UNIDAD OPERATIVA DE CONTRATACIÓN

ADENDA N° 1 – MCI N° 9PM/2025

Asunción, 14 de julio de 2025

Señores
PRESENTE

De nuestra consideración:
Con relación a la **LICITACIÓN DE MENOR CUANTÍA INTERNACIONAL (MCI) N° 9PM/2025 – SERVICIO DE CONEXIÓN DE CONTINGENCIA A LA RED SWIFT - ID N° 463927,** cumplimos en informar las siguientes modificaciones de la convocatoria:

Punto 1
El apartado Especificaciones Técnicas obrante en la Sección Suministros Requeridos – Especificaciones Técnicas, queda redactado como sigue:

Especificaciones Técnicas

MODALIDAD DE CONTRATACIÓN
Contrato Cerrado.

CONSIDERACIONES GENERALES
A continuación, se indican los requerimientos y condiciones generales y particulares que deben ser cumplidos por la firma adjudicada, en adelante Proveedor, para la prestación de los servicios solicitados y detallados en la presente Sección.
El Banco Central del Paraguay, en adelante BCP, designa a la Gerencia de Tecnología de la Información y Comunicaciones, en adelante GTIC, para la administración y control de estos servicios. La GTIC nombrará un supervisor, en adelante el Supervisor, quien se encargará de la administración y supervisión de los servicios descriptos.

DESCRIPCION DEL SERVICIO
El presente llamado tiene por objeto la contratación del servicio de conexión de contingencia a la red SWIFT para las áreas funcionales de la Gerencia de Mercados y la Gerencia de Operaciones y Pagos, respectivamente, conforme a las especificaciones técnicas que se detallan a continuación.
El servicio a ser proveído al BCP deberá comprender los siguientes puntos principales:

- Conexión física con la red SWIFT, para todos los ambientes disponibles con que cuente el BCP (Producción, contingencia, etc.).
- Conectividad a los servicios “FIN”, “FINPLUS (MX-ISO20022)”, “FileAct” e “InterAct” disponibles en la red SWIFT, para todos los ambientes disponibles con que cuente el BCP (Producción, contingencia, etc.).
- Servicio de Soporte y Asistencia Técnica a la infraestructura SWIFT del BCP, para todos los ambientes disponibles (Producción, contingencia, etc.).

El Proveedor deberá:

- Garantizar la disponibilidad del servicio en modalidad 24*7*365 mediante una infraestructura tecnológica de alta disponibilidad.
- Contar con número(s) telefónicos para llamadas de soporte en horario de 8.00 am a 6.00 pm hora local de cliente (lunes a viernes).
- Soporte Técnico para reporte de fallas: Se deberá proveer direcciones de correo electrónico, números de telefonía fija y móvil, así como nombre(s)/apellido(s) y cargos de los responsables del área técnica de la empresa.
- Soporte Administrativo y Comercial: Para el efecto, se deberá especificar los datos de contacto (correo y teléfono) de los representantes de las áreas administrativa y comercial de la empresa.

REQUERIMIENTOS GENERALES
El Oferente deberá presentar en su oferta una Nota de compromiso en virtud de la cual manifieste contar con los medios, equipos y recursos exigidos que se detallan a continuación:

Infraestructura del Data Center del Proveedor del Servicio
Los servidores principales y de backup del Proveedor del servicio, deberán ofrecer una infraestructura, abarcando espacio físico climatizado, con electricidad y disponibilidad de cableado estructurado.

Seguridad Física

- Acceso controlado y restringido al Data Center y sus zonas adyacentes.
- Edificio y puertas de acceso monitoreados a través de circuito cerrado de TV.
- Posibilidad de seleccionar el acceso a determinadas áreas por status.
- Seguridad física del Data Center contra accesos no autorizados y contra la influencia del ambiente externo.
- Vigilancia permanente los 365 días del año.

Electricidad

- Generadores de alimentación, en caso de emergencia.
- Sistema redundante de energía ininterrumpible (UPS's).
- No hay indisponibilidad (disponibles al 100%), gracias al mantenimiento regular de las UPS, de los generadores, de los transformadores y del sistema de aire acondicionado.
- Disponibilidad de 2 circuitos eléctricos independientes (fases) para cada bastidor.
- Protectores contra sobre-tensión.
- Piso sobre elevado antiestático con canalizaciones bajo-piso.
- Cableado eléctrico correctamente dimensionado y estructurado.
- Mantenimiento regular de la infraestructura instalada.
- Recursos de mantenimiento on-site para a infraestructura del Data Center.

Ambiente del Data Center

- Sistema de aire acondicionado y aire redundante con unidad de reserva.
- Sistema de alarma contra fuego.
- Detectores de humo y fuego en todas las áreas del Data Center, en el piso falso y el revestimiento.
- Extintores de incendio manuales dentro del Data Center.

Arquitectura del Data Center

- Servidores para SAA. (SWIFT Alliance Access).
- Servidores para SAG (SWIFT Alliance Gateway) / SNL (SWIFTNet Link).
- Conectividad "GOLD" a la red SWIFT o similar.
- Switches Ethernet.
- Ruteadores.
- Firewalls.

