Pliego 059-2024

Buenos Aires, 24 de Junio 2024

Razón Social
Domicilio:
Código Postal:
Municipio:
Provincia:
Teléfono:
Contacto Ventas:
Contacto Cobranzas:
Mail:
C.U.I.T.:
Banco:
Nº Cuenta:
C.B.U.:

COMPLETAR CON LOS DATOS DE LA FIRMA

De mi consideración:

Tengo el agrado de dirigirme a Ud. a fin de solicitarle se sirva enviar presupuesto por lo siguiente

		COTIZAR CON IVA INCLUIDO			
ITEAM	DESCRIPCIÓN	UNIDAD	CANT	PRECIO UNITARIO	TOTAL
1	**Licencia de reconocimiento, vulnerabilidad y búsqueda de información.**	C/U	1		
2	**Licencia de soporte avanzado**	C/U	1		
3	**Licencia de repuesta a incidente**	C/U	1		
4	**Servicio de operación asistida**	MES	6		
			Total		

Para presentar la OFERTA,
Ver artículo 15º del PLIEGO UNICO DE BASES Y CONDICIONES GENERALES (requisitos)
Aclaración: Aquellos oferentes que se encuentren registrados en el Sistema de

Información de proveedores (SIPRO) de la Administración Publica Nacional, y su estado sea INSCRIPTO, no estarán obligados a presentar la documentación requerida en el articulo 15, inciso G apartado VII del Pliego de Bases y Condiciones Generales del Fondo de Cooperación Tecnica y Financiera-CECBA-PSA Ley Nº 26.102 – Dto. 742-21 O.P., debiendo acreditarlo con la presentación de su certificado de inscripción.

LICENCIAMIENTO INTEGRAL DESTINADO A LA DETECCIÓN PREVIA DE POSIBLES VECTORES DE ATAQUE DE CIBERSEGURIDAD

ESPECIFICACIONES TÉCNICAS

OBJETO

El presente requerimiento tiene por objeto la adquisición de un Licenciamiento integral destinado a la detección previa de posibles vectores de ataque de ciberseguridad con el fin de prevenir incidentes, la colaboración con un equipo de servicio de respuesta a incidentes durante un posible evento de ciberseguridad y la colaboración posterior a un ataque, detectando posibles robos de información o suplantación de identidad y mitigarlos.
Los servicios serán prestados a la Policía de Seguridad Aeroportuaria (PSA), organismo actuante en la órbita del Ministerio de Seguridad; en un todo de acuerdo con las especificaciones descriptas en el presente documento.

BIENES Y/O SERVICIOS SOLICITADOS

Renglón	Descripción	Cantidad	Unidad de medida
1	Licencia de reconocimiento, vulnerabilidades y búsqueda de información	1	Unidad
2	Licencia de soporte avanzado	1	Unidad
3	Licencia de respuesta a incidente	1	Unidad
4	Servicio de operación asistida	6	Mes

RENGLON N° 1: LICENCIA DE RECONOCIMIENTO, VULNERABILIDADES Y BÚSQUEDA DE INFORMACIÓN:

La solución ofertada deberá tratarse de una licencia que permita realizar inteligencia sobre las amenazas de los activos vulnerables expuestos a los posibles atacantes de la PSA, y evaluar el nivel de riesgo con herramientas y tácticas que utilizan los atacantes. Asimismo, deberá incluir servicios de búsqueda de suplantación de identidad del organismo con fines delictivos y monitoreará posibles robos de información. El licenciamiento deberá ser por el término de TREINTA y SEIS (36) meses.

REQUERIMIENTO TÉCNICO

La licencia de reconocimiento, vulnerabilidades y búsqueda de información ofertada deberá cumplir con los siguientes lineamientos:

