Dirección Nacional de Contrataciones Públicas
E.E.U.U. 961 c/ Tte. Fariña - Asunción, Paraguay
Tel. y Fax +595 21 4154000 - dncp@contrataciones.gov.py

# Consultas Realizadas

# Licitación 474137 - Servicio de Antiphishing y Autenticación de Mensajes, Informes y Conformidad Basada en el Dominio del Banco - Ad Referéndum Ejercicio Fiscal 2026

## Consulta 1 - Actividad Economica

| Consulta | Fecha de Consulta | 05-01-2026 |
|---|---|---|

Buenas, se remite a la convocante la siguiente consulta sobre este fragmento del PBC:
Se deberá acreditar que el giro comercial de la empresa corresponde al procedimiento de contratación ofertado, para lo cual deberá presentar copia simple y legible del documento que acredite la actividad comercial, industrial o de servicio, pudiendo ser: la constancia de RUC, patente municipal o documentos constitutivos, siempre que de la documentación se desprenda su actividad comercial y la correspondencia al procedimiento objetado. Cuando no resulte aplicable la constancia de RUC o la patente municipal, el oferente deberá manifestar y justificar esta condición en su oferta y presentar otra documentación a los efectos de acreditar el giro comercial.

Consulta:
A que se refiere con giro comercial? Cual serían las actividades aceptadas? Se aceptan actividades de consultoría y gestiónd de servicios informáticos?

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

El Fragmento mencionado corresponde al estándar aprobado por la DNCP, favor considerar lo dispuesto en su texto " Se deberá acreditar que el giro comercial de la empresa corresponde al procedimiento de contratación ofertado..." "...deberá presentar copia simple y legible del documento que acredite la actividad comercial, industrial o de servicio, pudiendo ser: la constancia de RUC, patente municipal o documentos constitutivos, siempre que de la documentación se desprenda su actividad comercial y la correspondencia al procedimiento objetado."

## Consulta 2 - Herramientas para navegadores web - EETT

| Consulta | Fecha de Consulta | 05-01-2026 |
|---|---|---|

Herramientas para navegadores web que minimicen el impacto de ataques de phishing para clientes del Banco

¿Qué tipo de herramienta se espera específicamente? (ej. ¿Una extensión/plugin de navegador desarrollada a medida, una funcionalidad de seguridad nativa de la plataforma ofrecida, o alguna otra solución complementaria?)

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: Se espera una solución tecnológica que independientemente de su arquitectura cuente con la capacidad de proteger al cliente de manera preventiva. El criterio esencial de aceptación es que la protección se ejecute de forma automática, bloqueando o neutralizando el acceso a sitios maliciosos antes de que se materialice el riesgo y que este proceso ocurra de manera transparente, sin necesidad de ninguna acción, configuración o intervención manual por parte del cliente final para ser efectiva.

## Consulta 3 - Herramienta para navegador web

| Consulta | Fecha de Consulta | 05-01-2026 |
|---|---|---|

¿Es responsabilidad del banco la instalación y despliegue masivo de esta herramienta en los navegadores de los clientes finales, o es una herramienta de uso opcional y autogestionado por el cliente?

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: La responsabilidad del Banco se limita únicamente a poner a disposición el acceso, instalador oficial o funcionalidad a través de sus canales digitales públicos.

## Consulta 4 - Punto 16

| Consulta | Fecha de Consulta | 12-01-2026 |
|---|---|---|

En el apartado SUMINISTROS REQUERIDOS ESPECIFICACIONES TÉCNICAS ITEM 16 el requerimiento cita: "La solución debe de identificar y desactivar el uso no autorizado de material con contenido protegido por leyes de propiedad intelectual y/o leyes de protección de marca o de uso indebido no autorizado de marcas que sean objeto del servicio de detección de fraude"
Consulta: Favor de compartir un ejemplo del caso de uso específico de este requerimiento para dimensionar correctamente el servicio.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: Un caso de uso específico para este requerimiento sería la detección de uso no autorizado de logotipos o imagen corporativa en sitios web de terceros que, sin ser necesariamente phishing transaccional, buscan engañar al usuario ofreciendo falsos préstamos, promociones o sorteos en nombre del Banco. La solución debe ser capaz de identificar fraudes mediante el reconocimiento de imágenes o texto y gestionar su baja.

## Consulta 5 - Punto 21

| Consulta | Fecha de Consulta | 12-01-2026 |
|---|---|---|

En el apartado SUMINISTROS REQUERIDOS ESPECIFICACIONES TÉCNICAS ITEM 21 el requerimiento cita: " El servicio ofrecido debe contar con un portal o consola de administración, en la que se tenga la capacidad de monitoreo en tiempo real de la actividad anómala de phishing, reporte de nuevos casos, seguimiento de incidentes, estadísticas de gestión, reportes de incidentes en tiempo real e historial de casos, entre otros.

