

PLIEGO DE BASES Y CONDICIONES

Convocante:

Banco Central del Paraguay (BCP)

Uoc Banco Central del Paraguay

Nombre de la Licitación:

**LPN N° 13/2023 - CONTRATACIÓN DE SERVICIOS
DE GESTIÓN DE CIBERSEGURIDAD**

(versión 2)

ID de Licitación:

426350



Modalidad:

Licitación Pública Nacional

Publicado el:

24/04/2023

"Pliego para la Adquisición de Bienes y/o Servicios - Convencional"
Versión 1

RESUMEN DEL LLAMADO

Datos de la Convocatoria

ID de Licitación:	426350	Nombre de la Licitación:	LPN N° 13/2023 - CONTRATACIÓN DE SERVICIOS DE GESTIÓN DE CIBERSEGURIDAD
Convocante:	Banco Central del Paraguay (BCP)	Categoría:	7 - Servicios Técnicos
Unidad de Contratación:	Uoc Banco Central del Paraguay	Tipo de Procedimiento:	LPN - Licitación Pública Nacional

Etapas y Plazos

Lugar para Realizar Consultas:	SICP de la DNCP	Fecha Límite de Consultas:	26/04/2023 09:30
Lugar de Entrega de Ofertas:	Módulo de Ofertas Electrónicas	Fecha de Entrega de Ofertas:	04/05/2023 10:00
Lugar de Apertura de Ofertas:	Módulo de Ofertas Electrónicas	Fecha de Apertura de Ofertas:	04/05/2023 10:00

Adjudicación y Contrato

Sistema de Adjudicación:	Por Lote	Anticipo:	No se otorgará anticipo
Vigencia del Contrato:	Hasta Cumplimiento Total de Obligaciones		

Datos del Contacto

Nombre:	María Emilia Acha Palacios	Cargo:	Directora UOC - BCP
Teléfono:	6192022	Correo Electrónico:	uoc@bcp.gov.py

ADENDA

Adenda

Las modificaciones al presente procedimiento de contratación son los indicados a continuación:

Punto 1

El apartado ESPECIFICACIONES TÉCNICAS incluido en el punto ESPECIFICACIONES TÉCNICAS en Detalles de los productos y/ servicios con las respectivas especificaciones técnicas - CPS de la Sección SUMINISTROS REQUERIDOS ESPECIFICACIONES TÉCNICAS queda redactado como sigue:

ESPECIFICACIONES TÉCNICAS

ESPECIFICACIONES TÉCNICAS			
Requisito	Detalle y definiciones	REQUERIDO	OFRECIDO
LOTE N° 1 SERVICIOS SOC Y MESA DE AYUDA DE CIBERSEGURIDAD			
ITEM N° 1 - Servicio Security Operations Center (SOC)			
1.1.1 Generalidades del Servicio			
1.1.1.1	Se solicita el servicio SOC (Security Operations Center) tercerizado implementado actualmente en el BCP (Digiware), por un plazo de 24 meses computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato, con las mismas condiciones en las que se tiene contratado el servicio.	EXIGIDO	
ITEM N° 2 - Servicio de Mesa de Ayuda y Gestión de Incidentes de Ciberseguridad			
1.2.1 Generalidades del servicio			
1.2.1.1	Se solicita el servicio de suscripción a la herramienta Invgate Service Desk implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha a ser establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.	EXIGIDO	

1.2.1.2	Se deben incluir todas las licencias necesarias para al menos 20 agentes, sin limitaciones de usuarios clientes y capacidad de almacenamiento de por lo menos 100 GB.	EXIGIDO
1.2.1.3	El servicio debe incluir la provisión de un equipo de trabajo dedicado, compuesto como mínimo por 5 (cinco) técnicos, quienes realizarán las siguientes tareas: la gestión de incidentes de ciberseguridad, la operativa y administración de las herramientas de ciberseguridad del BCP y la gestión de la mesa de servicios implementada, con exclusividad absoluta para el BCP, hasta 40 horas semanales por cada técnico ya sea en modalidad onsite o remoto.	EXIGIDO
1.2.1.4	El servicio técnico contempla: Monitoreo de las alarmas de seguridad, revisión de alarmas y eventos de seguridad; análisis, evaluación y contención de primera línea de incidentes de seguridad; configuración de herramientas de seguridad, tales como firewalls, IPS, DLP, Antivirus, SIEM, Antispam, entre otros; configuración de reglas de correlación; configuración de las plataformas de mesa de servicios de seguridad; revisión técnica, auditoría de registros, test de seguridad e investigación y análisis forense de primer nivel; asistencia a usuarios finales para la resolución de casos; colaboración con el soporte externo de ciberseguridad.	EXIGIDO
1.2.1.5	Lugar de la prestación del servicio: On-Site (Oficinas del BCP) y/o Remoto, a definir con la contraparte del BCP. Horario de la prestación del servicio: On-Site en horario de 06:00 a 22:00, de lunes a viernes; Remoto disponible 24 horas, 7 días a la semana; horario a convenir con la contraparte del BCP.	EXIGIDO
1.2.1.6	Perfil requerido del personal: Entre 23 y 35 años. Estudiante y/o egresado de carreras de Informática. Debe poseer conocimientos sólidos en ciberseguridad, redes y gestión de incidentes, acreditable con por lo menos 40 horas de formación específica en ciberseguridad, a través de cursos o certificaciones sobre: administración y operación de herramientas de seguridad, test de intrusión, seguridad en redes e infraestructura tecnológica, entre otros. Experiencia laboral, al menos 1 (una) referencia certificada, acreditable con la presentación de la fotocopia simple de la referencia comprobable de los trabajos realizados que guarden relación con servicios de informática y/o ciberseguridad. El personal técnico que ejecutará el contrato deberá ser el designado por parte del Proveedor en su oferta.	EXIGIDO

- | | | |
|----------|--|---------|
| 1.2.1.7 | Herramientas de trabajo: El BCP proveerá el equipamiento y el espacio adecuados cuando el servicio sea realizado en sus oficinas. El oferente deberá proveer de todas las herramientas cuando el servicio sea realizado de manera remota, de conformidad con los requerimientos técnicos y de seguridad del BCP. | EXIGIDO |
| 1.2.1.8 | La asistencia del equipo técnico en ningún caso representa compromiso laboral alguno entre los individuos y el BCP, siendo el oferente el único responsable del cumplimiento de todas las obligaciones laborales que correspondan según el caso (pago de salarios, vacaciones, aguinaldo, pagos jubilatorios, horas extras, viáticos, compensaciones, seguros, entre otros). El oferente exime al BCP de toda erogación y responsabilidad asociada a la prestación del servicio. | EXIGIDO |
| 1.2.1.9 | Durante la duración del contrato, el BCP se reserva el derecho de solicitar reemplazos al equipo técnico, y el oferente debe presentar un nuevo integrante en un plazo no mayor a 10 días hábiles, el cual deberá cumplir con los requisitos establecidos en el PBC. | EXIGIDO |
| 1.2.1.10 | Ante la ausencia de uno o más miembros del equipo por 3 (tres) días hábiles o más, cualquiera fuere la razón, el oferente será responsable de proveer un reemplazo temporal, hasta tanto el afectado se reintegre, sin perjuicios de las sanciones contractuales que correspondan. | EXIGIDO |

LOTE N° 2 SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE SEGURIDAD DNS

ITEM N° 1 Servicio de suscripción a Solución de Seguridad DNS

2.1.1 Características de la solución

- | | | |
|---------|---|---------|
| 2.1.1.1 | Se solicita el servicio de suscripción al Software de seguridad DNS, Cisco Umbrella Secure Internet Gateway Essentials implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato. | EXIGIDO |
| 2.1.1.2 | La Solución deberá estar basada en la nube (servicio SWG Cloud) y debe proveer análisis de consultas y resoluciones de DNS para al menos 800 usuarios. | EXIGIDO |

LOTE N° 3 SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE SEGURIDAD PERIMETRAL DEFINIDA POR SOFTWARE

ITEM N° 1 Servicio de Suscripción a Solución de Seguridad Perimetral Definida por Software

3.1.1 Características de la Solución

3.1.1.1 Se solicita el servicio de suscripción a solución de seguridad perimetral definida por software Appgate SDP implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato. EXIGIDO

3.1.1.2 Se deben incluir todas las licencias necesarias para al menos 980 usuarios, y con protección para 2 (dos) sitios o centro de datos. EXIGIDO

LOTE N° 4 SERVICIO DE SUSCRIPCIÓN A SOLUCIONES DE CIBERSEGURIDAD

ITEM N° 1 - Servicio de suscripción a Solución de Análisis de Muestras de malware (Sandboxing)

4.1.1 Características principales de la Solución

4.1.1.1 Se solicita el servicio de suscripción a solución de análisis de muestras de malware (sandboxing) Trellix Virtual Advanced Threat Defense Appliance, implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato. EXIGIDO

ITEM N° 2 - Servicio de suscripción a Solución de Seguridad Antimalware y EDR

4.2.1 Características principales de la Solución

4.2.1.1 Se solicita el servicio de suscripción a la solución de seguridad antimalware y EDR Trellix MVISION Protect Plus EDR para 1200 usuarios, implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato. EXIGIDO

4.2.1.2 La Solución debe contar con un Registro Cloud de análisis de riesgo para al menos 25 mil diferentes servicios Cloud. EXIGIDO

4.2.1.3	Para cada servicio cloud se deben evaluar al menos 50 atributos y 260 sub atributos de riesgo.	EXIGIDO
4.2.1.4	Debe monitorear si los servicios Cloud cuentan con las siguientes certificaciones: EU GDPR, Trustee / BBB, Safe Harbor, ISO 27018, FISMA, FedRAMP, CSA Star, HITRUST, ISO 27017, SAS 70 / SSAE16 / ISAE 3402, ITIL, DCAA / SOC 3, ISO 27001, SOC 2, PCI Compliance y HIPAA	EXIGIDO
4.2.1.5	La Solución debe poder mostrar la exposición de los servicios Cloud a vulnerabilidades como: Cloudbleed, Heartbleed, Poodle, Freak, Ghostwriter.	EXIGIDO
4.2.1.6	La Solución debe identificar intentos de fuga de información por servicios no corporativos a través del análisis de Machine Learning y UEBA, correlacionado con la actividad de los usuarios en los servicios.	EXIGIDO
4.2.1.7	La Solución debe contar con la capacidad de control (Bloquear/Permitir) con base en atributos de Riesgo de Shadow IT.	EXIGIDO
4.2.1.8	La Solución debe tener la capacidad de aplicar políticas de DLP al tráfico Web y de servicios de Shadow IT.	EXIGIDO
4.2.1.9	La Solución debe tener la capacidad de aplicar políticas a la información en la nube basado en: - Diccionarios.	EXIGIDO
4.2.1.10	- Palabras clave	EXIGIDO
4.2.1.11	- Grupos de usuarios	EXIGIDO
4.2.1.12	- Expresiones regulares	EXIGIDO
4.2.1.13	La Solución debe permitir a los administradores: personalizar vistas y reportes, basados en la información que deseen ver.	EXIGIDO
4.2.1.14	La consola debe permitir programar la ejecución de reportes y que estos sean enviados vía correo electrónico en formato PDF, CSV o XLS.	EXIGIDO

- | | | |
|----------|--|---------|
| 4.2.1.15 | La Solución debe presentar un dashboard de madurez de implementación de la misma, donde se muestre el nivel de adopción de la herramienta en la entidad, comparativas anónimas con otros clientes de la misma vertical y recomendaciones de funcionalidades que deben ser implementadas. | EXIGIDO |
|----------|--|---------|

ITEM N° 3 - Servicio de suscripción a Solución de Gestión de Vulnerabilidades

4.3.1 Características principales de la Solución

- | | | |
|---------|---|---------|
| 4.3.1.1 | Se solicita el servicio de suscripción a la solución de gestión de vulnerabilidades. Tenable implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato. | EXIGIDO |
| 4.3.1.2 | Se deben incluir todas las licencias necesarias para al menos 512 (quinientos doce) activos de TI, entre ellos estaciones de trabajo, servidores, dispositivos de red, plataformas de virtualización y otros sistemas conectados. | EXIGIDO |

LOTE N° 5 - SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE DETECCIÓN Y RESPUESTA EXTENDIDA - XDR

ITEM N° 1 - Servicio de suscripción a Solución de Detección y Respuesta Extendida - XDR

5.1.1 Características principales de la Solución

- | | | |
|---------|---|---------|
| 5.1.1.1 | Se solicita el servicio de suscripción a una Solución de Detección y Respuesta Extendida XDR, con el objetivo de facilitar la integración y la respuesta avanzada a incidentes de ciberseguridad, ejecución de playbooks y análisis de amenazas. La Solución debe tener, nativamente y sin ningún tipo de desarrollo adicional, integración con las soluciones de seguridad de endpoint y servidores con las cuales cuenta actualmente el BCP (Trellix MVISION Protect Plus EDR). | EXIGIDO |
| 5.1.1.2 | La Solución debe incluir nativamente capacidades tales como: agregación y correlación de eventos, recolección de eventos de distintas fuentes de datos y definición de políticas de retención de información. Toda la información generada debe poder ser consumida por la propia Solución para la toma de decisiones, de forma nativa, y sin ningún tipo de desarrollo por fuera de la Solución. | EXIGIDO |