1. Brindar un mejor manejo y visibilidad del riesgo digital.
2. Permitir el monitoreo y gestión de riesgo de 2000 activos.
3. Recopilar inteligencia de varias fuentes, como Darkweb, Open Source e Investigación técnica, entre otras.
4. Tener una calificación de confianza basada en el estándar de la industria, como (Admiralty System) para todos los informes publicados. Permitir que los informes de inteligencia sean calificados según criterios de relevancia específicos para el panorama de amenazas específicos de la Fuerza.
5. Permitir que los informes de inteligencia sean calificados según criterios de relevancia específicos para el panorama de amenazas específicos de la Fuerza.
6. Cubrir todas las amenazas relevantes para el sector de la industria aerocomercial y los ataques a organismos públicas nacionales e internacionales.
7. Supervisar e informar sobre amenazas en Nuevas vulnerabilidades y exploits que se discuten activamente en Dark web y fuentes abiertas.
8. Encontrarse asignada al marco MITRE ATT&CK.
9. Proporcionar actualizaciones en tiempo real, a medida que se recopila nueva información o contexto de diversas fuentes.
10. Proporcionar inteligencia sobre fugas de credenciales a través de infracciones de terceros en una vista de línea de tiempo limpia.
11. Permitir una fuerte presencia en los sitios de darknet examinados y solo por invitación, como foros y mercados.
12. Realizar un monitoreo extensivo de Dark Web para inteligencia específica de la PSA mediante el monitoreo de salas de chat ocultas, sitios web privados, redes punto a punto, plataforma de redes sociales, sitios del mercado negro y botnets.
13. Realizar descubrimientos de datos filtrados en la dark web, incluidos archivos confidenciales, datos financieros/de tarjetas de crédito, PII, etc.
14. Tener la capacidad de interactuar con actores en Dark Web y recopilar inteligencia a través de HUMINT.
15. Tener la habilidad de pivotar hacia la inteligencia en términos de varios filtros tales como:
    - Nombre del adversario;
    - Motivación adversaria;
    - Industria de destino;
    - Geografía objetivo;
    - Tipos de informes;
    - Calificaciones de relevancia;
16. Poseer la capacidad para producir informes de alerta temprana basados en ataques iniciales y futuros y nuevos TTP.
17. Tener capacidad para informar exclusivamente sobre ataques de Ransomware y TTP relacionados.
18. Permitir realizar una investigación inicial dentro del sistema utilizando enriquecimientos en tiempo real para buscar IOC.

19. Permitir el seguimiento y monitoreo de marca como:
    - Detectar credenciales violadas, es decir, correos electrónicos. (En caso de clientes Bancarios también se pueden incluir los datos de la Tarjeta);
    - Identifique las credenciales filtradas que están disponibles en la dark web;
    - Identificar la fuente de la violación de datos (incluidos terceros);
    - Detectar información filtrada y datos confidenciales;
    - Capacidad de monitorear a la PSA como marca para cualquier ataque de phishing inminente;
    - Hacer detección de sitios de phishing mediante el uso de marcas de agua digitales; Identificar la dirección IP y los correos electrónicos de los usuarios phishing a través de campañas de phishing;
    - Identificar la dirección IP y los correos electrónicos de los usuarios phishing a través de campañas de phishing;
    - Capacidad para identificar nombres de dominio de apariencia similar que coincidan estrechamente con el Cliente;
    - Servicio de eliminación: eliminación de contenido sospechoso (sitios/perfil/etc.);
20. Realizar exposición y escaneo de Shadow IT: escaneos de puertos, dispositivos mal configurados, escaneos de certificados SSL, etc.
21. Tener soporte para categorizar los hallazgos de inteligencia de amenazas a través de MITRE ATT&CK Framework, etc.
22. Mostrar vulnerabilidades o configuraciones incorrectas del servidor (nube/en premisas).
23. Contar con informes de activos vulnerables y activos de shadow IT.
24. Tener la capacidad para escanear y monitorear la infraestructura de Internet de la PSA con el objeto de:
    - Identificar de Activos;
    - Identificar el cambio en los activos frente a Internet;
    - Identificar de Cambios en Puertos abiertos;
    - Identificar cualquier certificado SSL caducado o a punto de caducar;
25. Poseer funciones para analizar e investigar los IOC a pedido, como búsquedas de reputación de IP/Dominio/Hash/CVE para varios parámetros:
    - Información básica;
    - Búsqueda de listas negras;
    - Ubicación geográfica;
    - Información de la red;
    - Informes de inteligencia previos;
26. La plataforma debe tener características para integrarse con plataformas de colaboración como Microsoft Teams o Slack.
27. La plataforma debe tener funciones para proporcionar acceso basado en roles, alertas personalizadas, alertas de flash, etc.
28. Debe tener la capacidad de proporcionar analista por demanda para cualquier requerimiento de aclaración e investigación personalizada.

29. Debe admitir seguridad adicional al proporcionar autenticación de dos factores para el portal web.

RENGLON N° 2: Licencia de Soporte Avanzado:
La solución ofertada deberá tratarse de una licencia que permita mantener y optimizar los servicios fundamentales de ciberseguridad a través de recursos especializados, atención especializada, gestión proactiva de tickets, conferencias de seguimiento y capacitaciones, de la plataforma de ciberseguridad. El licenciamiento deberá ser por el término de TREINTA y SEIS (36) meses.

