Anexo V – Especificaciones Técnicas

Servicios profesionales para el Fortalecimiento de la Seguridad Informática de las Redes de Datos de CONAE.

1. Alcance

Servicios profesionales para la ejecución de un proceso de **Fortalecimiento de la Seguridad Informática de las Redes de Datos de la CONAE. Incluye relevamientos, capacitación y asistencia técnica.**

2. Relevamientos

Diagnóstico e identificación de puntos prioritarios para aumentar la Seguridad Informática en las redes del Organismo.

Deberán considerarse las siguientes sedes de CONAE:

1. Sede Paseo Colón , Paseo Colón 751, CABA
2. Sede Centro Espacial Teófilo Tabanera, Ruta C45 Km 8, Provincia de Córdoba

Deberá incluir como mínimo:

A. Diagnóstico de las redes, tipo "Black Box".

Relevamiento detallado de la seguridad de la red de datos, desde el exterior:

1. Detección de conexiones externas
2. Obtención de rangos de direcciones IP publicadas
3. Pruebas de passwords y autenticaciones varias
4. Detección de protocolos y escaneo de vulnerabilidades
5. Escaneo de puertos TCP, UDP, ICMP
6. Intentos de vulneración a través de Internet
7. Vulnerabilidad de servicios y aplicaciones

Esta lista no es exhaustiva y se incluye como una base mínima a cumplir. El oferente propondrá en su oferta otros puntos a evaluar que él considere que son necesarios para cumplir con el objetivo de la contratación.

El proveedor deberá recopilar la información que muestre la vulnerabilidad por el método Black Box previa coordinación con el personal de Sistemas de CONAE.

B. Relevamiento y diagnostico detallado desde el interior, tipo "White Box" incluyendo, entre otros:

1. Puertos y servicios de comunicaciones.

2. Sistemas operativos. Vulnerabilidades y actualizaciones.
3. Vulnerabilidades de servidores detectados en la red.
4. Vulnerabilidades de software instalado (propios o de terceros)
5. Vulnerabilidades de directorios compartidos.
6. Configuraciones de cuentas de usuarios y passwords.
7. Posibles vulnerabilidades de bases de datos.
8. Posibles vulnerabilidades de autenticación.
9. Posibles accesos no autorizados a información sensible.
10. Posibles vulnerabilidades de memorias corruptas, DoS (Denial of service) y ataques combinados, acceso a interfase de comandos.

Esta lista no es exhaustiva y se incluye como una base mínima a cumplir. El oferente propondrá en su oferta otros puntos a evaluar que él considere que son necesarios para cumplir con el objetivo de la contratación.

Estos trabajos deben incluir toda la red interna del organismo. A los efectos la cotización se cotizará por hora de trabajo, estimado un total necesario de 1000 (mil) horas-hombre de profesionales especializados.

Este relevamiento deberá realizarse desde las oficinas de Sistemas de CONAE, previa coordinación con el personal de la Unidad.

Toda la documentación se entregará en formato impreso y electrónico (pdf), en castellano o en inglés.

3. Capacitación

Será parte de los servicios la capacitación de hasta tres agentes profesionales de CONAE en el uso de herramientas profesionales avanzadas que permitan a los mismos realizar relevamientos periódicos del status de la nube de CONAE y reaccionar ante eventos críticos. La oferta incluirá una propuesta de plan de capacitación indicando el nivel de conocimientos mínimo requerido para ese personal. Dicho plan será evaluado por CONAE y ajustado con el proveedor según las necesidades del Organismo después de la emisión de la Orden de Compra.

1. Servicio de capacitación e intercambio de conocimientos.
2. Capacitar respecto del “ataque de día cero” y cómo proteger de manera efectiva los sistemas de CONAE.
3. Curso de orientación para CONAE y el equipo cibernético sobre amenazas en el campo cibernético.
4. Se implementará la formación en el lugar de trabajo, para cada producto, de acuerdo al mapa de estrategia cibernética, aprobado por la organización.

4. Asistencia técnica

Durante la vigencia del contrato para consultas y la solución de problemas, eventos e incidentes críticos. Procesos de análisis forenses si estos fueran necesarios.

Deberá incluirse también un equipo adicional de "respuesta ante incidentes" que reaccione a ataques en tiempo real, en modo de alerta las 24 horas, los 7 días de la semana, para reaccionar ante ciberataques e incidentes de fuga de información.

5. Entregables.

Al finalizar cada actividad o tarea el proveedor deberá entregar a la CONAE:

1. Reporte de estado: debe brindar un informe inmediato en caso que se detecten alguna vulnerabilidad crítica, y las recomendaciones para su mitigación inmediata.
2. Dos reportes semanales durante el desarrollo del proyecto.
3. Reporte ejecutivo de resultados relevantes.
4. Resumen de gestión
5. Informe detallado y documentación soporte del trabajo realizado.
6. Recomendaciones y plan de tareas en corto y mediano para implementar las mejoras identificadas/recomendadas para minimizar los riesgos y vulnerabilidades detectadas.
7. Ampliación del proceso de defensa y ciberseguridad.
8. Entrenamiento en la concientización de ciberseguridad
9. Plan de capacitación para CONAE y el equipo cibernético.