5.1.1.3	Se debe entregar todos los módulos de software necesarios para la correcta implementación de lo requerido en este ítem. Se deben incluir todas las licencias necesarias para al menos 750 EPS, con soporte y mantenimiento del fabricante por 24 meses computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.	EXIGIDO
5.1.1.4	La solución debe tener la capacidad de integrar al menos 300 tecnologías diferentes, sin licenciamiento adicional.	EXIGIDO
5.1.1.5	La solución debe tener la capacidad de minimizar el impacto de un incidente.	EXIGIDO
5.1.1.6	La solución debe poder centralizar los datos recibidos con el fin de contar con visibilidad de las amenazas y vulnerabilidades.	EXIGIDO
5.1.1.7	La solución debe soportar expresiones regulares compatibles con Perl.	EXIGIDO
5.1.1.8	La solución debe soportar operaciones booleanas como AND, OR y NOT.	EXIGIDO
5.1.1.9	Debe utilizar un lenguaje de análisis de datos para consultas de eventos para su posterior análisis.	EXIGIDO
5.1.1.10	La solución debe soportar dentro de la anatomía del lenguaje utilizado al menos los siguientes aspectos: búsquedas, filtros, elementos sintaxis como día y hora, operadores de comparación, funciones hash criptográfica, variables de expansión, histograma.	EXIGIDO
5.1.1.11	La solución debe proveer la capacidad de asignar un nombre de clase genérico que se refiera a eventos, por ejemplo, proxies: Bluecoat, firewall: Palo Alto, etc.	EXIGIDO
5.1.1.12	La solución debe incluir al menos los siguientes métodos de autenticación: local, Radius, LDAP, Active Directory, Sigle sign-on.	EXIGIDO
5.1.1.13	La solución debe proporcionar un flujo de trabajo de incidentes para rastrear eventos.	EXIGIDO
5.1.1.14	Para el tránsito de todos los datos, debe realizarse con un cifrado SSL/TLS.	EXIGIDO

5.1.1.15	La solución debe soportar al menos tres formas de contactar al soporte: licencia de suscripción, chat de soporte, por el servicio de expertise on demand.	EXIGIDO
5.1.1.16	La solución debe soportar una consola maestra de alertas, con capacidad de personalizar dashboards, búsquedas, y resultados de búsquedas.	EXIGIDO
5.1.1.17	La solución debe soportar el uso de API para la administración, así como para integración de fuentes de datos, si así se requiere.	EXIGIDO
5.1.1.18	Los indicadores deben ser cargados a través de archivos CSV o JSON.	EXIGIDO
5.1.1.19	Los indicadores deben de incluir al menos los siguientes campos: Value, Notes, Risk, Type.	EXIGIDO
5.1.1.20	La solución debe de soportar dos tipos de reglas: las creadas por el fabricante y las personalizadas.	EXIGIDO
5.1.1.21	La solución debe mostrar un gráfico que muestre el porcentaje de las reglas habilitadas creadas por el fabricante que están siendo utilizadas y las que no.	EXIGIDO
5.1.1.22	Las reglas deben contener al menos la siguiente información: riesgo, nombre, estatus, opción de deshabilitar y ver la regla.	EXIGIDO
5.1.1.23	La solución debe permitir asignar una contraseña al reporte en formato pdf cuando éste sea enviado por correo electrónico.	EXIGIDO
5.1.1.24	La solución debe contar con un dashboard que muestre información sobre: estadísticas de eventos por segundo, estado general del dispositivo, eficacia de los sensores.	EXIGIDO
5.1.1.25	La solución debe mostrar en las tablas de alertas, al menos la siguiente información: riesgo, tipo, origen, primer evento, último evento, sumario, estado, hash.	EXIGIDO
5.1.1.26	La solución debe soportar la personalización de tablas de alertas.	EXIGIDO

5.1.1.27	La solución debe indicar el nivel de amenaza basado en la inteligencia que realice, tomando en consideración al menos los siguientes aspectos: el valor de un evento indeterminado, el valor de un evento benigno, el valor de un evento sospechoso, el valor de un evento malicioso.	EXIGIDO
5.1.1.28	La solución debe poder asignar alertas a los usuarios como parte del proceso de escalamiento y gestión de incidentes.	EXIGIDO
5.1.1.29	La solución debe incluir una vista sobre consejos de investigación, que permitan ofrecer mayor detalle a través de preguntas con consultas de búsqueda asociadas y así tener una mejor comprensión de la amenaza.	EXIGIDO
5.1.1.30	La solución debe poder exportar alertas a formato tipo JSON o CSV.	EXIGIDO
5.1.1.31	La solución debe soportar la búsqueda y descarga de transcripciones de PCAP.	EXIGIDO
5.1.1.32	La solución debe soportar al menos los siguientes tipos de log; security log, sysmon log, system log, application log, appLocker log, PowerShell Log, defender log, IIS log.	EXIGIDO
5.1.1.33	La solución debe soportar la identificación de actividad sospechosa a través del análisis del comportamiento indicado por detectores, incluyéndose al menos los siguientes: Beacon Detection, DNS Entropy Detection, DNS Fast-flux Detection, Geofeasibility Detetection, Credetial Misuse Detection, Unacknowledged Connection Detection, Anomalous WSman Activity Detection, Port Scanning Detection, Port Probing Detection, Data Theft (outbond) exfiltration Detection, Inbound Connections Detection, Server outbound Connections Detection, VPN Compromised Account Detection.	EXIGIDO
5.1.1.34	La solución debe ser compatible para procesar registros a través de los siguientes métodos: IETF, syslog, RFC5424, RFC3164.	EXIGIDO
5.1.1.35	La solución debe permitir la detección, validación, e investigación de alertas/amenazas, para así reconstruir el killchain de un ataque.	EXIGIDO
5.1.1.36	La solución debe proveer la capacidad de generar una puntuación de riesgo.	EXIGIDO

5.1.1.37	La solución debe tener la capacidad de minimizar el impacto de un incidente de forma automática.	EXIGIDO
5.1.1.38	La solución debe generar una investigación visual guiada con los detalles de una incidencia.	EXIGIDO
5.1.1.39	La solución debe tener integrado playbooks que automatizan las acciones de respuesta a las amenazas.	EXIGIDO
5.1.1.40	La solución debe crear correlaciones automáticamente, a partir de alertas, utilizando análisis estadístico.	EXIGIDO
5.1.1.41	La solución debe soportar alertas de terceros de más de 600 fuentes.	EXIGIDO
5.1.1.42	La solución debe ser una plataforma de operación SaaS que permita tomar control de incidentes desde la detección hasta la respuesta.	EXIGIDO
5.1.1.43	La solución debe detectar incidentes correlacionando datos de múltiples herramientas.	EXIGIDO
5.1.1.44	La solución debe asistir en la toma de decisiones a través de inteligencia contextual sobre amenazas.	EXIGIDO
5.1.1.45	La solución debe permitir centralizar la infraestructura y los datos de seguridad.	EXIGIDO
5.1.1.46	La solución debe tener la capacidad de mejorar la detección de amenazas y vulnerabilidades con análisis avanzados de comportamiento de los usuarios	EXIGIDO
5.1.1.47	La solución debe incluir paneles que brinden descripción del estado de las operaciones de seguridad tales como: - Numero de amenaza	EXIGIDO
5.1.1.48	- Puntaje de riesgo.	EXIGIDO
5.1.1.49	- Matriz de MITRE ATT&CK.	EXIGIDO
5.1.1.50	- Amenazas asignadas.	EXIGIDO
5.1.1.51	- Uso de datos dentro del entorno.	EXIGIDO

5.1.1.52	- Salud del entorno.	EXIGIDO
5.1.1.53	- Coincidencias de inteligencia que muestran actores e indicadores.	EXIGIDO
5.1.1.54	La solución debe permitir acciones para asignar, cerrar, suprimir, contener y exportar una alerta.	EXIGIDO
5.1.1.55	La solución debe soportar acciones para remediar la amenaza.	EXIGIDO
5.1.1.56	La solución debe ser capaz de proporcionar una representación visual de cada incidente y un resumen de lo que sucedió (vectores que estuvieron involucrados - como las alertas conectadas, entre sí).	EXIGIDO
5.1.1.57	La solución debe proporcionar información de los activos (host - usuario) basados en: - Clasificación de riesgo	EXIGIDO
5.1.1.58	- Etiquetarlos como activo VIP	EXIGIDO
5.1.1.59	- Exportar a un archivo CSV o JSON.	EXIGIDO
5.1.1.60	La solución debe permitir la integración para automatizar tareas frecuentes a través de playbooks proporcionados por: Azure, Cloudvisory, detección bajo de manda, serviceNow, VirusTotal.	EXIGIDO
5.1.1.61	La solución debe contar con un portal que permita agregar conexiones a la nube, abarcando plataformas como: Amazon Web Services (AWS), Google Cloud Platform (GCP), GSuite, Microsoft Azure, Microsoft 365 y Microsoft Teams. También se admiten alertas de proveedores como MimeCast, Proofpoint, MS Defender, Sophos (AV), TrendMicro y CrowdStrike.	EXIGIDO
5.1.1.62	La solución debe permitir configurar notificaciones por correo electrónico.	EXIGIDO
5.1.1.63	La solución debe mostrar información sobre cada táctica (Mitre ATT&CK) que se intentó durante el periodo de tiempo especificado.	EXIGIDO

5.1.1.64	La solución debe mostrar el número de técnicas (Mitre ATT&CK) que se utilizaron en el intento de la táctica.	EXIGIDO
5.1.1.65	La solución debe detallar el número de amenazas asociadas a cada técnica (Mitre ATT&CK).	EXIGIDO
5.1.1.66	La solución debe proporcionar una comprensión del flujo de ataque a través de un gráfico que muestre los siguientes nodos: - Múltiples herramientas.	EXIGIDO
5.1.1.67	- Múltiples fuentes.	EXIGIDO
5.1.1.68	- Alertas múltiples.	EXIGIDO
5.1.1.69	- Activos múltiples.	EXIGIDO
5.1.1.70	- Múltiples artefactos.	EXIGIDO
5.1.1.71	La solución debe tener la capacidad de agrupar una amenaza a través de una correlación o una alerta.	EXIGIDO
5.1.1.72	La solución debe mostrar un gráfico de tabla que contenga al menos la siguiente información: riesgo, tipo, total de activos, total de eventos, primer evento, último evento, origen/destino, resumen (summary), asignación, estatus.	EXIGIDO
5.1.1.73	La solución debe ser capaz de calcular el riesgo de un activo multiplicando la suma de los puntajes de riesgo de todas las alertas por el número de reglas para dividirse entre el total de alertas utilizando la siguiente escala o similar: 0-59: puntuación - severidad baja; 60-79: puntuación - severidad media; 80 - 99: puntuación - severidad alta; Mayor o igual a 100: puntuación - severidad crítica.	EXIGIDO
5.1.1.74	La solución debe tener la capacidad de realizar las siguientes acciones relacionadas con la amenaza: - Contener	EXIGIDO
5.1.1.75	- Eliminar	EXIGIDO
5.1.1.76	- Asignar a un usuario	EXIGIDO

5.1.1.77	- Cierre o suprimir	EXIGIDO
5.1.1.78	La solución debe tener la capacidad de realizar las siguientes acciones relacionadas con la amenaza: - Activar un playbook	EXIGIDO
5.1.1.79	- Realizar una reparación	EXIGIDO
5.1.1.80	La solución debe mostrar una gráfica sobre las actividades playbooks ejecutadas en la organización.	EXIGIDO
5.1.1.81	La solución debe permitir la visualización del diagrama de flujo que realiza el seguimiento de cada paso de la ejecución dentro del playbook.	EXIGIDO
5.1.1.82	La solución debe permitir que el diagrama de flujo de la actividad del playbook y los detalles de la acción puedan ser exportados a formato JSON.	EXIGIDO
5.1.1.83	La solución debe soportar la asignación de acciones de respuesta a los playbooks a través de artefactos relevantes como: hashes MD5, alertas, dominios, direcciones IP).	EXIGIDO
5.1.1.84	La solución debe contar con la capacidad de que el fabricante cree paquetes de reglas dedicadas a tipos específicos de detección como: suplantación de identidad, para Windows, etc.	EXIGIDO
5.1.1.85	La solución debe permitir visualizar la regla a través de una tabla la información donde se identifique: nombre, consulta (query), estatus, playbook, riesgo, creación.	EXIGIDO

LOTE N° 6 - SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN FIREWALL DE APLICACIÓN WEB (WAF)

ITEM N° 1 - Servicio de suscripción a Solución Firewall de Aplicación Web (WAF)

6.1.1 Características principales de la Solución

6.1.1.1	Se solicita el servicio de suscripción a solución firewall de aplicación web Barracuda 660 Vx implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 12 meses computados a partir de fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.	EXIGIDO
---------	--	---------

6.1.1.2	<p>La Solución debe contar con las siguientes características:</p> <ul style="list-style-type: none"> Backend Servers Supported CPU Cores Allowed Throughput Response Control Outbound Data Theft Protection File Upload Control Vulnerability Scanner Integration Protection against Application DDoS Attacks Bot Defense/ Web Scraping Protection Network Firewall JSON Protection XML Firewall URL Encryption Adaptive Profiling AV for File Uploads Advanced Threat Protection Authentication and Authorization LDAP/RADIUS Load Balancing Caching and Compression Content Routing High Availability Advanced Routing 	EXIGIDO
---------	--	---------

LOTE N° 7 SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE DETECCIÓN Y RESPUESTA PARA NETWORKING - NDR

ITEM N° 1 Servicio de suscripción a Solución de Detección y Respuesta para Networking - NDR