REQUERIMIENTO TÉCNICO
La Licencia de soporte avanzado ofrecidos por fabricante ofertada deberá cumplir con los siguientes lineamientos:

1. Poseer servicio premium de fábrica, con niveles de atención diferenciales y enrutamiento de los casos de la entidad a un grupo de ingenieros especializados.
2. Incluir una reunión de inicio, en la cual se realizará un intercambio de la información necesaria para la configuración y operación correctas del servicio.
3. Incluir la designación de un ingeniero líder en la región enfocado en la resolución de los tickets generados por la PSA, la disponibilidad horaria deberá ser de lunes a viernes por OCHO (8) horas.
4. Incluir una capacitación online certificada incluyendo vouchers de certificación, para 10 personas, la cual deberá tener una duración mínima de OCHO (8) horas.
5. Incluir la gestión proactiva de tickets para actividades técnicas programadas fuera de horario, incluida la revisión de información y la redirección con equipos globales.
6. Incluir conferencias telefónicas periódicas para realizar un seguimiento de los tickets abiertos e informar el progreso.
7. Incluir una revisión trimestral, que cubra el análisis general de los tickets/actividades en curso y la obsolescencia de HW y SW.
8. Proporcionar informes de análisis de causa raíz (RCA) para incidentes críticos (Prioridad- 1 y Prioridad-2) relacionados con los dispositivos ofertados.
9. Incluir asistencia en la actualización de al menos uno de los dispositivos incluidos en la oferta, la asistencia puede incluir recomendación de software, pruebas de actualización y/o asistencia para la planificación.
10. Proporcionar al menos una recomendación de software anual para cualquiera de las familias de dispositivos incluidos en la oferta, basados en una depuración de bugs y en los requisitos operativos.
11. Notificar a la entidad de cualquier problema crítico abierto que pueda afectar su entorno.
12. Realizar al menos una reunión o asistencia técnica de forma presencial en la PSA, esta se acordará de forma previa con el Adjudicatario.
13. Realizar al menos dos asistencias remotas fuera del horario de atención para las ventanas de mantenimiento indicadas por la PSA, estas se acordarán de forma previa con el Adjudicatario.
14. Incluir una transferencia de conocimiento vía web en la que se explique una de las características configuradas en uno de los equipos de la entidad, la sesión debe incluir troubleshooting y recomendaciones a los problemas comúnmente vistos.

RENGLON N° 3: Licencia de respuesta a incidentes:

La solución ofertada deberá tratarse de una licencia que permita dar respuesta a incidentes administrada por el fabricante, a través de un equipo especializado en respuesta a incidentes que admita tomar acciones de remediación frente a un ataque o encontrar causa raíz.El licenciamiento deberá ser por el termino de DOCE (12) meses.

Durante la vigencia de la licencia se deberán generar los procesos y procedimientos de cómo prevenir un posible ataque informático, que tareas realizar durante el mismo y las tareas posteriores.

REQUERIMIENTO TÉCNICO

La Licencia de respuesta a incidentes ofertada deberá cumplir con los siguientes lineamientos:

1. Suministrar un servicio de evaluación inicial del plan de respuesta a incidentes de la entidad y proporcionar un informe del nivel de madurez, los resultados de la evaluación y un conjunto de recomendaciones.
2. Desarrollar con la entidad al menos dos manuales de estrategias de respuesta a Incidentes (playbooks) en caso de que un incidente de ciberseguridad tenga impacto en la red. El manual de estrategias guiará a los analistas de la entidad en la detección, contención, erradicación y recuperación.
3. Probar (ejercicios de simulación) con la entidad al menos dos de los manuales de estrategias de respuesta a incidentes desarrollados a fin de que la entidad cuente con un plan de acción de respuesta a incidentes claro y conciso.
4. Incluir la capacidad de brindar ayuda inicial a la entidad (4 horas) si un incidente de seguridad se presenta y de ofrecer bolsas de horas adicionales de acuerdo al soporte requerido para la detección, análisis, contención, reducción del impacto del incidente y recuperación de las operaciones.
5. Realizar una evaluación final del plan de respuesta a incidentes de la entidad y proporcionar un informe del nivel de madurez, los resultados de la evaluación y un conjunto de recomendaciones.
6. Poner a disposición ante la respuesta a incidentes de un equipo de trabajo que permita detectar como el atacante ingreso a la red o sistemas, si aún están dentro, toda huella que deje, que accesos han logrado y como erradicar y reparar la amenaza.
7. Cubrir todas las amenazas relevantes para el sector de la industria y los ataques a organizaciones pares del Cliente en la India e internacionalmente.
8. Deberá garantizar un SLA de una hora con un régimen de trabajo 24x7 (veinticuatro horas durante los siete días de la semana).
9. Garantía de nivel de servicio (SLA) desde que se produce el reporte de un incidente hasta el involucramiento del equipo no podrá ser superior a UNA (1) hora.