6. Plan de trabajo

El oferente deberá presentar un plan de trabajo y un cronograma, con una carga horaria total de 1000 (mil) horas-hombre de profesionales especializados como máximo, que es lo que CONAE estima como carga de trabajo suficiente para cumplir con lo requerido.

Los trabajos de capacitación se realizarán dentro del horario normal laboral de CONAE. Si fuera necesario se coordinará con el responsable de Sistemas los horarios o días alternativos.

El personal del oferente asignado que realizará los trabajos en las sedes de CONAE deberá cumplir con las normas institucionales, en lo que hace a ingreso, seguridad física, normas de comportamientos internas, uso de instalaciones y seguros entre otras (Ver Anexo VI NORMAS GENERALES DE CUMPLIMIENTO OBLIGATORIO PARA PROVEEDORES del presente Pliego)

7. Duración

El contrato tendrá una duración de 6 (seis) meses a partir de la fecha de recepción de la Orden de Compra, durante el cual se realizarán un mínimo de una actividad de black box, y dos de white box en fechas a convenir.

8. Antecedentes y oferta

Antecedentes necesarios para la empresa que realizará los trabajos:

1. Ciberseguridad como objeto primario de la empresa, y su principal especialidad.
2. La empresa deberá tener comprobada experiencia en ciberseguridad.

3. Clientes de primera línea, nacionales y/o internacionales en: telecomunicaciones, plantas industriales, agencias gubernamentales e instituciones financieras.
4. Desarrollos y/o implementaciones de seguridad con sistemas Fortinet y HP. (condición excluyente)
5. Personal con antecedentes y experiencia en ciberseguridad. Incluir CVs abreviados.
6. El proveedor deberá probar/demostrar que la empresa tendrá la habilidad de utilizar herramientas cibernéticas del departamente de R&D de la empresa y no confiar en herramientas automáticas de terceros.
7. El proveedor deberá tener un registro probado en los tres departamentos principales de operaciones: ofensivas civiles/militares, defensivas, investigación y análisis tales como: instalaciones críticas, oficinas de Gobierno, entre otras.

CONAE podrá solicitarles a los oferentes información adicional sobre los antecedentes presentados para corroborar o ampliar los mismos, lo que deberá ser contestado dentro de los 3 días. Si esto no sucediera o no se pudieran corroborar los antecedentes presentados y dado que los mismos se consideran esenciales para evaluar la calidad de la oferta, se podrá considerar, a los efectos de la elaboración del Informe Técnico, que la misma no cumple con los requerimientos técnicos aquí solicitados.

El oferente presentará el equipo de trabajo que interactuará con el personal de la CONAE. Este equipo deberá estar conformado por profesionales con amplios conocimientos en las distintas tecnologías informáticas relacionadas con ciberseguridad, así como también con experiencia comprobable de trabajos similares en compañías de primera línea a nivel nacional y/o internacional.

La oferta incluirá una propuesta detallada del proyecto, plan de entrenamiento y un cronograma preliminar para el inicio y ejecución de las actividades de Black y White box. Un cronograma definitivo será elaborado al finalizar el relevamiento de la red interna y se pueda determinar el alcance real de los trabajos. En ningún caso el cronograma definitivo puede superar los 6 (seis) meses, contados desde la fecha de la recepción de la Orden de Compra.

La oferta enumerará las herramientas profesionales avanzadas a utilizar para realizar las tareas y sobre las cuales se hará la capacitación del personal.

9. Confidencialidad

Se firmará un acuerdo de confidencialidad de la información. (Ver Anexo A)
Por razones de seguridad no se suministrarán otras informaciones, sobre la configuración o arquitectura de la red de CONAE, a las ya incluidas en este pliego. Los oferentes que cumplan los puntos **8.1 a 8.7 (Antecedentes y oferta)** y estimen que, para dimensionar los trabajos, requieren información adicional a la ya incluida, deberán cotizar cada una de las alternativas que consideren posibles en forma completa, tal como es requerida en este anexo. CONAE elegirá la oferta alternativa que considere más conveniente antes de la adjudicación.

10. Otros gastos

El servicio cotizado deberá incluir todos los gastos que demande la realización del trabajo, ya sea por traslado, hospedaje, viáticos, u otros.

11. Cotización

- La cotización debe incluir el IVA. Podrá realizarse en Pesos argentinos o en Dólares estadounidenses. En este último caso los pagos se realizarán en Pesos argentinos al tipo de cambio vendedor de BANCO DE LA NACION ARGENTINA vigente al momento de la acreditación bancaria correspondiente.