7.1.1 Características principales de la Solución:

7.1.1.1	<p>Se solicita el servicio de suscripción a una Solución de ciberseguridad para la detección y respuesta a incidentes para networking, mediante el análisis de la metadatos del tráfico de red, para 300 fuentes, con el objetivo de realizar la medición e identificación de IoCs (indicadores de compromiso) a través de la técnica de detección continua de compromisos, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.</p>	EXIGIDO
7.1.1.2	<p>La solución debe proporcionar, en modalidad de SaaS, la capacidad de medir el compromiso de la infraestructura tecnológica, en tiempo real, sin importar el formato enviado, siempre y cuando contenga la información necesaria.</p>	EXIGIDO

7.1.1.3	La solución debe tener la capacidad de recolectar, procesar y analizar las consultas DNS de la organización para identificar qué activos (estaciones de trabajo, servidores, equipos de red, etc.) están intentando comunicarse con potenciales atacantes.	EXIGIDO
7.1.1.4	La solución debe tener la capacidad de recolectar, procesar y analizar los datos del Spambox para identificar quién y cómo están intentando atacar a la organización.	EXIGIDO
7.1.1.5	La solución debe incluir agentes o colectores para al menos sistemas operativos Windows 10 o superior y Windows Server 2012 o superior.	EXIGIDO
7.1.1.6	La solución debe poder ser implementada y debe tener la capacidad de realizar el proceso de recolección de datos sin la necesidad de hardware de propósito específico, tal como network taps u otros. El proceso de recolección de datos para medir compromiso debe estar basado en metadatos.	EXIGIDO
7.1.1.7	El proceso de medición de compromiso debe estar basado en: consultas DNS, spambox, netflows, logs de proxy y/o firewall.	EXIGIDO
7.1.1.8	La solución debe tener la capacidad de clasificar el resultado de la medición de compromiso. Ejemplo: Malware, C&C, Phishing.	EXIGIDO
7.1.1.9	La solución debe almacenar datos de forma histórica de al menos 2 años.	EXIGIDO
7.1.1.10	La solución debe tener la capacidad de realizar una revisión histórica o 'playback' de nuevos ataques para identificar compromiso histórico basado en nueva información.	EXIGIDO
7.1.1.11	La solución debe identificar el origen del compromiso de manera precisa y sin la necesidad de la instalación de hardware de propósito específico.	EXIGIDO
7.1.1.12	El proceso de análisis de los metadatos de la organización debe estar basado en: - Correlación contra más de 80 fuentes de ciberinteligencia.	EXIGIDO

7.1.1.13	- Analizadores/algoritmos, supervisados o no, de machine learning e inteligencia artificial.	EXIGIDO
7.1.1.14	La solución debe implementar la capacidad de adicionar nuevas fuentes de ciberinteligencia con conceptos tales como BYOTI "Bring your own threat intelligence".	EXIGIDO
7.1.1.15	La solución debe proveer un portal web que sea accesible desde las últimas versiones estables de los navegadores Google Chrome, Firefox, Edge y Safari.	EXIGIDO
7.1.1.16	La solución debe incluir <i>al menos uno de</i> los siguientes métodos de autenticación: local, Radius, LDAP, Active Directory, Sigle sign-on.	EXIGIDO

7.1.2 Reportes y vistas

7.1.2.1	El portal debe contener una vista que provea estadísticas de los indicadores de compromiso.	EXIGIDO
7.1.2.2	La solución debe tener la opción de aplicar filtros predefinidos, como por fecha, ejemplo: Hoy, ayer, últimos 7 días, últimos 30 días.	EXIGIDO
7.1.2.3	La solución debe tener la opción de aplicar filtros por un periodo de tiempo personalizado.	EXIGIDO
7.1.2.4	La solución debe permitir agrupar los activos a través de etiquetas como: tipo de activos (estaciones de trabajo, servidores, equipos de red, etc.), grupos de usuarios, etc., de acuerdo con la necesidad de la organización.	EXIGIDO
7.1.2.5	La solución debe incluir frecuencia del compromiso por día de la semana y hora del día. Asimismo, debe mostrar la distribución del ataque basado en etiquetas previamente configuradas (ejemplo: usuario remoto, oficina central, IOT), también debe contar con recursos relacionados con los compromisos y con unas guías (playbooks) para cada tipo de ataque detectado.	EXIGIDO
7.1.2.6	La solución debe permitir mostrar los IoCs por cada compromiso detectado y se debe poder descargar directamente de la plataforma, en formato CSV.	EXIGIDO

7.1.2.7	La solución debe tener una vista de incidentes que permita gestionar incidentes abiertos, cerrar incidentes y silenciar incidentes llevando registro de las acciones tomadas en los mismos.	EXIGIDO
7.1.2.8	La solución debe incluir información del spambox como: volumen de correos analizados, destinatarios que reciben más spam, tendencias de ataques, días y horas de la semana en la que se recibe más correos maliciosos y correlación del spambox con respecto a la comunicación efectiva realizada hacia el potencial atacante.	EXIGIDO
7.1.2.9	La solución debe enviar reportes vía correo electrónico con información de resultados de la evaluación de compromiso.	EXIGIDO
7.1.2.10	La solución debe enviar notificación al correo electrónico del administrador de la plataforma o a los usuarios definidos en caso de la existencia de un indicador de compromiso detectado.	EXIGIDO
7.1.2.11	La solución debe tener la opción de configurar la periodicidad de las notificaciones, tales como: envío de correo con las alertas de la ultima hora o de las últimas 4 horas, etc.	EXIGIDO
7.1.2.12	La solución debe incluir en las notificaciones, el análisis de cada incidente basado en la matriz MITRE ATT&CK.	EXIGIDO
7.1.2.13	La solución debe permitir configurar la periodicidad de los reportes. Ejemplo: diario, semanal, bisemanal y mensual	EXIGIDO

7.1.3 Características y alertas

7.1.3.1	La solución debe poder responder de forma automática, conectándose vía API a la infraestructura tecnológica para ajustar las políticas de bloqueo pertinentes, ante la detección de un compromiso.	EXIGIDO
7.1.3.2	La solución debe incorporar capacidades automáticas de bloqueo con los fabricantes más reconocidos de la industria, tales como: Palo Alto Networks, Fortinet, Checkpoint, Cisco, entre otros.	EXIGIDO

7.1.3.3	La solución debe proporcionar una API de forma tal que la organización pueda construir la integración que requiera para propósitos de defensa o gestión de incidentes.	EXIGIDO
7.1.3.4	La solución debe tener la capacidad de realizar la descarga de información de amenazas en formato STIX.	EXIGIDO
7.1.3.5	La solución debe proporcionar el contexto de cada compromiso con referencias internas y externas para entender la naturaleza del mismo.	EXIGIDO
7.1.3.6	La solución debe permitir el direccionamiento del tráfico DNS a un DNS publico ofrecido por el proveedor.	EXIGIDO
7.1.3.7	La solución debe permitir consumir metadatos de plataformas de VPN para medición de compromiso de dispositivos remotos en modo full tunnel y split tunnel.	EXIGIDO
7.1.3.8	La solución debe proporcionar una API abierta para consumir metadatos, de forma que la organización pueda utilizarla para propósitos específicos.	EXIGIDO
7.1.3.9	La solución debe soportar colectores o su equivalente para los hipervisores VirtualBox, Hyper-V y VMware.	EXIGIDO

7.1.4 Calidad y capacidad del Talento Humano

7.1.4.1	El proveedor debe ofrecer la gestión de los incidentes generados en la solución en modalidad 7x24.	EXIGIDO
7.1.4.2	El alcance de la gestión de incidentes debe entregar al equipo de la organización la guía necesaria para la mitigación de estos, identificados por la solución.	EXIGIDO
7.1.4.3	El proveedor debe proporcionar el apoyo necesario para el despliegue de la solución.	EXIGIDO
7.1.4.4	El proveedor debe proporcionar resolución de dudas sobre la forma de mitigación de los compromisos detectados.	EXIGIDO

- 7.1.4.5 El proveedor debe disponibilizar EXIGIDO
entrenamiento/capacitación de la solución ofrecida para
traspaso de conocimiento al personal para asegurar la
correcta operación.
- 7.1.4.6 El proveedor debe incluir un plan de implementación, EXIGIDO
actualización u optimización, además del
acompañamiento continuo a lo largo de la duración de
la prestación del servicio.

Equipos y dispositivos existentes en el BCP:

Tipo	Descripción	Cantidad
Server	Total de Servidores Físicos	50
Storage	IBM, Dell	7
Hipervisores	ESXi 5, 6	34
Hipervisores	HyperV	2
Server	CentOS Linux	39
Server	RedHat	18
Server	Generic Linux	13
Server	Microsoft Windows Server Otros	54
Server	Microsoft Windows Server 2012	60
Server	Microsoft Windows Server 2016	3
MBD	MS SQL	5
MBD	PostgreSQL	1
MBD	MySQL	4
MBD	Sybase	4

MBD	Oracle	6
Server	Servidor de archivos	5
Server	Servidor Exchange	2
Firewall	Checkpoint	3
Firewall	Cisco FTD	2
Firewall	Cisco ASA	5
LB	Citrix	2
Router	Cisco IOS	3
Switch	Cisco IOS	70
Switch	Cisco NX-OS	15
Wireless	Cisco WLAN Controller	3
Wireless	Cisco AP	50
Proxy	Forcepoint	2
Usuarios	Estaciones de trabajo (PCs, Notebooks)	900
Usuarios	Dispositivos móviles (Android/iOS)	70

Punto 2

Se modifican las fechas establecidas en el SICP.

Se detectaron modificaciones en las siguientes cláusulas:

Sección: Suministros requeridos - especificaciones técnicas

- Detalles de los productos y/ servicios con las respectivas especificaciones técnicas - CPS

Se puede realizar una comparación de esta versión del pliego con la versión anterior en el siguiente enlace:

<https://www.contrataciones.gov.py/licitaciones/convocatoria/426350-lpn-n-13-2023-contratacion-servicios-gestion-ciberseguridad-1/pliego/2/diferencias/1.html?seccion=adenda>

La adenda es el documento emitido por la convocante, mediante la cual se modifican aspectos establecidos en la convocatoria y/o en las bases de la licitación y/o en los contratos suscriptos. La adenda será considerada parte integrante del documento cuyo contenido modifique.

DATOS DE LA LICITACIÓN

Los Datos de la Licitación constituye la información proporcionada por la convocante para establecer las condiciones a considerar del proceso particular, y que sirvan de base para la elaboración de las ofertas por parte de los potenciales oferentes.

Contratación Pública Sostenibles - CPS

Las compras públicas juegan un papel fundamental en el desarrollo sostenible, así como en la promoción de estilos de vida sostenibles.

El Estado, por medio de las actividades de compra de bienes y servicios sostenibles, busca incentivar la generación de nuevos emprendimientos, modelos de negocios innovadores y el consumo sostenible. La introducción de criterios y especificaciones técnicas con consideraciones sociales, ambientales y económicas tiene como fin contribuir con el Desarrollo Sostenible en sus tres dimensiones.

El símbolo “CPS” en este pliego de bases y condiciones, es utilizado para indicar criterios o especificaciones sostenibles.

Criterios sociales y económicos:

- Los oferentes deberán indicar bajo declaración jurada el pago del salario mínimo a sus colaboradores, además de garantizar la no contratación de menores.
- Los oferentes deberán dar cumplimiento a las disposiciones legales vigentes asegurando a los trabajadores dependientes condiciones de trabajo dignas y justas en lo referente al salario, cargas sociales, provisión de uniformes, provisión de equipos de protección individual, bonificación familiar, jornada laboral, asegurar condiciones especiales a trabajadores expuestos a trabajos insalubres y peligrosos, remuneración por jornada nocturna.
- Las deducciones al salario, anticipos y préstamos a los trabajadores no podrán exceder los límites legales. Los términos y condiciones relacionados a los mismos deberán comunicarse de manera clara, para que los trabajadores los entiendan.
- Los oferentes adjudicados deberán fomentar en la medida de lo posible, la creación de empleo local y el uso de suministros locales.

Criterios ambientales:

- El oferente adjudicado deberá utilizar en la medida de lo posible, insumos cuyo embalaje pueda ser reutilizado o reciclado.
- El oferente adjudicado deberá cumplir con los lineamientos ambientales, incluidos en el ordenamiento jurídico o dictado por la institución, tales como: cooperación en acciones de recolección, separación de residuos sólidos, disposición adecuada de los residuos, participación del personal en actividades de capacitación impartidas por la institución, entre otros.
- El oferente adjudicado deberá asegurar que todos los residuos generados por sus actividades sean adecuadamente gestionados (identificados, segregados y destinados) y buscar su reducción o eliminación en la fuente, por medio de prácticas como la modificación de los procesos de producción, manutención y de las instalaciones utilizadas, además de la sustitución, conservación, reciclaje o reutilización de materiales.