RENGLON N° 4: Servicio de Operación asistida:

Se solicita un Servicio de operación asistida, por el término de SEIS (06) meses, durante dicho servicio el adjudicatario trabajara en forma conjunta con la PSA, con el fin de mejorar las implementaciones de ciberseguridad y networking actuales, de manera de poder automatizar por completo los procesos de prevención, detección y respuesta de ciberseguridad.

El servicio mensual constará de OCHENTA (80) horas de servicios profesionales, las mismas serán utilizadas a requerimiento del área técnica de la PSA.

MODALIDAD DEL SERVICIO

El servicio deberá ser brindado los días hábiles en la franja horaria de 9 a 18 horas, el mismo podrá ser brindado bajo modalidad remota.

ALCANCE DEL SERVICIO

El servicio será utilizado para recibir la configuración y el asesoramiento sobre funcionalidades de las siguientes soluciones:

FortiGate 1800 – Sitio Central – Cantidad 1
FortiGate FG-60 – Sitios Remotos – Cantidad 40
FortiAuthenticator – Cantidad 1
FortiWeb – Cantidad
1 FortiDDoS – Cantidad 1
FortiMail – Cantidad 1
FortiSandbox – Cantidad 1
FortiSIEM – Cantidad 1
FortiDeceptor – Cantidad 1
FortiAP (Configuración de Controller – Lógico)

CONFIGURACIÓN DE SOLUCIÓN DE CIBERSEGURIDAD CON LOS SIGUIENTES ALCANCES

Firewall de Borde (FG-1800/Sitio Central & FG-60 Sitios Remotos)

Asesoría para el armado de Policy Package de Seguridad y QoS en la arquitectura actual SDWAN Fortinet que PSA ha implementado:

- Configuración de DOS (2) paquetes de políticas de seguridad, siendo uno para el sitio central HUB y otro compartido para utilizar como template en el resto de los sitios remotos SPOKEs.
- Configuración de DOS (2) perfiles de calidad de servicio para diferente tipo de tráfico.

FortiAuthenticator:

El alcance de los servicios profesionales será:

- Configuración de direccionamiento IP de la solución.
- Integración de perfiles de seguridad.
- Integración con AD.
- Creación de perfiles de seguridad por grupos de usuarios (máximo TRES -3- perfiles).
- Integración con DOS (2) sistemas actuales de PSA, que serán definidos por el área técnica una vez emitida la orden de compra.

Firewall Web:

El alcance de los servicios profesionales será:

- Análisis de la configuración teniendo presente los servicios actuales.
- Revisión de falla de los sitios internos debido a “x forward for”.
- Revisión de estado de funcionalidad de sitios internos.
- Configuración de hasta CUATRO (4) políticas de seguridad para defender aplicaciones web internas de ataques típicos como inyección de SQL y ataques de denegación de servicio (DoS). Configuración de hasta DOS (2) perfiles de seguridad para mitigar ataques típicos de seguridad mediante técnicas de análisis de patrones de tráfico, ajustando parámetros como la inspección de protocolo, la validación de entrada y la detección de patrones maliciosos.
- Vinculación con: FortiAnalyzer y FortiSIEM.

FortiMail:
El alcance de los servicios profesionales será:

- Configurar modo de operación.
- Configuración de direccionamiento IP de la solución.
- Configuración de licenciamiento.
- Definición de dominios a consolidar.
- Aplicar reglas de seguridad.
- Aplicar políticas de Antispam y Antivirus.
- Aplicar filtrado estático por palabras o frases baneadas.

FortiSandbox: Planificación y configuración de UN (1) FortiSandbox
El alcance de los servicios profesionales será:

- Configuración básica del FortiSandbox y licencia Sandbox Threat Intelligence.
- Vincular con: FortiAnalyzer, FortiDDOS, FortiWeb, FortiMail, FortiGate y FortiSIEM.

FortiSIEM:
El alcance de los servicios profesionales será:

- Agregación de servers
- Agregación de hasta DIEZ (10) endpoints
- Dashboard: Configuración hasta DOS (2) dashboards distintos.
- Configurar interfaces del sistema y zonas horarias para cada dispositivo.
- Configurar la puerta de enlace SMTP.
- Configurar las Credenciales necesarias.
- Asignar credenciales proporcionadas por el organismo de descubrimiento a direcciones IP y subredes.
- Políticas de notificación y manejo de incidentes: Crear y ajustar hasta TRES (3) políticas de notificación.