Consulta: Favor de compartir un ejemplo de la actividad anómala mencionada en este requerimiento para dimensionar correctamente el servicio.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: Una actividad anómala es la detección de una campaña masiva de registro de dominios en un corto periodo de tiempo. El portal debe permitir visualizar estos picos de actividad, identificar si pertenecen a un mismo actor y mostrar la evolución de la campaña.

## Consulta 6 - Punto 22

| Consulta | Fecha de Consulta | 12-01-2026 |
|---|---|---|

En el apartado SUMINISTROS REQUERIDOS ESPECIFICACIONES TÉCNICAS ITEM 22 el requerimiento cita: " El servicio debe incluir los respectivos análisis de los datos de los incidentes. Debe incluir los detalles de los incidentes, tales como: posibles causas, fuentes de los ataques, tomando en cuenta la evidencia que esté disponible.

Consulta: Favor de compartir un ejemplo del tipo de incidentes a detectar para dimensionar correctamente el servicio.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: La solución debe cubrir, sin limitarse a los citados, escenarios de Phishing Web Tradicional,
Suplantación en Redes Sociales, Aplicaciones Móviles Fraudulentas, etc.

## Consulta 7 - PBC

| Consulta | Fecha de Consulta | 12-01-2026 |
|---|---|---|

Alcance de las Acciones de Detención de Fraude
Referencia del Pliego:
* Punto 4.4: El servicio ofertado deberá permitir además ejecutar acciones que tiendan a eliminar o detener el fraude.
* Punto 19.19: La solución debe ser capaz de detectar y gestionar la desactivación de sitios.
Consulta:
En relación con la capacidad de "detener el fraude", se consulta si se considera un cumplimiento válido la implementación de mecanismos de bloqueo inmediato en el punto final (endpoint) del usuario, complementarios a la gestión de baja del sitio.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: Sí, se considera un cumplimiento válido. Se aceptará la funcionalidad de Bloqueo Preventivo como medida de mitigación inmediata.

## Consulta 8 - PBC

| Consulta | Fecha de Consulta | 12-01-2026 |
|---|---|---|

Herramientas de Protección para el Usuario Final
Referencia del Pliego:
* Punto 26.26: Herramientas para navegadores web que instaladas en los equipos permitan minimizar el impacto de ataques de phishing.

Consulta:
Se consulta si el requisito de "herramientas para navegadores" puede ser cubierto mediante un agente de seguridad que intercepte y analice el tráfico de red a nivel de dispositivo, protegiendo así la navegación independientemente del navegador utilizado.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: Si, se considerará cubierto el requisito por un agente de seguridad que intercepte y analice el tráfico de red protegiendo así la navegación independientemente del navegador utilizado.

## Consulta 9 - PBC

| Consulta | Fecha de Consulta | 12-01-2026 |
|---|---|---|

Cobertura de Tiendas de Aplicaciones y Análisis Forense
Referencia del Pliego:
* Punto 9.9: Búsqueda de aplicaciones móviles en tiendas oficiales y tiendas paralelas.
* Punto 27.27: Capaz de analizar e informar sobre la morfología del ataque, su origen, las técnicas del mismo.

Consulta:
Sobre el monitoreo de tiendas paralelas, se consulta si la solución debe tener la capacidad técnica de indexar y buscar en repositorios de terceros específicos y en la web abierta, más allá de las tiendas oficiales estándar.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: Sí, es un requisito indispensable. La solución debe contar con capacidades de Monitoreo de Amenazas Móviles que abarquen no solo las tiendas oficiales (Google Play/App Store), sino también la indexación de tiendas de terceros y la web abierta. Esto es crítico para identificar aplicaciones maliciosas que se distribuyen fuera de los canales controlados.

## Consulta 10 - PBC

| Consulta | Fecha de Consulta | 12-01-2026 |
|---|---|---|

Sobre el monitoreo de tiendas paralelas, se consulta si la solución debe tener la capacidad técnica de indexar y buscar en repositorios de terceros específicos y en la web abierta, más allá de las tiendas oficiales estándar.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: Sí, es un requisito indispensable. La solución debe contar con capacidades de Monitoreo de Amenazas Móviles que abarquen no solo las tiendas oficiales (Google Play/App Store), sino también la indexación de tiendas de terceros y la web abierta. Esto es crítico para identificar aplicaciones maliciosas que se distribuyen fuera de los canales controlados.

## Consulta 11 - PBC

| Consulta | Fecha de Consulta | 12-01-2026 |
|---|---|---|

Respecto al análisis de la "morfología del ataque", se consulta si este análisis requiere la inspección del código binario de la aplicación fraudulenta.

5. Procesamiento de Informes DMARC
Referencia del Pliego:
* Punto 10.10: El servicio debe ser capaz de procesar informes forenses DMARC y agregarlos a listas gestionadas.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: El servicio debe procesar Informes Forenses DMARC. Estos informes presentan evidencia detallada y completa. La solución debe ser capaz de ingerir y analizar esta data granular para identificar campañas de suplantación dirigida y aplicar contramedidas precisas en las listas gestionadas.

## Consulta 12 - PBC

| Consulta | Fecha de Consulta | 12-01-2026 |
|---|---|---|

Se consulta si el procesamiento de informes implica la capacidad de ingesta, agregación y visualización estructurada de la data forense para la gestión de políticas de correo.

6. Gestión de Buzones de Abuso
Referencia del Pliego:
* Punto 11.11: Gestionar de manera automática y/o manual los buzones de abuso.
Consulta:
Se consulta si la gestión automática debe incluir mecanismos de análisis sintáctico y clasificación para filtrar correos irrelevantes o spam masivo.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: 1) El servicio debe incluir la capacidad de ingesta y visualización de reportes para gestionar políticas de autenticación y detectar suplantación de correo. Adicionalmente, la gestión de buzones de abuso debe incluir Clasificación Automatizada para filtrar spam y priorizar amenazas reales. 2) El servicio debe actuar como una plataforma de inteligencia y visibilidad a partir de los datos obtenidos y clasificándolos apropiadamente de manera a que logre validar la legitimidad de los correos. El servicio debe permitir definir políticas de seguridad a través de la información accionable para fortalecer su postura ejecutando este proceso de manera nativa.

## Consulta 13 - PBC

| Consulta | Fecha de Consulta | 12-01-2026 |
|---|---|---|

Automatización y Capacidad de Respuesta
Referencia del Pliego:
* Punto 5.5: Pudiendo el BNF elegir automatizar el derribo o desmontaje de los sitios fraudulentos.
* Punto 20.20: Gestión de medidas y autorización de desmontajes.

Respecto a la automatización del derribo, se consulta si la solución debe poseer la capacidad de ejecutar acciones de baja basadas en reglas de confianza predefinidas, sin requerir intervención manual para cada incidente.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: La solución debe permitir la Orquestación Automatizada de bajas, ejecutando derribos automáticos optimizando así los tiempos de respuesta.

## Consulta 14 - Plazo de entrega

| Consulta | Fecha de Consulta | 12-01-2026 |
|---|---|---|

El servicio deberá estar disponible 24 Hs posteriores a la firma del contrato.

Se solicita cordialmente a la convacante extender por lo menos a 5 días la activación y puesta en marcha del servicio. El plazo de 24 hs sólo aplicaría si el servicio que actualmente cuenta el banco, se vuelve a renovar. Solo beneficia a la empresa que actualmente presta dicho servicio al banco.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: El plazo de entrega establecido obedece a la criticidad y naturaleza continua del servicio de seguridad, el cual no admite interrupciones ni ventanas de tiempo sin cobertura que expongan a la Institución a amenazas activas. Extender el plazo de activación generaría un riesgo operativo inaceptable para el Banco. Por tanto, los plazos se mantienen según lo estipulado en el Pliego de Bases y Condiciones.

## Consulta 15 - PBC

| Consulta | Fecha de Consulta | 26-01-2026 |
|---|---|---|

Monitoreo de Actividad Anómala (Portal)
Referencia del Pliego:
Item 21: Portal con capacidad de monitoreo en tiempo real de actividad anómala.
Consulta:
Favor de compartir un ejemplo de la actividad anómala mencionada en este requerimiento para dimensionar correctamente el servicio.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: Una actividad anómala es la detección de una campaña masiva de registro de dominios en un corto periodo de tiempo. El portal debe permitir visualizar estos picos de actividad, identificar si pertenecen a un mismo actor y mostrar la evolución de la campaña.

## Consulta 16 - PBC

| Consulta | Fecha de Consulta | 26-01-2026 |
|---|---|---|

Protección de Propiedad Intelectual y Marca
Referencia del Pliego:
Item 16: Identificar y desactivar el uso no autorizado de material con contenido protegido.
Consulta:
Favor de compartir un ejemplo del caso de uso específico de este requerimiento.

| Respuesta | Fecha de Respuesta | 04-02-2026 |
|---|---|---|

Se transcribe respuesta de la dependencia requirente: Un caso de uso específico es la identificación y desactivación de activos digitales que infringen la propiedad intelectual, como perfiles en redes sociales o sitios web que utilizan logotipos del Banco sin autorización para fines engañosos.