Conducta empresarial responsable:

Los oferentes deberán observar los más altos niveles de integridad, así como altos estándares de conducta de negocios, ya sea durante el procedimiento de licitación o la ejecución de un contrato. Asimismo, se comprometen a:

- No ofrecer, prometer, dar ni solicitar, directa o indirectamente, pagos ilícitos u otras ventajas indebidas para obtener o conservar un contrato u otra ventaja ilegítima.
- No ofrecer, prometer o conceder ventajas indebidas, pecuniarias o de otro tipo a funcionarios públicos. Tampoco deberán solicitar, recibir o aceptar ventajas indebidas, pecuniarias o de otro tipo, de funcionarios públicos o empleados de sus socios comerciales.
- Introducir políticas y programas contra la corrupción e implementarlas dentro de sus operaciones.
- Garantizar que todos los recursos a ser empleados en la ejecución de un contrato público sean de origen lícito.
- Garantizar que los fondos obtenidos de una licitación pública no sean destinados a fines ilícitos.

Difusión de los documentos de la licitación

Todos los datos y documentos de esta licitación deben ser obtenidos directamente del Sistema de Información de Contrataciones Públicas (SICP). Es responsabilidad del oferente examinar todos los documentos y la información de la licitación que obren en el mismo.

Aclaración de los documentos de la licitación

Todo oferente potencial que necesite alguna aclaración del pliego de bases y condiciones podrá solicitarla a la convocante. El medio por el cual se recibirán las consultas es el Sistema de Información de Contrataciones Públicas (SICP), y/o si es el caso, en la Junta de Aclaraciones que se realice en la fecha, hora y dirección indicados por la convocante.

La convocante responderá por escrito a toda solicitud de aclaración del pliego de bases y condiciones que reciba dentro del plazo establecido o que se derive de la Junta de Aclaraciones.

La convocante publicará una copia de su respuesta, incluida una explicación de la consulta, pero sin identificar su procedencia, a través del Sistema de Información de Contrataciones Públicas (SICP), dentro del plazo tope.

La inasistencia a la Junta de Aclaraciones no será motivo de descalificación de la oferta.

La convocante podrá optar por responder las consultas en la Junta de Aclaraciones o podrá diferirlas, para que sean respondidas conforme con los plazos de respuestas o emisión de adendas. En todos los casos se deberá levantar acta circunstanciada.

Documentos de la oferta

El pliego, sus adendas y aclaraciones no forman parte de la oferta, por lo que no se exigirá la presentación de copias de los mismos con la oferta.

Los oferentes inscriptos en el Sistema de Información de Proveedores del Estado (SIPE) de la DNCP, podrán presentar con su oferta, la constancia firmada emitida a través del SIPE, que reemplazará a los documentos solicitados por la convocante en el anexo pertinente del presente pliego.

Los oferentes deberán indicar en su oferta, que documentos que forman parte de la misma son de carácter confidencial e invocar la norma que ampara dicha reserva, para así dar cumplimiento a lo estipulado en la Ley N° 5282/14 "DE LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL". Si el oferente no hace pronunciamiento expreso amparado en la Ley, se entenderá que toda su oferta y documentación es pública.

Oferentes en consorcio

Dos o más interesados que no se encuentren comprendidos en las inhabilidades para presentar ofertas o contratar, podrán unirse temporalmente para presentar una oferta sin crear una persona jurídica.

Para ello deberán presentar escritura pública de constitución del consorcio o un acuerdo con el compromiso de formalizar el consorcio por escritura pública en caso de resultar adjudicados, antes de la firma del contrato.

Los integrantes de un consorcio no podrán presentar ofertas individuales ni conformar más de un consorcio en un mismo lote o ítem, lo que no impide que puedan presentarse individualmente o conformar otro consorcio que participe en diferentes partidas.

Aclaración de las ofertas

Con el objeto de facilitar el proceso de revisión, evaluación, comparación y posterior calificación de ofertas, el Comité de Evaluación solicitará a los oferentes, aclaraciones respecto de sus ofertas, dichas solicitudes y las respuestas de los oferentes se realizarán por escrito.

A los efectos de confirmar la información o documentación suministrada por el oferente, el Comité de Evaluación, podrá solicitar aclaraciones a cualquier fuente pública o privada de información.

Las aclaraciones de los oferentes que no sean en respuesta a aquellas solicitadas por la convocante, no serán consideradas.

No se solicitará, ofrecerá, ni permitirá ninguna modificación a los precios ni a la sustancia de la oferta, excepto para confirmar la corrección de errores aritméticos.

Disconformidad, errores y omisiones

Siempre y cuando una oferta se ajuste sustancialmente al pliego de bases y condiciones, el Comité de Evaluación, requerirá que cualquier disconformidad u omisión que no constituya una desviación significativa, sea subsanada en cuanto a la información o documentación que permita al Comité de Evaluación realizar la calificación de la oferta.

A tal efecto, el Comité de Evaluación emplazará por escrito al oferente a que presente la información o documentación necesaria, dentro de un plazo razonable establecido por el mismo, bajo apercibimiento de rechazo de la oferta. El Comité de Evaluación, podrá reiterar el pedido cuando la respuesta no resulte satisfactoria, toda vez que no viole el principio de igualdad.

Con la condición de que la oferta cumpla sustancialmente con los Documentos de la Licitación, la Convocante corregirá errores aritméticos de la siguiente manera y notificará la oferente para su aceptación:

1. Si hay una discrepancia entre un precio unitario y el precio total obtenido al multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido.
2. Si hay un error en un total que corresponde a la suma o resta de subtotales, los subtotales prevalecerán y se corregirá el total
3. En caso de que el oferente haya cotizado su precio en guaraníes con décimos y céntimos, la convocante procederá a realizar el redondeo hacia abajo.
4. Si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras a menos que la cantidad expresada en palabras corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras de conformidad con los párrafos (1) y (2) mencionados.

Idioma de la oferta

La oferta deberá ser presentada en idioma castellano o en su defecto acompañado de su traducción oficial, realizada por un traductor público matriculado en la República del Paraguay.

La convocante permitirá con la oferta, la presentación de catálogos, anexos técnicos o folletos en idioma distinto al castellano y sin traducción:

Sí, la convocante aceptará la presentación de catálogos, anexos técnicos, folletos, certificaciones y otros textos complementarios en idioma inglés, los cuales no requerirán traducción fidedigna al idioma castellano. Los documentos citados presentados en otros idiomas distintos al castellano y al inglés deberán estar traducidos al castellano por un traductor público matriculado en la República del Paraguay.

Idioma del contrato

El contrato, así como toda la correspondencia y documentos relativos al Contrato, deberán ser escritos en idioma castellano. Los documentos de sustento y material impreso que formen parte del contrato, pueden estar redactados en otro idioma siempre que estén acompañados de una traducción realizada por traductor matriculado en la República del Paraguay, en sus partes pertinentes al idioma castellano y, en tal caso, dicha traducción prevalecerá para efectos de interpretación del contrato.

El proveedor correrá con todos los costos relativos a las traducciones, así como todos los riesgos derivados de la exactitud de dicha traducción.

Moneda de la oferta y pago

La moneda de la oferta y pago será:

En Guaraníes para todos los oferentes

La cotización en moneda diferente de la indicada en este apartado será causal de rechazo de la oferta. Si la oferta seleccionada es en guaraníes, la oferta se deberá expresar en números enteros, no se aceptarán cotizaciones en decimos y céntimos.

Visita al sitio de ejecución del contrato

La convocante dispone la realización de una visita al sitio con las siguientes indicaciones:

No Aplica

Al culminar la o las visitas, se labrará acta en la cual conste, la fecha, lugar y hora de realización, en la cual se identifique el nombre de las personas que asistieron en calidad de potenciales oferentes, así como del funcionario encargado de dicho acto.

Los gastos relacionados con dicha visita correrán por cuenta del oferente.

Cuando la convocante haya establecido que no será requisito de participación, el oferente podrá declarar bajo fe de juramento conocer el sitio y que cuenta con la información suficiente para preparar la oferta y ejecutar el contrato.

Precio y formulario de la oferta

El oferente indicará el precio total de su oferta y los precios unitarios de los bienes que se propone suministrar, utilizando para ello el formulario de oferta y lista de precios, disponibles para su descarga a través del SICP, formando ambos un único documento.

1. Para la cotización el oferente deberá ajustarse a los requerimientos que se indican a continuación:

a) El precio cotizado deberá ser el mejor precio posible, considerando que en la oferta no se aceptará la inclusión de descuentos de ningún tipo.

b) En el caso del sistema de adjudicación por la totalidad de los bienes requeridos, el oferente deberá cotizar en la lista de precios todos los ítems, con sus precios unitarios y totales correspondientes.

c) En el caso del sistema de adjudicación por lotes, el oferente cotizará en la lista de precios uno o más lotes, e indicará todos los ítems del lote ofertado con sus precios unitarios y totales correspondientes. En caso de no cotizar uno o más lotes, los lotes no cotizados no requieren ser incorporados a la planilla de precios.

d) En el caso del sistema de adjudicación por ítems, el oferente podrá ofertar por uno o más ítems, en cuyo caso deberá cotizar el precio unitario y total de cada uno o más ítems, los ítems no cotizados no requieren ser incorporados a la planilla de precios.

2. En caso de que se establezca en las bases y condiciones, los precios indicados en la lista de precios serán consignados separadamente de la siguiente manera:

a) El precio de bienes cotizados, incluidos todos los derechos de aduana, los impuestos al valor agregado o de otro tipo pagados o por pagar sobre los componentes y materia prima utilizada en la fabricación o ensamblaje de los bienes;

b) Todo impuesto al valor agregado u otro tipo de impuesto que obligue la República del Paraguay a pagar sobre los bienes en caso de ser adjudicado el contrato; y

c) El precio de otros servicios conexos (incluyendo su impuesto al valor agregado), si lo hubiere, enumerados en los datos de la licitación.

3. En caso de indicarse en el SICP, que se utilizará la modalidad de contrato abierto, cuando se realice por montos mínimos y máximos deberán indicarse el precio unitario de los bienes ofertados; y en caso de realizarse por cantidades mínimas y máximas, deberán cotizarse los precios unitarios y los totales se calcularán multiplicando los precios unitarios por la cantidad máxima correspondiente.

4. El precio del contrato que cobre el proveedor por los bienes suministrados en virtud del contrato no podrá ser diferente a los precios unitarios cotizados en su oferta, excepto por cualquier ajuste previsto en el mismo.

5. En caso que se requiera el desglose de los componentes de los precios será con el propósito de facilitar a la convocante la comparación de las ofertas.

Abastecimiento simultáneo

En caso de que se opte por el sistema de abastecimiento simultaneo, en éste apartado se deberá indicar la manera de distribución

de los mismos:

No Aplica

Incoterms

La edición de incoterms para esta licitación será:

No Aplica

Las expresiones DDP, CIP, FCA, CPT y otros términos afines, se regirán por las normas prescriptas en la edición vigente de los Incoterms publicada por la Cámara de Comercio Internacional.

Durante la ejecución contractual, el significado de cualquier término comercial, así como los derechos y obligaciones de las partes serán los prescritos en los Incoterms, a menos que sea inconsistente con alguna disposición del Contrato.

Autorización del Fabricante

Los productos a los cuales se le requerirá Autorización del Fabricante son los indicados a continuación:

El oferente deberá presentar fotocopia simple del documento vigente que acredite fehacientemente que el Oferente es Fabricante y/o Representante Oficial y/o Distribuidor Oficial y/o Partner Autorizado por el Fabricante para el Paraguay de la solución a ser utilizada en el marco del servicio, ya sea mediante documento emitido por la firma autorizante o mediante la presentación del Formulario correspondiente incluido en la Sección Formularios debidamente suscripto por la firma autorizante.

Cuando la convocante lo requiera, el oferente deberá acreditar la cadena de autorizaciones, hasta el fabricante, productor o prestador de servicios.

Muestras

Se requerirá la presentación de muestras de los siguientes productos y en las siguientes condiciones:

No Aplica

En caso de ser solicitadas, las muestras deberán ser presentadas junto con la oferta, o bien en el plazo fijado por la convocante en este apartado, la cual será considerada requisito indispensable para la evaluación de la oferta. La falta de presentación en la forma

y plazo establecido por la convocante será causal de descalificación de la oferta.

Ofertas Alternativas

Se permitirá la presentación de oferta alternativa, según los siguientes criterios a ser considerados para la evaluación de la misma:

No Aplica

Copias de la oferta - CPS

El oferente presentará su oferta original. En caso de que la convocante requiera la presentación de copias lo deberá indicar en este apartado, las copias deberán estar identificadas como tales.

Cuando la presentación de ofertas se realice a través del sistema de Oferta Electrónica, la convocante no requerirá de copias.

Cantidad de copias requeridas:

0 copias

Formato y firma de la oferta

1. El formulario de oferta y la lista de precios serán firmados, física o electrónicamente, según corresponda por el oferente o por las personas debidamente facultadas para firmar en nombre del oferente.
2. No serán descalificadas las ofertas que no hayan sido firmadas en documentos considerados no sustanciales.
3. Los textos entre líneas, tachaduras o palabras superpuestas serán válidos solamente si llevan la firma de la persona que firma la Oferta.
4. La falta de foliatura no podrá ser considerada como motivo de descalificación de las ofertas.

Periodo de validez de las ofertas

Las ofertas deberán mantenerse válidas (en días corridos) por:

90

Las ofertas se deberán mantener válidas por el periodo indicado en el presente apartado, a partir de la fecha límite para la

presentación de ofertas, establecido por la convocante. Toda oferta con un periodo menor será rechazada.

La convocante en circunstancias excepcionales podrá solicitar, por escrito, al oferente que extienda el periodo de validez de la oferta, por lo tanto la Garantía de Mantenimiento de la Oferta deberá ser también prorrogada.