FortiDDoS:
El alcance de los servicios profesionales será:

- Análisis de configuración actual y respectivos servicios activos.
- Revisión del diseño de implementación realizado.
- Revisión de las alertas del equipo legacy de PSA para ver la factibilidad de conversión al modelo arquitectónico del FortiDDoS. Definición de hasta VEINTE (20) alertas a traspasar del modelo legacy al FortiDDoS.
- Definición de hasta VEINTE (20) alertas a traspasar del modelo legacy al FortiDDoS.
- Elaboración de templates de configuración de las alertas definidas y su respectiva implementación.
- Definición de la modalidad de integración a red en el cliente (Simple Deployment o Multiple Service Providers Deployment).
- Validación de existencia de balanceadores de tráfico y su integración al servicio.
- Creación hasta TRES (3) perfiles de usuarios de gestión.
- Configuración hasta CINCO (5) Service Protection Policy.

Controller para Access Points: Configuración de los los FortiGates del Sitio Central como controller para el servicio WiFi
El alcance de los servicios profesionales será:

- Licenciamiento y configuración inicial de administración.
- Despliegue lógico y registro de OCHO (8) APs (Access Points) en controladora.
- Creación de perfiles de radio.
- Configuración de DOS (2) SSIDs.
- Configuración de reglas de seguridad.

FortiDeceptor:
El alcance de los servicios profesionales será:

- Configuración de direccionamiento IP de la solución.
- Configuración de licenciamiento.
- Implementación de aprendizaje automático y reconocimiento de activos a proteger.
- Configuración de hasta DIEZ (10) Decoys con configuración automática según el inventario de activos a proteger.
- Configuración de hasta CINCO (5) Honeypots con configuración estándar.
- Vinculación con: FortiAnalyzer, FortiDDOS, FortiGate y FortiSIEM.

DOCUMENTACION A PRESENTAR CON LA OFERTA

Los oferentes deberán acompañar:

a) Certificado de Representación, emitido por FORTINET, específicamente para este procedimiento de licitación, del cual surja expresamente que la firma oferente se encuentra habilitada a presentar la cotización.
b) Folletería y descripción técnica de las características del software ofrecido. En caso de presentarse folletos o notas técnicas deberán ser en español, dejándose expresa constancia que las mismas podrían llegar a ser verificadas contra el material en el sitio web del fabricante.
c) Deberán acreditar la realización de proyectos de características técnicas similares (preferentemente con Organismos públicos), indicando:
    - Nombre de la Empresa / Organismo.
    - Dirección.
    - Nombre y Apellido del responsable.
    - Orden de compra (en caso de corresponder).

BASES Y CONDICIONES PARTICULARES

Entidad Contratante: **FONDO DE COOPERACIÓN TÉCNICA Y FINANCIERA – CECBA – PSA – LEY 26102 – DTO.742-21 O.P**
CUIT: **30-71749460-8**
Domicilio legal: **AV. CALLAO 1542**
Localidad: **CIUDAD AUTÓNOMA DE BUENOS AIRES**
Provincia: **BUENOS AIRES**
Correo electrónico de contacto: **compras@colegio-escribanos.org.ar**
Teléfono de contacto: **4809-7000**
Modalidad de Contratación: **COMPULSA DE OFERTAS**
Número de proceso de contratación: **PLIEGO 059/2024**
Rubro o actividad comercial: **LICENCIA DE SOFTWARE**
Objeto de la contratación: **ADQUISICION DE LICENCIAMIENTO INTEGRAL DESTINADO A LA DETECCION PREVIA DE POSIBLES VECTORES DE ATAQUE DE CYBERSEGURIDAD.**
Costo del Pliego: **SIN COSTO**
Medio de difusión: **INVITACIONES + PAGINA WEB PSA**
Consultas y Aclaraciones: **HASTA 48 HORAS ANTES DE LA FECHA Y HORA DE APERTURA DE OFERTAS**
Fecha y horario de apertura de ofertas: **03/07/2024 – 15:30 hrs**
Fecha y horario límite para la presentación de ofertas: **03/07/2024 – 15:00hrs**
Modalidad de presentación de ofertas: **DIGITAL (archivos .PDF)**
Lugar de presentación y recepción de ofertas: **CORREO ELECTRÓNICO (compras@colegio-escribanos.org.ar).**

CLÁUSULAS PARTICULARES

ARTÍCULO 1°. - COMUNICACIONES Y NOTIFICACIONES

Todas las comunicaciones y notificaciones entre el ENTE COOPERADOR y los/las interesados/as, oferentes, adjudicatarios/as o cocontratantes, se realizarán de acuerdo a lo establecido en el artículo N°5 del PLIEGO ÚNICO DE BASES Y CONDICIONES GENERALES DEL FONDO DE COOPERACIÓN TÉCNICA Y FINANCIERA - CECBA - PSA - LEY 26102 - DTO.742-21 O.P.

Asimismo, se consideran validas aquellas que realice el ENTE COOPERADOR a través del sitio web de la POLICIA DE SEGURIDAD AEROPORTUARIA (https://www.argentina.gob.ar/psa).

