días desde la entrega del producto 2.
<b>Segunda Etapa: Remediación (Sujeta a Viabilidad)</b>	
Producto 4	50 días desde la entrega del producto 3.
Producto 5	25 días desde la entrega del producto 4.
Producto 6	15 días desde la entrega del producto 5.

## 10. Criterios de aceptación

El área de Tecnología de la Información, en acuerdo con la Coordinación del Programa, dará visto bueno en aceptación de cada uno de los entregables mencionados anteriormente con el fin de realizar cada desembolso al consultor. La comunicación que hará oficial la aceptación de cada entregable será por medio de correo electrónico.

## 11. Cronograma de Pagos

Los honorarios de la presente consultoría se abonarán de la siguiente manera:

USD 10.000 (dólares americanos diez mil) por concepto de la auditoría en materia de seguridad, enumerando todas las vulnerabilidades detectadas así como la determinación de un plan de trabajo estimado en horas en el que se detallen los trabajos a realizar (primera etapa).

Asimismo, ANDE se reserva la posibilidad de solicitar la ejecución del referido plan de trabajo (segunda etapa), lo que supondrá el devengamiento de honorarios adicionales, los que ANDE informará oportunamente según el plan de trabajo a realizar. El/la Consultor/a conoce y acepta que ANDE se reserva también la facultad de ejecutar el referido plan de trabajo según lo presentado o bien realizar un nuevo llamado a estos efectos.

Las condiciones de pago se basarán en los entregables del proyecto. Los pagos serán realizados de acuerdo con lo indicado en la siguiente tabla:

### Primera Etapa: Análisis y Recomendaciones

Descripción	Condición de pago
Primer pago (30%)	Luego de la presentación y aceptación por parte de ANDE del <b>Producto 1.</b>
Segundo pago (70%)	Luego de la presentación y aceptación por parte de ANDE del <b>Producto 2 y 3.</b>

### Segunda Etapa: Remediación (si corresponde)

Descripción	Condición de pago
Primer pago (60%)	Luego de la presentación y aceptación por parte de ANDE del <b>Producto 4.</b>
Segundo pago (40%)	Luego de la presentación y aceptación por parte de ANDE del <b>Producto 5 y 6.</b>

## 12. Requisitos de postulación

El/la consultor/a deberá:

- Poseer ciudadanía de uno de los países miembros del BID.
- No tener otro contrato a tiempo completo en proyecto alguno financiado con recursos del BID.
- En caso de tener parentesco (hasta tercer grado de consanguinidad y/o segundo grado de afinidad, así como matrimonio o concubinato) de algún funcionario del Banco, el consultor lo pondrá en conocimiento del Contratante y éste deberá consultar al Banco previa formalización de la contratación.
- Los funcionarios del gobierno o servidores públicos (funcionarios del Estado, Gobiernos Departamentales, Entes y Servicios Descentralizados), cualquiera sea la naturaleza del vínculo, solamente pueden ser contratados como consultores individuales o como miembros de un equipo de una firma consultora, siempre que (i) no estén contratados a tiempo completo, (ii) en caso de estar contratados a tiempo completo que estén de licencia sin goce de sueldo, (iii) no sean contratados por la entidad en la que hayan trabajado durante el período inmediatamente anterior al que comenzaron la licencia; y (iv) su contratación no genere un conflicto de interés. Se exceptúan en este punto los docentes en la enseñanza pública.

## 13. Postulación

Las personas interesadas deberán presentar su postulación a [adquisicionesbid@ande.org.uy](mailto:adquisicionesbid@ande.org.uy), hasta el **22 de noviembre de 2024 a las 17:00 hs** indicando el valor hora estimado (impuestos incluidos) en caso de ejecutar la segunda etapa, período de garantía del trabajo y adjuntando Currículum Vitae (anexando certificaciones solicitadas en el punto 5).

Se debe incluir la siguiente referencia en la línea de asunto del mensaje de correo electrónico: **“Consultoría consultor/a para Análisis y Remediación en Ciberseguridad”**.

## 14. Consentimiento de tratamiento de datos

Quienes se presenten, desde ya consienten expresamente que ANDE dé tratamiento a sus datos personales, incorporando los mismos a la base de datos de ANDE según corresponda. A tales efectos, el titular podrá ejercer sus derechos de acceso, actualización, rectificación y supresión dirigiéndose al correo: [datospersonales@ande.org.uy](mailto:datospersonales@ande.org.uy)

En el tratamiento de los datos personales proporcionados por los postulantes, los mismos podrán ser utilizados para las finalidades propias de ANDE. Asimismo, el titular faculta a ANDE a transferir sus datos a terceros exclusivamente con objeto de análisis, monitoreo, evaluación y estudios que ANDE entienda contribuyen a su finalidad. Los datos recabados en el marco de la presente convocatoria serán tratados por ANDE en calidad de responsable y en observancia de lo previsto en la normativa vigente, a saber: Ley N° 18.331 de Protección de Datos Personales y Habeas Data y Decretos N° 664/008 y 414/009. Los datos personales serán tratados con el grado de protección adecuado, tomándose las medidas de seguridad necesarias para evitar su alteración, pérdida, tratamiento o acceso no autorizado por parte de terceros.

## 15. Exoneración de responsabilidad. Desistimiento del llamado

ANDE se reserva el derecho de dar de baja el llamado en cualquier etapa de su realización, así como desestimar cualquier postulación que no se ajuste a las condiciones establecidas en el presente; reservándose también el derecho a rechazarlas si no las considera convenientes, sin generar derecho alguno a los postulantes a reclamar por gastos, honorarios o indemnizaciones por daños y perjuicios, ni por ningún concepto.

ANDE podrá -por cualquier causa y en cualquier momento antes de que venza el plazo de presentación de propuestas- modificar los documentos mediante "aclaraciones", ya sea por iniciativa propia o en atención a aclaraciones solicitadas por los/las interesados/as. Las "aclaraciones" serán publicadas en el mismo sitio donde se publica el presente llamado. ANDE se reserva el derecho de rechazar a su exclusivo juicio, la totalidad de las propuestas.

## 16. Consultas y aclaraciones

Las preguntas o solicitudes de aclaración se deben enviar por escrito al siguiente mail: [adquisicionesbid@ande.org.uy](mailto:adquisicionesbid@ande.org.uy)

El plazo límite para enviar preguntas es el **20 de noviembre de 2024 a las 17:00 hs.**

## 17. Aceptación de los Términos y Condiciones

Por el solo hecho de presentarse al llamado, se entenderá que quienes postulen, conocen y aceptan sin reservas los términos y condiciones establecidos en el presente documento.

## 18. Propiedad de la información

La propiedad de la información resultante de la presente consultoría será de ANDE. Toda información obtenida para el cumplimiento de las actividades, así como sus informes y toda clase de documentos que se produzca/n relacionados con la ejecución del trabajo contratado deberán ser considerados confidenciales y de propiedad exclusiva de ANDE.

La persona consultora no podrá hacer uso de tal documentación o informes, bases de datos y encuestas, salvo para referirse a ellos o citarlos como antecedentes de su actividad técnica o profesional.