El oferente puede rehusarse a tal solicitud sin que se le haga efectiva su Garantía de Mantenimiento de Oferta. A los oferentes que acepten la solicitud de prórroga no se les pedirá ni permitirá que modifiquen sus ofertas.

Garantías: instrumentación, plazos y ejecución.

1. La garantía de mantenimiento de oferta deberá expedirse en un monto en guaraníes que no deberá ser inferior al porcentaje especificado en el SICP. El oferente puede adoptar cualquiera de las formas de instrumentación de las garantías dispuestas por las normativas vigentes.

2. En los contratos abiertos, el porcentaje de las garantías a ser presentado por los oferentes que participen, deberá ser aplicado sobre el monto máximo del llamado; si la adjudicación fuese por lote o ítem ofertado, deberán sumarse los valores máximos de cada lote o ítem ofertado, a fin de obtener el monto sobre el cual se aplicará el porcentaje de la citada garantía.

3. En caso de instrumentarse a través de Garantía Bancaria, deberá estar sustancialmente de acuerdo con el formulario de Garantía de Mantenimiento de oferta incluido en la Sección "Formularios".

4. La garantía de mantenimiento de oferta en caso de oferentes en consorcio deberá ser presentado de la siguiente manera:

- Consorcio constituido por escritura pública: deberán emitir a nombre del consorcio legalmente constituido por escritura pública, del líder del consorcio o de todos los socios que la integran;
- Consorcio en proceso de formación con acuerdo de intención: deberán emitir a nombre del líder del consorcio en proceso de formación con acuerdo de intención o de todos los miembros que la integran.

5. La garantía de mantenimiento de ofertas podrá ser ejecutada:

- a) Si el oferente altera las condiciones de su oferta,
- b) Si el oferente retira su oferta durante el período de validez de la oferta,
- c) Si no acepta la corrección aritmética del precio de su oferta, en caso de existir,
- d) Si el adjudicatario no procede, por causa imputable al mismo a:
 - d.1. Suministrar los documentos indicados en el pliego de bases y condiciones para la firma del contrato,
 - d.2. Firmar el contrato,
 - d.3. Suministrar en tiempo y forma la garantía de cumplimiento de contrato,
 - d.4. Cuando se comprobare que las declaraciones juradas presentadas por el oferente adjudicado con su oferta sean falsas,
 - d.5. Si el adjudicatario no presentare las legalizaciones correspondientes para la firma del contrato, cuando éstas sean requeridas, o
 - d.6. No se formaliza el consorcio por escritura pública, antes de la firma del contrato.

6. Las garantías tanto de Mantenimiento de Oferta, Cumplimiento de Contrato o de Anticipo, sea cual fuere la forma de instrumentación adoptada, deberá ser pagadera ante solicitud escrita de la convocante donde se haga constar el monto reclamado, cuando se tenga acreditada una de las causales de ejecución de la póliza. En estos casos será requisito que previamente el oferente sea notificado del incumplimiento y la intimación de que se hará efectiva la ejecución del monto asegurado.

7. Si la entrega de los bienes o la prestación de los servicios se realizare en un plazo menor o igual a diez (10) días calendario, posteriores a la firma del contrato, la garantía de fiel cumplimiento deberá ser entregada antes del cumplimiento de la prestación.

8. La garantía de Fiel Cumplimiento de Contrato será liberada y devuelta al proveedor, a requerimiento de parte, a más tardar treinta (30) días contados a partir de la fecha de cumplimiento de las obligaciones del proveedor en virtud de contrato, incluyendo cualquier obligación relativa a la garantía de los bienes.

Periodo de Validez de la Garantía de Mantenimiento de Oferta

El plazo de validez de la Garantía de Mantenimiento de Oferta (en días calendario) será de:

120

El oferente deberá presentar como parte de su oferta una Garantía de Mantenimiento de acuerdo al porcentaje indicado para ello en el SICP y por el plazo indicado en este apartado.

Porcentaje de Garantía de Fiel Cumplimiento de Contrato

El Porcentaje de Garantía de Fiel Cumplimiento de Contrato es de:

10,00 %

La garantía de Fiel Cumplimiento de Contrato deberá ser presentada por el proveedor, dentro de los 10 días calendarios siguientes a partir de la fecha de suscripción del contrato, de conformidad con lo dispuesto en el artículo 39 de la Ley N° 2051/2003.

Periodo de validez de la Garantía de Cumplimiento de Contrato

El plazo de vigencia de la Garantía de Fiel Cumplimiento de Contrato será de:

La Garantía deberá estar vigente hasta por lo menos 30 (treinta) días posteriores al vencimiento del plazo máximo de entrega/instalación de los bienes o prestación de los servicios previsto en el presente PBC.

Periodo de validez de la Garantía de los bienes

El plazo de validez de la Garantía de los bienes será el siguiente:

El Proveedor deberá emitir una Garantía de Buen Servicio y Calidad, mediante una nota en carácter de declaración jurada a nombre de la Convocante, en virtud de la cual el Oferente manifieste que correrán a su cargo, por cuenta propia y sin costo para el BCP, las reposiciones, sustituciones, reparaciones y/o modificaciones que correspondan, cuando se observasen

fallas y/o deficiencias en los servicios ofertados, por causas que le fueran imputables, a partir de la fecha de emisión de la conformidad del área técnica (Departamento de Ciberseguridad) y durante el plazo establecido para el servicio de cada lote ofertado en el apartado Especificaciones Técnicas de la Sección Suministros Requeridos especificaciones técnicas del PBC.

En caso de que dicha Garantía haya sido presentada por el Proveedor al momento de la presentación de su oferta, la misma será válida durante la ejecución contractual, no siendo necesaria la presentación de la misma nuevamente

Tiempo de funcionamiento de los bienes

El periodo de tiempo estimado de funcionamiento de los bienes, para los efectos de repuestos será de:

No Aplica

Plazo de reposición de bienes

El plazo de reposición de bienes para reparar o reemplazar será de:

El establecido en cada caso por el BCP en la nota escrita de requerimiento a ser remitida al Proveedor.

El proveedor garantiza que todos los bienes suministrados están libres de defectos derivados de actos y omisiones que este hubiera incurrido, o derivados del diseño, materiales o manufactura, durante el uso normal de los bienes en las condiciones que imperen en la República del Paraguay.

1. La Contratante comunicará al proveedor la naturaleza de los defectos y proporcionará toda evidencia disponible, inmediatamente después de haberlos descubierto. La contratante otorgará al proveedor facilidades razonables para inspeccionar tales defectos.

Tan pronto reciba ésta comunicación, y dentro del plazo establecido en este apartado, deberá reparar o reemplazar los bienes defectuosos, o sus partes sin ningún costo para la contratante.

2. Si el proveedor después de haber sido notificado, no cumple dentro del plazo establecido, la contratante, procederá a tomar medidas necesarias para remediar la situación, por cuenta y riesgo del proveedor y sin perjuicio de otros derechos que la contratante pueda ejercer contra el proveedor en virtud del contrato.

Cobertura de Seguro de los bienes

La cobertura de seguro requerida a los bienes será:

No Aplica

A menos que se disponga otra cosa en este apartado, los bienes suministrados deberán estar completamente asegurados en guaraníes, contra riesgo de extravío o daños incidentales ocurridos durante la fabricación, adquisición, transporte, almacenamiento y entrega, de acuerdo a los incoterms aplicables.

Sistema de presentación de ofertas

El Sistema de presentación de ofertas para esta licitación será:

Un sobre

Los sobres deberán:

1. Indicar el nombre y la dirección del oferente;
2. Estar dirigidos a la convocante;
3. Llevar la identificación específica del proceso de licitación indicado en el SICP; y
4. Llevar una advertencia de no abrir antes de la hora y fecha de apertura de ofertas.
5. Identificar si se trata de un sobre técnico o económico.

Si los sobres no están cerrados e identificados como se requiere, la Convocante no se responsabilizará en caso de que la oferta se extravíe o sea abierta prematuramente.

Plazo para presentar las ofertas

Las ofertas deberán ser recibidas por la Convocante en la dirección y hasta la fecha y hora que se indican en el SICP.

La Convocante podrá a su discreción, extender el plazo originalmente establecido para la presentación de ofertas mediante una adenda. En este caso todos los derechos y obligaciones de la convocante y de los oferentes previamente sujetos a la fecha límite original para presentar las ofertas quedarán sujetos a la nueva fecha prorrogada.

Cuando la presentación de la oferta sea electrónica deberá sujetarse a la reglamentación vigente.

Retiro, sustitución y modificación de las ofertas

1. Un oferente podrá retirar, sustituir o modificar su oferta después de presentada mediante el envío de una comunicación por escrito, debidamente firmada por el representante autorizado. La sustitución o modificación correspondiente de la oferta deberá acompañar dicha comunicación por escrito.

2. Todas las comunicaciones deberán ser:

a) Presentadas conforme a la forma de presentación e identificación de las ofertas y además los respectivos sobres deberán estar marcados "RETIRO", "SUSTITUCION" o "MODIFICACION";

b) Recibidas por la convocante antes del plazo límite establecido para la presentación de las ofertas;

Las ofertas cuyo retiro, sustitución o modificación fuere solicitada serán devueltas sin abrir a los oferentes remitentes, durante el acto de apertura de ofertas.

3. Ninguna oferta podrá ser retirada, sustituida o modificada durante el intervalo comprendido entre la fecha límite para presentar ofertas y la expiración del período de validez de las ofertas indicado en el Formulario de Oferta, o cualquier extensión si la hubiere, caso contrario, se hará efectiva la Garantía de Mantenimiento de Oferta.

Apertura de ofertas

1. La Convocante abrirá las ofertas y en caso de que hubiere notificaciones de retiro, sustitución y modificación de ofertas presentadas, las leerá en el acto público con la presencia de los oferentes o sus representantes a la hora, en la fecha y el lugar establecidos en el SICP.

2. Cuando la presentación de oferta sea electrónica, el acto de apertura deberá sujetarse a la reglamentación vigente, en la fecha, hora y lugar establecidos en el SICP.

3. Primero se procederá a verificar de entre las ofertas recibidas por courier o entregadas personalmente, los sobres marcados como:

a) "RETIRO". Se leerán en voz alta y el sobre con la oferta correspondiente no será abierto sino devuelto al Oferente remitente. No se permitirá el retiro de ninguna oferta a menos que la comunicación de retiro pertinente contenga la autorización válida para solicitar el retiro y sea leída en voz alta en el acto de apertura de las ofertas.

b) "SUSTITUCION" se leerán en voz alta y se intercambiará con la oferta correspondiente que está siendo sustituida; la oferta sustituida no se abrirá y se devolverá al Oferente remitente. No se permitirá ninguna sustitución a menos que la comunicación de sustitución correspondiente contenga una autorización válida para solicitar la sustitución y sea leída en voz alta en el acto de apertura de las ofertas.

c) "MODIFICACION" se abrirán y leerán en voz alta con la oferta correspondiente. No se permitirá ninguna modificación a las ofertas a menos que la comunicación de modificación correspondiente contenga la autorización válida para solicitar la modificación y sea leída en voz alta en el acto de apertura de las ofertas. Solamente se considerarán en la evaluación los sobres que se abren y leen en voz alta durante el Acto de Apertura de las Ofertas.

4. Los representantes de los oferentes que participen en la apertura de las ofertas deberán contar con autorización suficiente para suscribir el acta y los documentos que soliciten, bastando para ello la presentación de una autorización escrita del firmante de la oferta, esta autorización podrá ser incluida en el sobre oferta o ser portado por el representante.

5. Se solicitará a los representantes de los oferentes que estén presentes que firmen el acta. La omisión de la firma por parte de un Oferente no invalidará el contenido y efecto del acta. Se distribuirá una copia del acta a todos los presentes.

6. Las ofertas sustituidas y modificadas presentadas, que no sean abiertas y leídas en voz alta durante el acto de apertura no podrán ser consideradas para la evaluación sin importar las circunstancias y serán devueltas sin abrir a los oferentes remitentes.

7. La falta de firma en un documento sustancial, es considerada una omisión sustancial que no podrá ser subsanada en ninguna oportunidad una vez abiertas las ofertas.

8. En el sistema de un solo sobre el acta de apertura deberá ser comunicada al Sistema de Información de Contrataciones Públicas para su difusión, dentro de los dos (02) días hábiles de la realización del acto de apertura.

9. En el sistema de doble sobre, el acta de apertura técnica deberá ser comunicada al SICP, para su difusión, dentro de los dos (02) días hábiles de la realización del acto de apertura, se procederá de igual manera una vez finalizado el acto de apertura económico.

REQUISITOS DE CALIFICACIÓN Y CRITERIOS DE EVALUACIÓN

Esta sección contiene los criterios que la convocante utilizará para evaluar la oferta y determinar si un oferente cuenta con las calificaciones requeridas. Ningún otro factor, método o criterio será utilizado.

Condición de Participación

Podrán participar de ésta licitación, individualmente o en forma conjunta (consorcio), los oferentes domiciliados en la República del Paraguay, que no se encuentren comprendidos en las prohibiciones o limitaciones para presentar propuestas y contratar con el Estado, establecidas en la Ley N° 2051/03 "De Contrataciones Públicas".

Requisitos de Calificación

Capacidad Legal

Los oferentes deberán declarar que no se encuentran comprendidos en las limitaciones o prohibiciones para contratar con el Estado, contempladas en el artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, declaración que forma parte del formulario de oferta.

Serán desechadas las ofertas de los oferentes que se encuentren comprendidos en las prohibiciones o limitaciones para contratar a la hora y fecha límite de presentación de ofertas o a la fecha de firma del contrato.

A los efectos de la verificación de la existencia de prohibiciones o limitaciones contenidas en los incisos a) y b), m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, el comité de evaluación realizará el siguiente análisis:

1. Verificará que el oferente haya proporcionado el formulario de ofertas que incluye la declaratoria debidamente firmada.
2. Verificará los registros del personal de la convocante para detectar si el oferente o sus representantes, se hallan comprendidos en el presupuesto del inciso a) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021.
3. Verificará por los medios disponibles, si el oferente y los demás sujetos individualizados en las prohibiciones o limitaciones contenidas en los incisos a) y b), m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, aparecen en la base de datos del SINARH o de la Secretaría de la Función Pública.
4. Si se constata que alguno de las personas mencionadas en el párrafo anterior figura en la base de datos del SINARH o de la Secretaría de la Función Pública, el comité analizará acabadamente si tal situación le impedirá ejecutar el contrato, exponiendo los motivos para aceptar o rechazar la oferta, según sea el caso.
5. Verificará que el oferente haya proporcionado el formulario de Declaración de Miembros, de conformidad a estándar debidamente firmado en su oferta y cotejará los datos con las personas físicas inhabilitadas que constan en el registro de "Sanciones a Proveedores" del SICP a fin de detectar si directores, gerentes, socios gerentes, quienes ejerzan la administración, accionistas, cuotapartistas o propietarios se hallan comprendidos en el presupuesto del inciso m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021.

El comité podrá recurrir a fuentes públicas o privadas de información, para verificar los datos proporcionados por el oferente.

6. Si el Comité confirma que el oferente o sus integrantes poseen impedimentos, la oferta será rechazada y se remitirán los antecedentes a la Dirección Nacional de Contrataciones Públicas (DNCP) para los fines pertinentes.

Análisis de precios ofertados

Durante la evaluación de ofertas, luego de haber realizado la corrección de errores aritméticos y de ordenar las ofertas presentadas de menor a mayor, el Comité de Evaluación procederá a solicitar a los oferentes una explicación detallada de la composición del precio ofertado de cada ítem, rubro o partida adjudicable, conforme a los siguientes parámetros:

1. En contrataciones en general: cuando la diferencia entre el precio ofertado y el precio referencial sea superior al 25% para ofertas por debajo del precio referencial y del 15% para ofertas que se encuentren por encima del referencial establecido por la convocante y difundido con el llamado a contratación.

Si el oferente no respondiese la solicitud, o la respuesta no sea suficiente para justificar el precio ofertado del bien o servicio, el precio será declarado inaceptable y la oferta rechazada.

El análisis de los precios, con esta metodología, será aplicado a cada ítem, rubro o partida que componga la oferta y en cada caso deberá ser debidamente fundada la decisión adoptada por la Convocante en el ejercicio de su facultad discrecional.

Certificado de Producto y Empleo Nacional - CPS

A los efectos de acogerse al beneficio de la aplicación del margen de preferencia, el oferente deberá contar con el Certificado de Producto y Empleo Nacional (CPEN). El certificado debe ser emitido como máximo a la fecha y hora tope de presentación de ofertas.

La falta del CPEN no será motivo de descalificación de la oferta, sin embargo, el oferente no podrá acogerse al beneficio.

El comité de evaluación verificará en el portal oficial indicado por el Ministerio de Industria y Comercio (MIC) la emisión en tiempo y forma del CPEN declarado por los oferentes. No será necesaria la presentación física del Certificado de Producto y Empleo Nacional.

Independientemente al sistema de adjudicación, el margen de preferencia será aplicado a cada bien o servicio objeto de contratación que se encuentre indicado en la planilla de precios.

a) Consorcios:

a.1. Provisión de Bienes

El CPEN debe ser expedido a nombre del oferente que fabrique o produzca los bienes objeto de la contratación. En el caso que ninguno de los oferentes consorciados fabrique o produzca los bienes ofrecidos, el consorcio deberá contar con el CPEN correspondiente al bien ofertado, debiendo encontrarse debidamente autorizado por el fabricante. Esta autorización podrá ser emitida a nombre del consorcio o de cualquiera de los integrantes del mismo.

a.2. Provisión de Servicios (se entenderá por el término servicio aquello que comprende a los servicios en general, las consultorías, obras públicas y servicios relacionados a obras públicas).

Todos los integrantes del consorcio deben contar con el CPEN.

Excepcionalmente se admitirá que no todos los integrantes del consorcio cuenten con el CPEN para aplicar el margen de preferencia, cuando el servicio específico se encuentre detallado en uno de los ítems de la planilla de precios, y de los documentos del consorcio (acuerdo de intención o consorcio constituido) se desprenda que el integrante del consorcio que cuenta con el CPEN será el responsable de ejecutar el servicio licitado.

Margen de preferencia local - CPS

Para contrataciones realizadas por Unidades Operativas que se encuentren conformadas dentro de un municipio o departamento se deberá considerar que, si la oferta evaluada como la más baja pertenece a una firma u empresa domiciliada fuera del territorio departamental de la convocante, ésta será comparada con la oferta más baja de la firma u empresa domiciliada dentro del territorio de la convocante, agregándole al precio total de la oferta propuesta por la primera una suma del diez por ciento (10%) del precio. Si en dicha comparación adicional la oferta de la firma u empresa domiciliada dentro del territorio departamental de la convocante resultare ser la más baja, se la seleccionará para la adjudicación; en caso contrario se seleccionará la oferta de servicios de la firma u empresa domiciliada fuera del territorio departamental de la convocante.

En el caso de que el oferente, sea de la zona y además cuente con margen de preferencia, se le aplicará únicamente el margen de este último.

Las convocatorias deberán acogerse a las condiciones específicas para la aplicación del Margen de Preferencia Local establecidas en la reglamentación emitida por la DNCP.

Requisitos documentales para evaluación de las condiciones de participación

1. Formulario de Oferta (*)

[El formulario de oferta y lista de precios, generados electrónicamente a través del SICP, deben ser completados y firmados por el oferente.]

Dichos documentos completados y firmados además de formar parte de la oferta ingresada en el módulo de ofertas electrónicas del SICP a más tardar en la fecha y hora establecida al efecto en el SICP, deberán ser remitidos posteriormente en formato físico en el lugar y fecha y hora máxima establecidos en el SICP, conforme a lo establecido en la Resolución DNCP N° 1930/2020 Por la cual se dispone la utilización del Sistema de Información de Contrataciones Públicas para la presentación y apertura de ofertas electrónicas en los procedimientos de contratación.

2. Garantía de Mantenimiento de Oferta (*)

La garantía de mantenimiento de oferta debe ser extendida, bajo la forma de una garantía bancaria o póliza de seguro de caución.

Dicho documento además de formar parte de la oferta ingresada en el módulo de ofertas electrónicas del SICP a más tardar en la fecha y hora establecida al efecto en el SICP, deberá ser remitido posteriormente en formato físico en el lugar y fecha y hora máxima establecidos en el SICP, conforme a lo establecido en la Resolución DNCP N° 1930/2020 Por la cual se dispone la utilización del Sistema de Información de Contrataciones Públicas para la presentación y apertura de ofertas electrónicas en los procedimientos de contratación.

3. Fotocopia simple de Certificado de Cumplimiento con la Seguridad Social. (**)

4. Fotocopia simple de Certificado de Producto y Empleo Nacional, emitido por el MIC, en caso de contar. (**)

5. Certificado de Cumplimiento Tributario. (**)

6. Patente comercial del municipio en donde esté asentado el establecimiento principal del oferente. (**)

7. Declaración Jurada de Aceptación de Uso de Oferta Electrónica, en virtud de la cual el Oferente acepta todas las obligaciones a partir del uso del módulo habilitado para la presentación y apertura de la oferta electrónica, en los términos de la Resolución DNCP N° 1930/2020 Por la cual se dispone la utilización del Sistema de Información de Contrataciones Públicas para la presentación y apertura de ofertas electrónicas en los procedimientos de contratación. A tales efectos, el oferente deberá proceder a descargar la proforma de la Declaración Jurada que se encuentra en la sección Formularios del SICP (www.contrataciones.gov.py/dncp/sipe.html#formularios), de conformidad a las disposiciones contenidas en las Guías de Presentación y Apertura de Ofertas Electrónicas, debiendo estar debidamente cargada y en estado ACTIVO en el SIPE al momento de la carga de la oferta electrónica. (**)

8. Declaración Jurada de Declaración de Miembros, de conformidad con el formulario estándar N° 5 Sección Formularios (**)

9. Documentos legales

9.1. Oferentes Individuales. Personas Físicas.

a. Fotocopia simple de la Cédula de Identidad del firmante de la oferta (*).

b. Fotocopia simple de Constancia de inscripción en el Registro Único de Contribuyentes RUC(**).

c. En el caso que suscriba la oferta otra persona en su representación, deberá acompañar una fotocopia simple de su cédula de identidad y una fotocopia simple del poder suficiente otorgado por Escritura Pública para presentar la oferta y representarlo en los actos de la licitación. No es necesario que el poder esté inscripto en el Registro de Poderes (*).

9.2. Oferentes Individuales. Personas Jurídicas.

a. Fotocopia simple de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos (*).

b. Fotocopia simple de la Constancia de inscripción en el Registro Único de Contribuyentes. (**)

c. Fotocopia simple de los documentos de identidad de los representantes o apoderados de la sociedad. (**)

d. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al oferente. Estos documentos pueden consistir en: un poder suficiente otorgado por Escritura Pública (no es necesario que esté inscripto en el Registro de Poderes); o los documentos societarios que justifiquen la representación del firmante, tales como las actas de asamblea y de directorio en el caso de las sociedades anónimas (*).

9.3. Oferentes en Consorcio.

a. Cada integrante del consorcio que sea una persona física domiciliada en la República del Paraguay deberá presentar los documentos requeridos para Oferentes Individuales especificados en el apartado Oferentes Individuales Personas Físicas, de acuerdo a lo indicado para cada documento. Cada integrante del consorcio que sea una persona jurídica domiciliada en Paraguay deberá presentar los documentos requeridos para Oferentes Individuales Personas Jurídicas, de acuerdo a lo indicado para cada documento.

b. Original o fotocopia simple del consorcio constituido o del acuerdo de intención de constituir el consorcio por escritura pública en caso de resultar adjudicados y antes de la firma del contrato. El acuerdo de intención deberá hallarse instrumentado, como mínimo en un documento privado con certificación de firmas por Escribano Público. El consorcio constituido deberá estar formalizado por Escritura Pública (*).

c. Fotocopia simple de los documentos que acrediten las facultades de los firmantes del acuerdo de intención de consorciarse. (*)

Estos documentos pueden consistir en:

- i. Un poder suficiente otorgado por escritura pública por cada miembro del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o
- ii. Los documentos societarios de cada miembro del consorcio, que justifiquen la representación del firmante, tales como actas de asamblea y de directorio en el caso de las sociedades anónimas.

d. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al consorcio, cuando se haya formalizado el consorcio. (*)

Estos documentos pueden consistir en:

- i. Un poder suficiente otorgado por escritura pública por la Empresa Líder del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o
- ii. Los documentos societarios de la Empresa Líder, que justifiquen la representación del firmante, tales como actas de asamblea y de directorio en el caso de las sociedades anónimas.

Los documentos indicados con asterisco (*) son considerados documentos sustanciales a ser presentados con la oferta.

Los documentos indicados con doble asterisco (**) deberán estar vigentes a la fecha y hora tope de presentación de ofertas.

Capacidad Financiera

Con el objetivo de calificar la situación financiera del oferente, se considerarán los siguientes índices:

a) Para contribuyentes de IRACIS:

Deberán cumplir con los siguientes parámetros respecto a los ejercicios fiscales 2019, 2020 y 2021:

a. **Ratio de Liquidez:** activo corriente / pasivo corriente

Deberá ser igual o mayor que 1, en promedio, en los años citados.

b. Endeudamiento: pasivo total / activo total

No deberá ser mayor a 0,80 en promedio, en los años citados.

c. Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital.

El promedio en los años citados no deberá ser negativo.

b) Para contribuyentes de IRPC:

Deberán cumplir el siguiente parámetro respecto a los ejercicios fiscales 2019, 2020 y 2021:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales citados.

c) Para contribuyentes de IRP:

Deberán cumplir el siguiente parámetro respecto a los ejercicios fiscales 2019, 2020 y 2021:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales citados.

d) Para contribuyentes de exclusivamente IVA General:

Deberán cumplir el siguiente parámetro respecto a los últimos 12 (doce) meses (contados desde el mes anterior a la fecha de apertura de ofertas):

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los meses citados.

Para la evaluación de la situación financiera de los Consorcios, se evaluará a todos los integrantes del mismo debiendo cumplir cada uno de ellos los requisitos exigidos de capacidad en forma individual.

Requisitos documentales para la evaluación de la capacidad financiera

a. Balance General y Cuadro de Estado de Resultados de los años 2019, 2020 y 2021 para contribuyentes de IRACIS.

b. IVA General de los últimos 12 meses (contados desde el mes anterior a la fecha de apertura de ofertas), para contribuyentes sólo del IVA General.

c. Formulario 106 de los años 2019, 2020 y 2021 para contribuyentes del IRPC.

d. Formulario 104 de los años 2019, 2020 y 2021 para contribuyentes de Renta Personal.

Experiencia requerida

Con el objetivo de calificar la experiencia del oferente, se considerarán los siguientes índices:

- Demostrar una antigüedad mínima de 5 (cinco) años de existencia legal (inclusive para las firmas unipersonales).
- Demostrar la experiencia en la prestación de servicios de ciberseguridad y/o servicios relacionados a la provisión e instalación de soluciones de ciberseguridad con contrato/s ejecutado/s, y/o facturas, y/o recepciones finales por un monto equivalente al 30 % como mínimo del monto total del/los lote/s ofertado/s en la presente licitación, de los años: 2018 a 2022.

En caso de Consorcios el Socio Líder deberá cumplir con el requisito establecido en los inc. a) y c), así como el 60% del requisito mínimo establecido en el inc. b). Los Socios restantes combinados deben cumplir con el 40% del requisito mínimo establecido en el inc. b).

Requisitos documentales para la evaluación de la experiencia

a. Fotocopia simple de Estatuto de Constitución y/o Constancia de RUC que demuestren una antigüedad mínima de 5 (cinco) años de existencia legal (inclusive para las firmas unipersonales).

b. Fotocopia/s simple/s de contrato/s ejecutado/s, y/o facturas, y/o recepciones finales de haber prestado servicios de ciberseguridad y/o servicios relacionados a la provisión e instalación de soluciones de ciberseguridad, a Instituciones Públicas y/o Privadas, en el periodo comprendido entre los años 2018 a 2022, cuyos montos sumados representen un monto igual o superior al 30% del monto total del/los lote/s ofertado/s en la presente licitación. Podrán presentarse la cantidad de fotocopia/s de contrato/s ejecutado/s, y/o factura/s, y/o recepciones finales que fueren necesarias para acreditar el monto solicitado, siempre y cuando dichas provisiones hayan sido realizadas dentro del periodo mencionado.

c. Fotocopia simple de referencias satisfactorias de clientes finales, como mínimo 1 (uno), formalizadas por documentos que contengan la debida identificación y suscripción del emisor, de haber prestado servicios de ciberseguridad y/o servicios relacionados a la provisión e instalación de soluciones de ciberseguridad, en el periodo comprendido entre los años 2018 al 2022, expedidas por Instituciones Públicas y/o Privadas con quienes mantiene y/o mantuvo relaciones comerciales.

Capacidad Técnica

El Oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de capacidad técnica:

Los requisitos de capacidad técnica a ser evaluados se detallan en el siguiente punto:

Requisito documental para evaluar la capacidad técnica

- a. Para los Lotes N° 5 y 7: Catálogos o impresos descriptivos de las soluciones ofertadas, incluyendo el modelo exacto a ser ofertado con los vínculos (links/URL) oficiales del fabricante, en los cuales se puedan corroborar las especificaciones técnicas de éstas.
- b. Nota en carácter de declaración jurada en la cual el Oferente manifieste que cuenta con el personal técnico capacitado a efectos de la instalación, configuración, implementación y mantenimiento de las soluciones objeto del servicios y para la ejecución de los servicios ofertados, asumiendo la responsabilidad por los trabajos del personal técnico asignado, los equipos y las tareas realizadas comprendidas en las especificaciones técnicas.
- c. Para el Lote N° 1, Ítem N° 2: Curriculum vitae actualizado del personal técnico responsable del Oferente, correspondiente al equipo técnico, al menos 5 (cinco) analistas de seguridad, en el cual se acrediten los requisitos indicados en el apartado N° 1.2.1.6 con el cual satisfarán los requerimientos de los servicios. El BCP se reserva el derecho a verificar la información y para el efecto se deberá incluir un contacto telefónico y correo electrónico. Asimismo, se deberá presentar fotocopia simple de los documentos que acrediten la formación técnica, profesional y la experiencia laboral de los mismos.
- d. Para los Lote N° 5 y 7: Fotocopia simple del documento que acredite que el personal técnico responsable del Oferente, al menos 1 (uno), cuenta con certificación vigente del fabricante de la solución a ser utilizada en el marco del servicio.
- e. Nota en carácter de declaración jurada en la cual se detallen las especificaciones técnicas de las soluciones y servicios ofertados para cada lote, con la inclusión de las descripciones y demás requisitos exigidos en la Sección Especificaciones Técnicas y Suministros Requeridos.
- f. Garantía de Buen Servicio y Calidad, mediante una nota en carácter de declaración jurada a nombre de la Convocante, en virtud de la cual el Oferente manifieste que correrán a su cargo, por cuenta propia y sin costo para el BCP, las reposiciones, sustituciones, reparaciones y/o modificaciones que correspondan, cuando se observasen fallas y/o deficiencias en los servicios ofertados, por causas que le fueran imputables, a partir de la fecha de emisión de la conformidad del área técnica (Departamento de Ciberseguridad) y durante el plazo establecido para el servicio de cada lote ofertado en el apartado Especificaciones Técnicas de la Sección Suministros Requeridos especificaciones técnicas del PBC
- g. Para el Lote N° 1, Ítem 2: Nota en carácter de Declaración jurada, por la cual el Oferente manifieste que se compromete a brindar el soporte, actualización y garantía del fabricante por 24 meses contados a partir de la conformidad por los servicios, otorgada por el Departamento de Ciberseguridad

h. **Para los Lotes N° 2, 3, 4, 5, y 7:** Nota en carácter de Declaración jurada, por la cual el Oferente manifieste que se compromete a brindar el soporte, actualización y garantía del fabricante por 24 meses contados a partir de la conformidad por el servicio, otorgada por el Departamento de Ciberseguridad.

i. **Para el Lote 6:** Nota en carácter de Declaración jurada, por la cual el Oferente manifieste que se compromete a brindar el soporte, actualización y garantía del fabricante por 12 meses contados a partir de la conformidad por el servicio, otorgada por el Departamento de Ciberseguridad.

j. Documento vigente que acredite fehacientemente que el Oferente es Fabricante y/o Representante Oficial y/o Distribuidor Oficial y/o Partner Autorizado por el Fabricante para el Paraguay de la solución a ser utilizada en el marco del servicio, ya sea mediante documento emitido por la firma autorizante o mediante la presentación del Formulario correspondiente incluido en la Sección Formularios debidamente suscripto por la firma autorizante.

Otros criterios que la convocante requiera

Otros criterios para la evaluación de las ofertas a ser considerados en ésta contratación serán:

a. El BCP se reserva el derecho de solicitar a los oferentes que cumplan con los documentos sustanciales una demostración de las funcionalidades de los softwares ofrecidos para realizar los servicios, si así lo considerase necesario, con el fin de verificar el cumplimiento de los requerimientos establecidos en el cuadro de Especificaciones Técnicas obrante en la Sección Especificaciones Técnicas y Suministros Requeridos. Dicha demostración para la evaluación de ofertas podrá realizarse a elección del BCP en forma remota o presencial en el BCP (Av. Federación Rusa y Augusto Roa Bastos), en la fecha y hora a ser comunicada por escrito, con la presencia de los funcionarios designados por el Departamento de Ciberseguridad.

b. La convocante se reserva el derecho a requerir la información y/o documentación adicional que estime pertinente a fin de acreditar la veracidad de la información contenida en la documentación presentada por el oferente referente a los requisitos documentales para la evaluación citados más arriba.

Criterios de desempate de ofertas

En caso de que existan dos o más oferentes solventes que cumplan con todos los requisitos establecidos en el pliego de bases y condiciones del llamado, igualen en precio y sean sus ofertas las más bajas, el comité de evaluación determinará cuál de ellas es la mejor calificada para ejecutar el contrato utilizando los criterios dispuestos para el efecto por la DNCP en la reglamentación pertinente.

Nota1: Conforme a lo previsto en el Decreto reglamentario de la Ley de Contrataciones los adjudicatarios de los contratos resultantes de los procesos licitatorios, deberán inscribirse en el Sistema de Información de Proveedores del Estado - SIPE, como requisito previo a la emisión del Código de Contratación respectivo, no siendo la inscripción una exigencia para participar en el proceso tradicional.

SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS

Esta sección constituye el detalle de los bienes con sus respectivas especificaciones técnicas - EETT, de manera clara y precisa para que el oferente elabore su oferta. Salvo aquellas EETT de productos ya determinados por plantillas aprobadas por la DNCP.

Suministros y Especificaciones técnicas

El Suministro deberá incluir todos aquellos ítems que no hubiesen sido expresamente indicados en la presente sección, pero que pueda inferirse razonablemente que son necesarios para satisfacer el requisito de suministro indicado, por lo tanto, dichos bienes y servicios serán suministrados por el Proveedor como si hubiesen sido expresamente mencionados, salvo disposición contraria en el Contrato.

Los bienes y servicios suministrados deberán ajustarse a las especificaciones técnicas y las normas estipuladas en este apartado. En caso de que no se haga referencia a una norma aplicable, la norma será aquella que resulte equivalente o superior a las normas oficiales de la República del Paraguay. Cualquier cambio de dichos códigos o normas durante la ejecución del contrato se aplicará solamente con la aprobación de la contratante y dicho cambio se registrará de conformidad a la cláusula de adendas y cambios.

El Proveedor tendrá derecho a rehusar responsabilidad por cualquier diseño, dato, plano, especificación u otro documento, o por cualquier modificación proporcionada o diseñada por o en nombre de la Contratante, mediante notificación a la misma de dicho rechazo.

Detalles de los productos y/ servicios con las respectivas especificaciones técnicas - CPS

Los productos y/o servicios a ser requeridos cuentan con las siguientes especificaciones técnicas:

GENERALIDADES:

■ MÓDULO DE OFERTAS ELECTRÓNICAS:

De acuerdo a lo establecido en la Res. DNCP N° 1930/20 Por la cual se dispone la utilización del Sistema de Información de Contrataciones Públicas para la presentación y apertura de ofertas electrónicas en los procedimientos de contratación:

- El oferente que participe en el presente procedimiento de contratación deberá contar, como condición previa, con un usuario activo en el Sistema de Información de Proveedores del Estado (SIPE) para acceder al módulo de oferta electrónica a efectos de la presentación y apertura de ofertas.
- Presentación de ofertas electrónicas: la oferta deberá ser presentada a través del módulo de ofertas electrónicas del SICP a más tardar en el día y hora señalados al efecto en el SICP. Asimismo, podrá ser modificada y retirada hasta antes del día y hora previstos para la presentación de ofertas y realización del acto de apertura, según corresponda en cada caso de acuerdo a las disposiciones legales.
- Carga de Ofertas electrónicas: ingresando al módulo habilitado en el SICP, a través de su usuario y contraseña, el oferente generará su oferta. En ella cargará todos los documentos requeridos en el presente pliego de bases y condiciones, los cuales deberán ser incorporados electrónicamente y estar debidamente firmados, según corresponda.
- Remisión de documentos en formato físico: A los efectos de la verificación y validación de la documentación que integra las ofertas electrónicas recibidas, se establecerá en el SICP lugar, fecha y hora límites para que el oferente remita en sobre cerrado: el Formulario de Oferta, la Lista de Precios y la Garantía de Mantenimiento de oferta

originales en formato físico. El plazo establecido por la Convocante en el SICP no podrá ser superior a dos días hábiles posteriores a la fecha prevista para el acto de apertura. La falta de presentación de la documentación física en el lapso señalado será motivo de rechazo de la oferta electrónica y la conducta del oferente será analizada conforme a lo establecido en el título séptimo De las Infracciones y Sanciones de la Ley 2051/2003. La presentación física del Formulario de Oferta, de la Lista de Precios y de la Garantía de Mantenimiento de Oferta no será requerida cuando los documentos hayan sido suscritos digitalmente en las condiciones y términos previstos por la Ley N° 4017/2010 "De validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico". En los casos en que la Garantía de Mantenimiento de Oferta fuera instrumentada mediante una póliza de seguros digital, la presentación física no será requerida si el documento cumple con los requerimientos y condiciones exigidas por la Superintendencia de Seguros del Banco Central del Paraguay.

• **PORCENTAJE DE LA GARANTÍA DE MANTENIMIENTO DE OFERTA**

El porcentaje indicado en el SICP para la Garantía de Mantenimiento de Oferta es del 5% cinco por ciento.

■ **ADENDAS AL PBC:**

La adenda es el documento emitido por la convocante, mediante la cual se modifican aspectos establecidos en la convocatoria y/o en las bases de la licitación. La adenda será considerada parte integrante del documento cuyo contenido modifique.

La convocante podrá introducir modificaciones o enmiendas a los pliegos de bases y condiciones, siempre y cuando se ajuste a los parámetros establecidos en la Ley.

La convocante podrá prorrogar el plazo de presentación de ofertas a fin de dar a los posibles oferentes, un plazo razonable para que puedan tomar en cuenta la enmienda en la preparación de sus ofertas. Esta prórroga deberá quedar asentada en la adenda citada.