- *La oferta deberá indicar el precio unitario de la hora-hombre de un profesional especializado y discriminar las tareas a realizar detallando el total nominal las horas-hombre asignadas a cada tarea, así como el costo total para esa tarea.*

12. Plazo de entrega

Los primeros trabajos (Black Box) se comenzarán dentro los 10 días corridos de recibida la OC.

13. Forma de pago

Pagos parciales con la aceptación por parte de CONAE de la finalización adecuada de la tarea, incluyendo la recepción de los entregables acordados.

Anexo A

ACUERDO DE CONFIDENCIALIDAD

Este ACUERDO DE CONFIDENCIALIDAD ("ACUERDO") se celebra entre la empresa…… ("Parte Receptora"), y la Comisión Nacional de Actividades Espaciales ("Parte Reveladora"), ambas organizadas bajo las leyes de la República Argentina y surtirá efectos a partir del… de…….de 201…

Con referencia a la revelación de información confidencial entre la Comisión Nacional de Actividades Espaciales y la Parte Receptora, y considerando los acuerdos, contratos y convenios vigentes entre las partes, estas convienen es este acto lo siguiente:

1. Información Confidencial y Materiales Confidenciales

(a) "Información Confidencial" significa información no pública que la Parte Reveladora identifique como confidencial o las que, bajo las circunstancias que rodean a la revelación, deba ser tratada como confidencial. "Información Confidencial" incluye, sin limitación, información relacionada con productos de software o de hardware de la Parte Reveladora lanzados o no a la venta, al mercadeo o promoción; de cualquier producto de la Parte Reveladora; prácticas o políticas comerciales de la Parte Reveladora; datos de ingeniería de desarrollos de hardware o software; configuración de equipos y redes; listados y otros datos de clientes, usuarios y empleados; interfaces; diseños gráficos; así como toda información recibida de terceros que la Parte Reveladora está obligada a tratar como confidencial. Toda Información Confidencial revelada a la Parte Receptora por cualquier compañía o entidad subsidiaria o agente ("afiliados") de la Parte Reveladora se contempla en este ACUERDO.

(b) La Información Confidencial no incluye ninguna información que: (i) sea o llegue a ser pública y disponible de una forma que no constituya violación por parte de la Parte Receptora de cualquier obligación hacia la Parte Reveladora; (ii) o que haya sido conocida por la Parte Receptora antes de que la Parte Reveladora le diera a conocer dicha información (iii) o que sea conocida por la Parte Receptora a través de una fuente diferente de la Parte Reveladora y que no sea a través del incumplimiento de una obligación de confidencialidad debida a la Parte Reveladora o (iv) que haya sido desarrollada independientemente por la Parte Receptora.

(c) "Materiales Confidenciales" son todos los materiales tangibles que contienen información confidencial, incluyendo sin limitación, documentos escritos o impresos, cintas, discos o disquetes para computadoras que puedan leerse por computadoras o personas.

2. Restricciones

(a) La Parte Receptora no revelará ninguna Información Confidencial a terceros. La Parte Receptora podrá revelar Información Confidencial solamente si la Parte Reveladora se lo autoriza expresamente.

(b) La Parte Receptora deberá tomar las medidas de seguridad que sean razonables y por lo menos tan efectivas como las que tome para proteger su propia Información Confidencial, para mantener confidencial la Información Confidencial. La Parte Receptora puede revelar Información Confidencial

o Material Confidencial solo a los empleados o asesores de la Parte Receptora que necesiten conocerla. La Parte Receptora ha celebrado o celebrará contratos escritos apropiados con sus empleados y asesores que sean suficientes para permitir el cumplimiento de todas las disposiciones de este ACUERDO.

(c) La Parte Receptora se compromete a separar todos los Materiales Confidenciales de los materiales confidenciales de terceros para evitar que se mezclen.

(d) La Parte Receptora no realizará ingeniería inversa o regresiva, no descompilará o desensamblará ningún software o programa revelado a la Parte Receptora.

3. Derechos y Recursos

(a) La Parte Receptora notificará inmediatamente a la Parte Reveladora del descubrimiento de cualquier uso no autorizado o revelación de la Información Confidencial y/o de los Materiales Confidenciales, o de cualquier otro incumplimiento de este ACUERDO por la Parte Receptora y cooperará con la Parte Reveladora de forma razonable para ayudar a la Parte Reveladora a recuperar la posesión de la Información Confidencial y/o de los Materiales Confidenciales y prevenir su futuro uso no autorizado.

(b) La Parte Receptora devolverá todos los originales, copias, reproducciones y resúmenes de la información Confidencial o de los Materiales Confidenciales a pedido de la Parte Reveladora o, a opción de la Parte Reveladora, certificará la destrucción de la misma.