Sitio de Contingencia

El Data Center del Proveedor del servicio deberá contar con un sitio alterno de procesamiento o de contingencia el cual deberá estar conectado al Data Center del Proveedor por un enlace dedicado, de forma que, cuando hubiera necesidad, el tráfico de mensajes será desviado para el sitio de contingencia, de forma a minimizar la indisponibilidad de los servicios. Este sitio alterno o de contingencia deberá contar una conectividad "SILVER" o "BRONZE" a la red SWIFT o similar.

Seguridad Lógica

Todos los componentes de la conexión del BCP con los aplicativos del Data Center del Proveedor del servicio deberán ser protegidos a través de listas de acceso en los ruteadores, políticas de firewall, NAT (Network Address Translation) y criptografía, posibilitando asimismo la seguridad lógica exigida por SWIFT para que todo el tráfico de datos entre el BCP y SWIFT sean preservados íntegros y confiables.

Disponibilidad

El Proveedor del servicio deberá asegurar la disponibilidad de la conectividad con la red de SWIFT las 24 horas del día, los 7 días de la semana, los 365 días del año.

El Proveedor del servicio deberá garantizar la redundancia de su hardware para asegurar la disponibilidad de los servicios de conexión con la red de SWIFT.

El Proveedor del servicio deberá comunicar al BCP sobre cualquier situación que comprometa el envío o recepción de mensajes, tanto a nivel del Proveedor del servicio como a nivel de la red de SWIFT, en un periodo máximo de 1 (una) hora.

Servicio de Soporte y Asistencia Técnica a la infraestructura SWIFT del BCP

El Proveedor del servicio deberá brindar soporte de primer nivel al BCP, para las aplicaciones de SWIFT instaladas en el BCP (Ej.: Alliance Access, Alliance Web Platform, Alliance Remote Gateway), permitiendo que éste procese las transacciones de SWIFT en línea con las responsabilidades que SWIFT impone a sus usuarios. Para la configuración o setup inicial del servicio, este soporte incluye el apoyo al "Administrador de la infraestructura SWIFT del BCP" sobre la creación de Certificados necesarios para conectividad al Gateway del proveedor, acceso al O2M (Online Operarations Manager) y definición de controles de expiración de certificados.

El Proveedor del servicio deberá poner a disposición del BCP los servicios de un especialista para responder a las solicitudes del BCP, **en un periodo máximo de una hora**, durante el horario de atención comercial. Fuera del horario de atención comercial habrá especialistas en guardia pasiva para atender las solicitudes del BCP. Para el efecto, deberá proporcionar la identidad, correo electrónico y número telefónico del contacto en el centro de soporte.

El servicio de soporte se presta de manera remota, coordinando con la prestadora la fecha del mismo con un mínimo de una semana de anterioridad.

El horario del soporte estándar será de 8.00 am a 6.00 pm hora local del cliente (lunes a viernes).

Acompañamiento fines de semana y nocturno previa solicitud durante el horario hábil, al menos 48 horas antes de su ejecución.

Soporte en la administración del sistema

- Actualización de parches SWIFT e instalación de nuevas versiones (Manos Remotas).
- Actualización de tabla de sintaxis SWIFT (Manos remotas).

- Actualización de archivo de corresponsales (BIC directory).
- Definición de esquemas, reglas de ruteo, Exit Points y Message Partners.
- Apoyo en la configuración de firmas LAU o SHA.
- Automatización de Procesos SWIFT - Start DB - Stop DB - LTs - Etc.
- Configuración, conexión y desconexión de terminales lógicos.
- Recomendaciones en ejecución de Backups en frío y Backups en caliente.
- Recomendaciones en replicación histórica a ambiente de respaldo y contingencia.

Soporte en la administración de seguridad del sistema

- Definición de perfiles de acceso y usuarios.
- Recomendaciones de debida política de manejo de claves.
- Recomendaciones de manejo de claves de los oficiales de seguridad.

Soporte en la administración de Claves Bilaterales (RMAs)

- Apoyo en el intercambio de claves: Accept-Reject-Revoke-Delete.
- Apoyo a procesos de exportación e importación de claves.
- Recomendaciones de Backup y Respaldo de claves.

Soporte en la activación del Event Journal

- Apoyo para la configuración automática de alertas a la mesa de ayuda.
- Recomendación y apoyo en la configuración de listas de distribución de alertas.
- Recomendaciones para configuración de alertas.
- Recomendaciones para el tratamiento de alertas.

Acompañamiento en las pruebas del Plan de Contingencia

- Acompañamiento en activación de Servidores SWIFT en sitio alterno del cliente.
- Identificación de fallas y diagnóstico de las VPN Boxes.
- Identificación de fallas por caída de internet o canales.
- Acompañamiento en redireccionamiento terminales lógicas.
- Acompañamiento en migración de información histórica a sitio de contingencia.
- Acompañamiento en activación de contingencia.
- Acompañamiento en el retorno a producción.

Acompañamiento en activación y desactivación de servidor de respaldo y/o de servidor de contingencia.

- Apoyo en configuración de servidores y traslado de BD e información histórica.
- Orientación en el uso de servicios de la red e impacto en costos adicionales:
    - Bulk Payments, FileAct Real Time o Store & Forward, Interact.
    - SCORE, MACUG para servicios a corporativos.
    - Y-Copy, Fileact Header Copy.
- Orientación en temas de facturación por tráfico de mensajería.

Sistema WEB para la administración de casos de soporte

- Atención con SLA de los casos según su clasificación: críticos, urgentes y normales.
- Tiempo de atención es inferior a 15 minutos.
- Tiempo de respuesta:
    - Dos (2) horas para casos críticos.
    - Hasta ocho (8) horas para casos urgentes.
    - Hasta tres (3) días casos normales o de mantenimiento.

Servicios adicionales:

- Acompañamiento para realizar las pruebas y migración a nuevas versiones SWIFT.
- Apoyo en los procesos a ejecutar en www.swift.com
- Soporte en la administración de certificados PKI y su renovación.
- Acompañamiento en pruebas Backup / Restore o DataBase Recovery.
- Recomendaciones para el manejo de información histórica de mensajes y eventos.
- Recomendaciones en estrategia de procesos de Backups y Restore.
- Reportes estadísticos sobre el servicio, medición de tiempos de asistencia, tiempos de respuesta, etc., bajo demanda.

ACUERDO DE NIVEL DE SERVICIO:

El Proveedor deberá cumplir con los términos del Acuerdo de Nivel de Servicio (ANS o SLA por sus siglas en inglés), a fin de garantizar la disponibilidad de técnicos en los siguientes tiempos de respuesta: 7 días de la semana, 24 horas al día, 365 días al año (Atención remota), con los siguientes términos:

En caso de un incidente, el tiempo que transcurra desde que el Proveedor es informado hasta el tiempo de respuesta no podrá superar los 60 (sesenta) minutos.

El Proveedor deberá:

- Contar con personal, medios y recursos necesarios para el diagnóstico y soporte técnico especializado.
- Cumplir con todas las condiciones exigidas en las presentes especificaciones técnicas.

- Disponer de un sistema de tickets para realizar el seguimiento de los incidentes. El sistema debe poder ser accedido vía web por parte del Supervisor.
- Disponer de una cuenta de correo electrónico para la recepción de los incidentes según se definen en este anexo.
- Contar con una herramienta en línea que permita la gestión de incidentes.
- Indicar, adicionalmente, vía nota, los medios y recursos con que cuenta para atender este servicio (tanto para la notificación como para el seguimiento y control del estado de cada incidente).
- Emitir un comprobante de servicio por cada incidente, con los siguientes datos del servicio técnico realizado:
    - Hacer referencia al incidente/ítem afectado.
    - Nivel de criticidad definido por el Supervisor
    - Tiempo total de resolución desde la apertura hasta la resolución completa.
    - Causa de la avería.
    - Acciones llevadas a cabo para su resolución.
    - Otras observaciones que el Proveedor desee hacer constar.
    - Fecha de finalización de la tarea y del periodo del informe.
    - Observaciones y recomendaciones.

RECURSOS PROVEIDOS POR EL BCP

- Conceder una identificación para movilidad interna al personal técnico del Proveedor y facilitar su acceso a instalaciones del BCP, cuando los trabajos de mantenimiento así lo requieran.
- Facilitar toda la información referente a la red e infraestructura que sean necesarios para la correcta prestación del servicio.

RECURSOS BRINDADOS POR EL PROVEEDOR

- Identificación del personal técnico habilitado por el Proveedor, cuando los trabajos de mantenimiento así lo requieran.

ADMINISTRACIÓN DEL CONTRATO

La administración del contrato estará a cargo de la Gerencia de Tecnología de la Información y Comunicaciones (GTIC) en coordinación con el Departamento de Ciberseguridad.

COMPROMISO DE CONFIDENCIALIDAD

El personal interviniente del Proveedor deberá firmar un Compromiso de Confidencialidad de la Información, dado que el personal contratado podría acceder a información confidencial del BCP.

CONFORMIDAD DE LOS SERVICIOS

Se emitirá un documento de aprobación del área técnica de la GTIC por los servicios realizados, conjuntamente con el área técnica del Departamento de Ciberseguridad y las áreas funcionales operativas del negocio, como ser la Gerencia de Mercados y la Gerencia de Operaciones y Pagos, respectivamente.

Punto 2

Se modifican las fechas en el SICP.

Atentamente.

MARIA EMILIA ACHA PALACIOS
Firmado digitalmente por MARIA EMILIA ACHA PALACIOS
Fecha: 2025.07.14 14:27:19 -03'00'

Directora
Unidad Operativa de Contratación

LUIS FERNANDO VERA ORTIZ
Firmado digitalmente por LUIS FERNANDO VERA ORTIZ
Fecha: 2025.07.14 13:04:47 -03'00'