ARTÍCULO 2°. - CONSULTAS AL PLIEGO DE BASES Y CONDICIONES PARTICULARES

Las consultas deberán realizarse mediante correo electrónico a la dirección de correo electrónico compras@colegio-escribanos.org.ar, y deberán ser efectuadas hasta DOS (2) días hábiles antes de la fecha fijada para la apertura de ofertas.

ARTÍCULO 3°. - PLAZO DE MANTENIMIENTO DE LA OFERTA.

Los oferentes deberán mantener las ofertas por el término de **treinta (30) días corridos**, contados a partir de la fecha del acto de apertura**. El plazo antes aludido, se renovará en forma automática por un lapso igual al inicial, y así sucesivamente, salvo que el oferente manifestare en forma expresa su voluntad de no renovar el plazo de mantenimiento con una antelación mínima de DIEZ (10) días corridos al vencimiento de cada plazo.**

ARTÍCULO 4°. - COTIZACIÓN.

Los oferentes deberán cotizar por todos los renglones (adjudicación íntegra) y deberán utilizar la tabla de la página 1 del presente Pliego de Cotización.

No se admitirán oferentes por cantidades parciales para cada renglón.

ARTÍCULO 5°. - MONEDA DE COTIZACIÓN.

La propuesta económica deberá ser formulada en DOLARES ESTADOUNIDENSES.

Las Ofertas expresadas en otra moneda, serán automáticamente desestimadas.

Los precios cotizados deberán incluir, indefectiblemente, el importe correspondiente a la alícuota del IVA y todo otro impuesto, arancel o tasa que corresponda abonar para la comercialización. En caso de no hacerse expresa mención a ello en la Oferta, quedará tácitamente establecido que dichos valores se hallan incluidos en la misma.

Los precios cotizados serán considerados a todos los efectos fijos e inamovibles. Se entenderá en consecuencia que se encuentran incluidas en el precio todas las prestaciones que, de acuerdo a su juicio y experiencia, deberá realizar para el fiel y estricto cumplimiento de sus obligaciones, aunque las mismas no estén explicitadas en la oferta.

ARTÍCULO 6°. - GARANTÍA DE MANTENIMIENTO DE OFERTA
Los/las oferentes deberán constituir una garantía de mantenimiento de la oferta del CINCO PORCIENTO (5%) del monto total de la oferta por el plazo de oferta. En el caso de cotizar con descuentos o alternativas, la garantía se calculará sobre el mayor monto propuesta. La garantía de mantenimiento de la oferta, será constituida por el plazo inicial y sus eventuales renovaciones.

ARTÍCULO 7°. - GARANTÍA DE CUMPLIMIENTO DEL CONTRATO
Los/las adjudicatarios/as deberán garantizar el cumplimiento de sus obligaciones contractuales constituyendo una garantía de cumplimiento del contrato del DIEZ PORCIENTO (10%) del monto total del contrato.
El plazo para la presentación de dicha garantía no podrá exceder los TRES (3) días hábiles, contados a partir del día hábil siguiente a la notificación de la mencionada Orden de Compra.

ARTÍCULO 8°. - FORMAS DE LAS GARANTÍAS
Las garantías podrán constituirse de las siguientes formas:
a) **Seguro de caución**, emitido por entidades aseguradoras habilitadas a tal fin por la SUPERINTENDENCIA DE SEGUROS DE LA NACIÓN, extendidas a favor del FONDO DE COOPERACIÓN.

ARTÍCULO 9°. - ADJUDICACIÓN – CRITERIO DE SELECCIÓN
La adjudicación recaerá sobre aquella oferta que, ajustándose en un todo al PLIEGO ÚNICO DE BASES Y CONDICIONES GENERALES DEL FONDO DE COOPERACIÓN TÉCNICA Y FINANCIERA - CECBA - PSA - LEY 26102 - DTO.742-21 O.P. y a lo requerido en el presente pliego particular, resulte **económicamente más conveniente.**

ARTÍCULO 10°. - ADJUDICACIÓN (VER ART. 4 COTIZACIÓN)
La adjudicación se realizará bajo el criterio POR ADJUDICACION INTEGRA.

ARTÍCULO 11°. - ENTREGA.
Plazo/Fecha/Horario: NOVENTA (90) días corridos a partir de la Orden de Compra.
Lugar: of.102- Instituto de Formacion Ezeiza- Autopista Tte. Gral. Ricchieri Km 25.5 S/N- Ezeiza Contacto Martin Fernandez (011)5193-0200 interno 99024
Otros: Coordinacion: Área de Infraestructra, Teléfono N° 5193 0200 Internos 99973 / 99923 / 999723 / 999722. Correo: infraestructura@psa.gov.ar.
Admite entregas parciales: No.

ARTÍCULO 12°. - PLAZO DE PAGO.
El plazo para el pago de las facturas será de hasta QUINCE (15) días corridos a partir de la entrega de

la factura correspondiente.

ARTÍCULO 13°. - MODALIDAD Y MONEDA DE PAGO.

Los pagos se realizarán mediante transferencia bancaria, en PESOS ARGENTINO.

Cotización en moneda extranjera, se calculará el monto del desembolso tomando en cuenta el tipo de cambio vendedor divisa del BANCO DE LA NACIÓN ARGENTINA vigente al momento de la ejecución del pago correspondiente.

ARTÍCULO 14°. - CESIÓN O SUBCONTRATACIÓN.

No podrá subcontratarse o cederse el contrato objeto de la presente contratación.

ARTÍCULO 15°. - AUMENTO O DISMINUCIÓN DEL CONTRATO CON CONSENTIMIENTO DEL CONTRATANTE

Con consentimiento de el/la cocotratante se podrá aumentar por ítem/renglón completo, hasta un SESENTA POR CIENTO (60%).

ARTÍCULO 16°. - ANTICIPO FINANCIERO.

EL/la adjudicatario/a no podrá solicitar un pago anticipado

ARTICULO 17º - MUESTRAS

No se solicitan.

ARTÍCULO 18°. – VISITA A LAS INSTALACIONES

El oferente no deber realizar visitas a las instalaciones.

ARTÍCULO 19°. OPCIÓN DE PRÓRROGA

NO APLICA.

ARTÍCULO 20°. - PENALIDADES.

Los oferentes, adjudicatarios o cocontratantes podrán ser pasibles de las penalidades que se enumeran a continuación.

a) Pérdidas de la Garantía de mantenimiento de oferta:

1.- Si el oferente manifiesta su voluntad de no mantener su oferta fuera del plazo fijado para realizar tal manifestación o retirara su oferta sin cumplir con los plazos de mantenimiento.

b) Pérdida de la garantía de cumplimiento del contrato:

1.- Por incumplimiento contractual, si el cocontratante desistiere en forma expresa del contrato antes de vencido el plazo fijado para su cumplimiento, o vencido el plazo de cumplimiento original del contrato o de su extensión, y habiendo vencido el plazo de las intimaciones realizadas por el ENTE COOPERADOR, en todos los casos, sin que los bienes fueran entregados o prestados los

servicios de conformidad.

2.- Por cesión o subcontratación del contrato sin autorización del ENTE COOPERADOR.

c) Rescisión por su culpa:

1.- Por incumplimiento contractual, si el cocontratante desistiere en forma expresa del contrato antes de vencido el plazo fijado para su cumplimiento, o vencido el plazo de cumplimiento original del contrato o de su extensión, y habiendo vencido el plazo de las intimaciones que realizara el ENTE COOPERADOR, en todos los casos, sin que los bienes fueran entregados o prestados los servicios de conformidad.

2.- Por ceder el contrato sin autorización del ENTE COOPERADOR.

3.- En caso de no integrar la garantía de cumplimiento del contrato luego de la intimación cursada por el ENTE COOPERADOR, quedando obligado a responder por el importe de la garantía no constituida de acuerdo al orden de afectación de penalidades establecido en el presente reglamento.

d) Diferencia de precio por la nueva contratación de la prestación y/o servicio a un tercero, en caso de rescisión contractual por su culpa.

e) Sanción pecuniaria por mora en el cumplimiento de sus obligaciones:

1.- Se aplicará una sanción pecuniaria del CERO COMA CINCO POR CIENTO (0,5%) del valor de lo satisfecho fuera de término por cada día hábil de atraso.

2.- En caso de los contratos de servicios o de tracto sucesivo, que observaran incumplimiento de las pautas establecidas o la falta de resultados satisfactorios, darán lugar a la aplicación de penalidades, de acuerdo al siguiente detalle:

2.a. Primer incumplimiento: sanción pecuniaria del CERO COMO CINCO POR CIENTP (0,5) % de la facturacion mensual

2.b. Segunda incumplimiento: sanción pecuniaria del UNO PORCIENTO (1) % de la facturacion mensual

2.c. Tercer incumplimiento: sanción pecuniaria del DOS PORCIENTO (2) % de la facturacion mensual

2.d. Cuarto incumplimiento: sanción pecuniaria del TRES PORCIENTO (3) % de la facturacion mensual

2.e. Quinto incumplimiento: sanción pecuniaria del CINCO PORCIENTO (5) % de la facturacion mensual

2.f. Sexto incumplimiento: sanción pecuniaria del SIETE PORCIENTO (7) % de la facturacion mensual

2.g. Séptimo incumplimiento: sanción pecuniaria del DIEZ PORCIENTO (10) % de la facturacion mensual.