(c) La Parte Receptora reconoce que la compensación de los daños monetarios podría ser insuficiente en ese caso de revelación de la Información Confidencial, y que la Parte Reveladora tendrá derecho, sin que ello constituya una renuncia, a cualesquiera otros derechos o recursos, a pedir y obtener órdenes judiciales de hacer o de no hacer que fueran consideradas apropiadas por un tribunal competente.

(d) La Parte Reveladora puede inspeccionar las instalaciones de la Parte Receptora mediante previo aviso razonable y durante las horas normales de oficina, para verificar el cumplimiento de las disposiciones de este ACUERDO por la Parte Receptora.

4. Otras Disposiciones

(a) Toda la Información Confidencial y los Materiales Confidenciales, son y permanecerán propiedad de la Parte Reveladora. Al revelar información a la Parte Receptora y/o sus afiliados, la Parte Reveladora no otorga ningún derecho explícito o implícito a la Parte Receptora sobre ninguna patente, derecho de autor, marca comercial o de fábrica, o información comercial secreta.

(b) Si cualquiera de las partes proporciona software que no ha sido lanzado al mercado como Información Confidencial o Material Confidencial, de acuerdo a este ACUERDO dicho software preliminar se proveerá “tal como está” sin ninguna clase de garantía. La Parte Receptora conviene que la Parte Reveladora ni sus afiliados serán responsables por cualquier daño relacionado al uso que haga la Parte Receptora de dicho software preliminar.

(c) Cualquier software y documentación que se provea de conformidad con el presente ACUERDO se proporciona con DERECHOS RESTRINGIDOS.

(d) Las disposiciones de confidencialidad contenidas en este ACUERDO no se interpretarán como limitaciones al derecho de las partes a desarrollar o adquirir independientemente productos sin usar la Información Confidencial de la otra parte. Cada parte será libre de usar para cualquier propósito los residuos que resultaren del acceso a, o del trabajo, con Información Confidencial, bajo la condición de que dicha parte mantenga la Información Confidencial en secreto, de conformidad con

las disposiciones de este ACUERDO. El término “residuos” significa información en una forma no tangible, la cual puede haber sido retenida por las personas que han tenido acceso a la Información Confidencial, incluyendo ideas conceptos, know-how o técnicas contenidas en ellos. Ninguna parte tiene la obligación de limitar o de restringir las funciones de tales personas o de pagar regalías por cualquier trabajo que resulte del uso de los residuos. Sin embargo, lo anterior no otorga a ninguna de las partes una licencia sobre las patentes o derechos de autor de la otra parte.

(e) Este ACUERDO constituye el contrato completo entre las partes con relación a la materia del mismo. Este ACUERDO no podrá ser modificado excepto por convenio escrito con fecha posterior a la de este ACUERDO y suscrito por ambas partes. Ninguna de las disposiciones de este ACUERDO se tendrá por renunciadas por cualquier acto o consentimiento de la Parte Reveladora, sus agentes o empleados, excepto mediante documento escrito firmado por un funcionario autorizado de la Parte Reveladora. Ninguna renuncia a las disposiciones de este ACUERDO constituirá una renuncia a cualquiera de las otras disposiciones o a la misma disposición en otra ocasión.

(f) Si cualquiera de las partes contratan los servicios de abogados para hacer cumplir cualquier derecho derivado o relacionado con este ACUERDO, la parte que prevalezca tendrá derecho a recuperar los horarios legales que fueren razonables. Este ACUERDO se interpretará y será regido por las leyes de la República Argentina. A tal fin, las partes constituyen domicilio en los indicados al pié del presente ACUERDO, y acuerdan someterse a la competencia de los Tribunales Federales Nacionales de la Capital Federal, renunciando a todo otro fuero o jurisdicción.

(g) Sujeto a las limitaciones establecidas en este ACUERDO, el mismo surtirá efectos para el beneficio de ambas partes y será obligatorio para las mismas, para sus sucesores y cesionarios.

(h) Si cualquier disposición de este ACUERDO fuese declarada ilegal, inválida o inejecutable por la autoridad judicial competente, las demás disposiciones permanecerán con pleno vigor y eficacia.

(i) Todas las obligaciones creadas por este ACUERDO prevalecerán sobre las modificaciones o terminación de la relación de negocios entre las partes.

En prueba de conformidad se firman dos ejemplares de un único y mismo tenor y a un solo efecto, en la Ciudad Autónoma de Buenos Aires, a los… días del mes de… de 20…

Por CONAE	Por la EMPRESA
Dirección: Paseo Colón 751	Dirección:
Ciudad Autónoma de Buenos Aires	
Firma por CONAE:	Firma por la EMPRESA:
Nombre	Nombre:
Cargo:	Cargo: