UNIDAD OPERATIVA DE CONTRATACIÓN
ADENDA N° 2 – LPN N° 35/2017

Asunción, 03 de octubre de 2017.

Señores
PRESENTE

De nuestra consideración:

En atención a lo establecido en el punto IAO 8.2 de la Sección I. Datos de la Licitación (DDL) del Pliego de Bases y Condiciones, para la **LICITACIÓN PÚBLICA NACIONAL N° 35/2017 PARA LA ADQUISICIÓN DE LICENCIAS Y SOFTWARES PARA EL BANCO CENTRAL DEL PARAGUAY - ID N° 326032**, aprobada por Resolución N° 2, Acta N° 62, de fecha 12 de setiembre del 2017 del Directorio de la Institución, cumplimos en informar las modificaciones al PBC para el presente llamado:

Punto 1

En la Sección III. Suministros Requeridos, Anexo Técnico, punto 2- ESPECIFICACIONES TÉCNICAS, el LOTE N° 3 - FIREWALL PARA APLICATIVOS WEB (GTIC), queda redactada de la siguiente manera:

LOTE N° 3 - FIREWALL PARA APLICATIVOS WEB (GTIC)			
Ítem	**Descripción técnica**	**Mínimo Exigido**	**Ofrecido**
1. Marca	Se deberá especificar la marca ofertada	Especificar	
2. Protección contra	DOS y DDOS (ataque de denegación de servicios y de denegación de servicios distribuido)	Exigido	
	Inyección SQL y Blind SQL Injection	Exigido	
	Inyección de scripts (tanto del intérprete como PHP, así como scripts del Sistema Operativo)	Exigido	
	Inclusión de archivos remotos en el servidor (File Injection)	Exigido	
	Ejecución remota de comandos (Command Injection)	Exigido	
	Listado de carpetas y/o archivos del servidor	Exigido	
	Cookie Poisoning (envenenamiento de cookies)	Exigido	
	Secuestro de sesiones	Exigido	
	Cross-Site scripting (XSS)	Exigido	
	Cross-Site Request Forgery (CSRF)	Exigido	
	Server Side Request Forgery (SSRF)	Exigido	
	CRLF Injection	Exigido	
	Cache-Poisoning	Exigido	
	Cache-based defacement	Exigido	
	Page Injection	Exigido	
	SYN Flood (Inundación de SYN)	Exigido	
	LDAP Injection y Blind LDAP Injection	Exigido	
	SSI Injection (Server-Side Includes)	Exigido	
	NULL Byte Injection	Exigido	
	Peticiones en hexadecimal	Exigido	
	Ataque de fuerza bruta a formularios	Exigido	
	PHP Object Injection	Exigido	
	Shellshock	Exigido	
	Peticiones HTTP falsificadas	Exigido	
	Injección de Payload mediante la verificación de codificación URL	Exigido	
	JavaScript Botnet	Exigido	
	La utilización del servidor web como proxy	Exigido	
	Aprovechamiento de "comentarios inline" para ofuscación de ataques	Exigido	
3. Funciones Básicas	Protección de ejecución dinámica de consultas (peticiones que al transformar -char() y/o concatenar se crea una sentencia)	Exigido	
	El WAF tendrá que eliminar directamente una petición que coincida con sus reglas, esto es para evitar el ataque mediante anidación de expresiones	Exigido	
	Enmascaramiento del servidor web y el Sistema Operativo	Exigido	
	Enmascaramiento de la firma del servidor web (Ej.: que la respuesta HTTP no diga Apache o IIS)	Exigido	
	Detección y bloqueo de violaciones y anomalías en los protocolos	Exigido	
	Bloqueo de acceso por dirección IP al servidor web (para evitar la utilización de algunas herramientas de ataque)	Exigido	
	Monitoreo tanto en los HEADERS, METHOD, URI como en los BODY de recepción y envío (REQUEST y RESPONSE) (también debe controlar el tamaño de las peticiones)	Exigido	
	Enmascaramiento de mensajes de errores del servidor (también	Exigido	

Zinzia Abadie Pastore
Jefa
Div. Procesos Administrativos

GUSTAVO BENÍTEZ
Pool de Técnicos de Infraestructura Tecnológica

Lic. Carlos E. Pérez López
Gerente
Gerencia de Tecnología de la Información y Comunicación

Silvia Ramírez
Gerente "GPI"

VICTOR D. SCHAERER

UNIDAD OPERATIVA DE CONTRATACIÓN
ADENDA N° 2 – LPN N° 35/2017

	mensajes de fallo del servidor)		
	Identificación de robots maliciosos; Spam Bots	Exigido	
	Seguimiento de incidentes mediante IPs o ID de sesiones para mejorar los bloqueos	Exigido	
	Correlación de incidentes (si sobrepasa cierta cantidad de reglas asignadas se realiza un bloqueo)	Exigido	
	Bloqueo de determinados agentes (User-Agent) de conexión en la petición HTTP (o si no posee ninguna)	Exigido	
	Bloqueo de conexiones provenientes de la red TOR (la lista de IPs se debe actualizar automáticamente de forma periódica)	Exigido	
	Detección y bloqueo de escaneres de vulnerabilidades	Exigido	
	Geolocalización de las direcciones IP sospechosas	Exigido	
	Debe permitir la utilización de Listas Blancas a nivel de IP (tanto IP públicas como privadas)	Exigido	
	Mantenimiento de las reglas según las nuevas vulnerabilidades y/o exploits registrados	Exigido	
	Debe permitir realizar reglas personalizadas	Exigido	
	Análisis de comportamiento de las direcciones IP y sus peticiones	Exigido	
	HTTP/HTTPS Throughput: >= 20Mbps	Exigido	
	Cantidad de transacciones HTTP/HTTPS por segundo: >= 1000 en al menos 20Mbps	Exigido	
4. Reportes	Integración con soluciones SIEM implementadas actualmente.	Exigido	
5. Implementación y capacitación.	Se debe incluir la implementación, configuración y monitoreo del software; así como la capacitación al personal designado por el área técnica administradora del Contrato del BCP, para realizar reglas personalizadas.	Exigido	
6. Actualizaciones	Incluye suscripción de actualizaciones de software por 36 meses	Exigido	
7. Garantía del Fabricante	Incluye Garantía del Fabricante por 36 (treinta y seis) meses	Exigido	
8. Soporte	Incluye Soporte por 36 (treinta y seis) meses	Exigido	
9. Licenciamiento	Incluye Licenciamiento por 36 (treinta y seis) meses	Exigido	
10. Garantía de Buen Funcionamiento y Calidad	Se requiere Garantía de Buen Funcionamiento y Calidad por 36 meses	Exigido	
11. Cantidad	2 (dos) unidades	Exigido	

Zinzia Abadie Pastore
Jefa
Div. Procesos Administrativos

GUSTAVO BENÍTEZ
Pool de Técnicos de Infraestructura Tecnológica

Lic. Carlos E. Pérez López
Gerente
Gerencia de Tecnología de la Información y Comunicación

Punto 2

Se informa que se han modificado en el SICP las fechas del límite de consultas, de entrega de ofertas y de apertura de ofertas.

Atentamente,

VICTOR SHAERER RUOTTI
Encargado de Despacho
Unidad Operativa de Contratación

SILVIA PATRICIA NÚÑEZ
Gerente
Gerencia de Patrimonio y Logística

CARLOS BENÍTEZ VIEIRA
Gerente General
Banco Central del Paraguay