2.h. Octavo incumplimiento: sanción pecuniaria del QUINCE PORCIENTO (15) % de la facturacion mensual

2.i. Si el adjudicatario y/o cocotratante hubiere cometido más de DIEZ PORCIENTO (10)

incumplimientos, el ENTE COOPERADOR se reserva la posibilidad de rescisión del contrato.
3. OTRAS: detallar.

ARTÍCULO 21°. - DATOS DE INTERÉS PARA LA DECLARACION JURADA DE INTERESES
Consejo Directivo del Colegio de Escribanos de la CIUDAD de BUENOS AIRES
Presidente: Jorge Andrés De Bártolo
Secretario: Magdalena Tato
Tesorero: Ramiro Gutiérrez De Lío
Miembros del Consejo de Administración del ENTE COOPERADOR
Mariana Claudia Massone
Paula Maria Rodriguez Foster
Carlos Eduardo Medina
Miembros de la Comisión Fiscalizadora del Fondo de Cooperación Técnica y Financiera Ley Nº 26.102.
Titulares:
Martín Siracussa, D.N.I. N° 31.475.615: Por el MINISTERIO DE SEGURIDAD DE LA NACIÓN
Luis Marcelo KALEK, D.N.I. N° 18.366.843: Por la POLICÍA DE SEGURIDAD AEROPORTUARIA
Karen Noelia NARDONE, D.N.I. N° 26.427.849: Por la POLICÍA DE SEGURIDAD AEROPORTUARIA.
Suplentes:
Gustavo Luis GAVASSA, D.N.I. N° 16.161.674: Por el MINISTERIO DE SEGURIDAD DE LA NACIÓN.
Gabriela Verónica HADDADD, D.N.I. Nº 25.024.034: Por la POLICÍA DE SEGURIDAD AEROPORTUARIA.
Sandra Daniela CABRERA, D.N.I. Nº 21.003.808: Por la POLICÍA DE SEGURIDAD AEROPORTUARIA.
Director Nacional de la POLICIA DE SEGURIDAD AEROPORTUARIA
Alfredo Hernan GALLARDO.

Cotizar precios con IVA INCLUIDO, exclusivamente en este formulario, y enviar su propuesta vía correo electrónico a la casilla de compras@colegio-escribanos.org.ar, hasta las 15:00 hs. del día 03 de Julio de 2024.

Muy Importante: no serán consideradas las ofertas que no sean remitidas en este formulario. Cualquier aclaración y/o alternativa podrán realizarla en hoja aparte.
"Facturar en formularios B o C a FONDO DE COOPERACIÓN TÉCNICA Y FINANCIERA – CECBA – PSA – LEY 26102 – DTO.742-21 O.P, aclarando la condición ante el IVA: EXENTO, y el Nº de CUIT: 30-71749460-8, y el domicilio: Avda. Callao 1542, Capital Federal. Lo mismo rige para los remitos y recibos que se emitan."; "La mercadería/servicio deberá ser entregada/prestado mediante remitos y facturas en original y duplicado", "El pago se realizará dentro de los 15 días contados a partir de la recepción en el Departamento de Finanzas y Control de la factura y el remito con la conformidad definitiva de la entrega de los materiales y/o servicios contratados, mediante transferencia

bancaria; "El Colegio de Escribanos de la Ciudad de Buenos Aires como administrador del FONDO DE COOPERACIÓN TÉCNICA Y FINANCIERA – CECBA – PSA – LEY 26102 – dto.742-21 o.p, se reserva el derecho de declarar desierto este (COMPULSA DE OFERTAS), aún cuando se hubieren presentado una o mas ofertas, así como de adjudicar en forma total o parcial a la Empresa cuya propuesta considere la más conveniente, a su solo arbitrio, pudiendo ser o no la de menor precio."; A los efectos de la responsabilidad compartida de los artículos 30 y 136 de la Ley 20.744 y sus modificatorias, el adjudicatario se compromete a observar y cumplir fielmente con todas las normas al trabajo y los organismos de Seguridad Social. Asimismo, se obliga a cumplir con las prescripciones de la Ley 19.587 y la Ley 24.557. El Colegio de Escribanos podrá rescindir la presente adjudicación en el caso de incumplimiento del obligado, sin perjuicio de ejercer el derecho de retención sobre las sumas adeudadas a los contratistas."

Forma de Pago: en PESOS ARGENTINO de curso legal, mediante transferencia bancaria.

Sin otro particular saludo a Ud. muy atentamente.