■ **RESPONSABILIDADES GENERALES DEL PROVEEDOR:**

1. El Proveedor deberá suministrar todos los bienes o servicios de acuerdo con las condiciones establecidas en el pliego de bases y condiciones y sus adendas, así como en el Contrato y sus adendas.
2. El Proveedor será responsable de cualquier indemnización por daños causados en el marco de la ejecución del contrato por él o su personal a los funcionarios y/o a terceros, y/o a los bienes de éstos, y/o a los bienes o instalaciones o imagen reputacional de la Contratante; por causas imputables al mismo.
3. Responder por todo incumplimiento o consecuencia imputable al mismo, derivados de la incorrecta o incompleta ejecución de lo contratado.
4. Contratar y mantener el personal calificado necesario para la realización de los servicios requeridos. Cumplir con todas las leyes laborales y de Seguridad Social vigentes. Asumir todos los riesgos en los términos del Código del Trabajo vigente, liberando al BCP de cualquier responsabilidad al respecto.
5. Cumplir con todas las medidas de seguridad que se requieran respecto a su personal, a fin de evitar accidentes de trabajo durante la ejecución contractual.
6. El Proveedor deberá indemnizar y eximir de cualquier responsabilidad a la contratante y a sus empleados y funcionarios, por cualquier litigio, acción legal o procedimiento administrativo, reclamación, demanda, pérdida, daño, costo y gasto cualquiera sea su naturaleza, incluidos los honorarios y gastos de representación legal, en los cuales pueda incurrir la contratante como resultado de riesgos profesionales o muerte de los empleados del Proveedor, sea reclamado por el trabajador o sus causahabientes durante la vigencia del contrato. Como riesgos profesionales se entenderán los accidentes de trabajo y enfermedades profesionales. Se considerarán igualmente accidentes del trabajo los hechos constituidos por caso fortuito o fuerza mayor inherentes al trabajo que produzcan las mismas lesiones.

■ **CONFIDENCIALIDAD DE LA INFORMACIÓN**

De acuerdo a lo indicado en la Sección Especificaciones técnicas y Suministros Requeridos, el personal del Proveedor deberá firmar un Compromiso de Confidencialidad de la Información en los términos del Formulario de la Sección Formularios Adicionales.

MODALIDAD DE CONTRATACIÓN

Contrato Cerrado.

- LOTE N° 1 SERVICIOS SOC Y MESA DE AYUDA DE CIBERSEGURIDAD.
- LOTE N° 2 - SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE SEGURIDAD DNS.
- LOTE N° 3 - SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE SEGURIDAD PERIMETRAL DEFINIDA POR SOFTWARE.
- LOTE N° 4 SERVICIO DE SUSCRIPCIÓN A SOLUCIONES DE CIBERSEGURIDAD.

- LOTE N° 5 - SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE DETECCIÓN Y RESPUESTA EXTENDIDA XDR.
- LOTE N° 6 SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN FIREWALL DE APLICACIÓN WEB (WAF).
- LOTE N° 7 SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE DETECCIÓN Y RESPUESTA PARA NETWORKING NDR.

ESPECIFICACIONES TÉCNICAS

ESPECIFICACIONES TÉCNICAS			
Requisito	Detalle y definiciones	REQUERIDO	OFRECIDO
LOTE N° 1 SERVICIOS SOC Y MESA DE AYUDA DE CIBERSEGURIDAD			
ITEM N° 1 - Servicio Security Operations Center (SOC)			
1.1.1 Generalidades del Servicio			
1.1.1.1	Se solicita el servicio SOC (Security Operations Center) tercerizado implementado actualmente en el BCP (Digiware), por un plazo de 24 meses computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato, con las mismas condiciones en las que se tiene contratado el servicio.	EXIGIDO	
ITEM N° 2 - Servicio de Mesa de Ayuda y Gestión de Incidentes de Ciberseguridad			
1.2.1 Generalidades del servicio			
1.2.1.1	Se solicita el servicio de suscripción a la herramienta Invgate Service Desk implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha a ser establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.	EXIGIDO	
1.2.1.2	Se deben incluir todas las licencias necesarias para al menos 20 agentes, sin limitaciones de usuarios clientes y capacidad de almacenamiento de por lo menos 100 GB.	EXIGIDO	
1.2.1.3	El servicio debe incluir la provisión de un equipo de trabajo dedicado, compuesto como mínimo por 5 (cinco) técnicos, quienes realizarán las siguientes tareas: la gestión de incidentes de ciberseguridad, la operativa y administración de las herramientas de ciberseguridad del BCP y la gestión de la mesa de servicios implementada, con exclusividad absoluta para el BCP, hasta 40 horas semanales por cada técnico ya sea en modalidad onsite o remoto.	EXIGIDO	

1.2.1.4	El servicio técnico contempla: Monitoreo de las alarmas de seguridad, revisión de alarmas y eventos de seguridad; análisis, evaluación y contención de primera línea de incidentes de seguridad; configuración de herramientas de seguridad, tales como firewalls, IPS, DLP, Antivirus, SIEM, Antispam, entre otros; configuración de reglas de correlación; configuración de las plataformas de mesa de servicios de seguridad; revisión técnica, auditoría de registros, test de seguridad e investigación y análisis forense de primer nivel; asistencia a usuarios finales para la resolución de casos; colaboración con el soporte externo de ciberseguridad.	EXIGIDO	
1.2.1.5	Lugar de la prestación del servicio: On-Site (Oficinas del BCP) y/o Remoto, a definir con la contraparte del BCP. Horario de la prestación del servicio: On-Site en horario de 06:00 a 22:00, de lunes a viernes; Remoto disponible 24 horas, 7 días a la semana; horario a convenir con la contraparte del BCP.	EXIGIDO	
1.2.1.6	<p>Perfil requerido del personal: Entre 23 y 35 años. Estudiante y/o egresado de carreras de Informática. Debe poseer conocimientos sólidos en ciberseguridad, redes y gestión de incidentes, acreditable con por lo menos 40 horas de formación específica en ciberseguridad, a través de cursos o certificaciones sobre: administración y operación de herramientas de seguridad, test de intrusión, seguridad en redes e infraestructura tecnológica, entre otros.</p> <p>Experiencia laboral, al menos 1 (una) referencia certificada, acreditable con la presentación de la fotocopia simple de la referencia comprobable de los trabajos realizados que guarden relación con servicios de informática y/o ciberseguridad.</p> <p>El personal técnico que ejecutará el contrato deberá ser el designado por parte del Proveedor en su oferta.</p>	EXIGIDO	
1.2.1.7	Herramientas de trabajo: El BCP proveerá el equipamiento y el espacio adecuados cuando el servicio sea realizado en sus oficinas. El oferente deberá proveer de todas las herramientas cuando el servicio sea realizado de manera remota, de conformidad con los requerimientos técnicos y de seguridad del BCP.	EXIGIDO	
1.2.1.8	La asistencia del equipo técnico en ningún caso representa compromiso laboral alguno entre los individuos y el BCP, siendo el oferente el único responsable del cumplimiento de todas las obligaciones laborales que correspondan según el caso (pago de salarios, vacaciones, aguinaldo, pagos jubilatorios, horas extras, viáticos, compensaciones, seguros, entre otros). El oferente exime al BCP de toda erogación y responsabilidad asociada a la prestación del servicio.	EXIGIDO	

1.2.1.9	Durante la duración del contrato, el BCP se reserva el derecho de solicitar reemplazos al equipo técnico, y el oferente debe presentar un nuevo integrante en un plazo no mayor a 10 días hábiles, el cual deberá cumplir con los requisitos establecidos en el PBC.	EXIGIDO	
1.2.1.10	Ante la ausencia de uno o más miembros del equipo por 3 (tres) días hábiles o más, cualquiera fuere la razón, el oferente será responsable de proveer un reemplazo temporal, hasta tanto el afectado se reintegre, sin perjuicios de las sanciones contractuales que correspondan.	EXIGIDO	
LOTE N° 2 SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE SEGURIDAD DNS			
ITEM N° 1 Servicio de suscripción a Solución de Seguridad DNS			
2.1.1 Características de la solución			
2.1.1.1	Se solicita el servicio de suscripción al Software de seguridad DNS, Cisco Umbrella Secure Internet Gateway Essentials implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.	EXIGIDO	
2.1.1.2	La Solución deberá estar basada en la nube (servicio SWG Cloud) y debe proveer análisis de consultas y resoluciones de DNS para al menos 800 usuarios.	EXIGIDO	
LOTE N° 3 SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE SEGURIDAD PERIMETRAL DEFINIDA POR SOFTWARE			
ITEM N° 1 Servicio de Suscripción a Solución de Seguridad Perimetral Definida por Software			
3.1.1 Características de la Solución			

3.1.1.1	Se solicita el servicio de suscripción a solución de seguridad perimetral definida por software Appgate SDP implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.	EXIGIDO	
3.1.1.2	Se deben incluir todas las licencias necesarias para al menos 980 usuarios, y con protección para 2 (dos) sitios o centro de datos.	EXIGIDO	
LOTE N° 4 SERVICIO DE SUSCRIPCIÓN A SOLUCIONES DE CIBERSEGURIDAD			
ITEM N° 1 - Servicio de suscripción a Solución de Análisis de Muestras de malware (Sandboxing)			
4.1.1 Características principales de la Solución			
4.1.1.1	Se solicita el servicio de suscripción a solución de análisis de muestras de malware (sandboxing) Trellix Virtual Advanced Threat Defense Appliance, implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.	EXIGIDO	
ITEM N° 2 - Servicio de suscripción a Solución de Seguridad Antimalware y EDR			
4.2.1 Características principales de la Solución			
4.2.1.1	Se solicita el servicio de suscripción a la solución de seguridad antimalware y EDR Trellix MVISION Protect Plus EDR para 1200 usuarios, implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.	EXIGIDO	
4.2.1.2	La Solución debe contar con un Registro Cloud de análisis de riesgo para al menos 25 mil diferentes servicios Cloud.	EXIGIDO	
4.2.1.3	Para cada servicio cloud se deben evaluar al menos 50 atributos y 260 sub atributos de riesgo.	EXIGIDO	

4.2.1.4	Debe monitorear si los servicios Cloud cuentan con las siguientes certificaciones: EU GDPR, Trustee / BBB, Safe Harbor, ISO 27018, FISMA, FedRAMP, CSA Star, HITRUST, ISO 27017, SAS 70 / SSAE16 / ISAE 3402, ITIL, DCAA / SOC 3, ISO 27001, SOC 2, PCI Compliance y HIPAA	EXIGIDO	
4.2.1.5	La Solución debe poder mostrar la exposición de los servicios Cloud a vulnerabilidades como: Cloudbleed, Heartbleed, Poodle, Freak, Ghostwriter.	EXIGIDO	
4.2.1.6	La Solución debe identificar intentos de fuga de información por servicios no corporativos a través del análisis de Machine Learning y UEBA, correlacionado con la actividad de los usuarios en los servicios.	EXIGIDO	
4.2.1.7	La Solución debe contar con la capacidad de control (Bloquear/Permitir) con base en atributos de Riesgo de Shadow IT.	EXIGIDO	
4.2.1.8	La Solución debe tener la capacidad de aplicar políticas de DLP al tráfico Web y de servicios de Shadow IT.	EXIGIDO	
4.2.1.9	La Solución debe tener la capacidad de aplicar políticas a la información en la nube basado en: - Diccionarios.	EXIGIDO	
4.2.1.10	- Palabras clave	EXIGIDO	
4.2.1.11	- Grupos de usuarios	EXIGIDO	
4.2.1.12	- Expresiones regulares	EXIGIDO	
4.2.1.13	La Solución debe permitir a los administradores: personalizar vistas y reportes, basados en la información que deseen ver.	EXIGIDO	
4.2.1.14	La consola debe permitir programar la ejecución de reportes y que estos sean enviados vía correo electrónico en formato PDF, CSV o XLS.	EXIGIDO	
4.2.1.15	La Solución debe presentar un dashboard de madurez de implementación de la misma, donde se muestre el nivel de adopción de la herramienta en la entidad, comparativas anónimas con otros clientes de la misma vertical y recomendaciones de funcionalidades que deben ser implementadas.	EXIGIDO	

ITEM N° 3 - Servicio de suscripción a Solución de Gestión de Vulnerabilidades			
4.3.1 Características principales de la Solución			
4.3.1.1	Se solicita el servicio de suscripción a la solución de gestión de vulnerabilidades Tenable implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.	EXIGIDO	
4.3.1.2	Se deben incluir todas las licencias necesarias para al menos 512 (quinientos doce) activos de TI, entre ellos estaciones de trabajo, servidores, dispositivos de red, plataformas de virtualización y otros sistemas conectados.	EXIGIDO	
LOTE N° 5 - SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE DETECCIÓN Y RESPUESTA EXTENDIDA - XDR			
ITEM N° 1 - Servicio de suscripción a Solución de Detección y Respuesta Extendida - XDR			
5.1.1 Características principales de la Solución			
5.1.1.1	Se solicita el servicio de suscripción a una Solución de Detección y Respuesta Extendida XDR, con el objetivo de facilitar la integración y la respuesta avanzada a incidentes de ciberseguridad, ejecución de playbooks y análisis de amenazas. La Solución debe tener, nativamente y sin ningún tipo de desarrollo adicional, integración con las soluciones de seguridad de endpoint y servidores con las cuales cuenta actualmente el BCP (Trellix MVISION Protect Plus EDR).	EXIGIDO	
5.1.1.2	La Solución debe incluir nativamente capacidades tales como: agregación y correlación de eventos, recolección de eventos de distintas fuentes de datos y definición de políticas de retención de información. Toda la información generada debe poder ser consumida por la propia Solución para la toma de decisiones, de forma nativa, y sin ningún tipo de desarrollo por fuera de la Solución.	EXIGIDO	

5.1.1.3	Se debe entregar todos los módulos de software necesarios para la correcta implementación de lo requerido en este ítem. Se deben incluir todas las licencias necesarias para al menos 750 EPS, con soporte y mantenimiento del fabricante por 24 meses computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.	EXIGIDO	
5.1.1.4	La solución debe tener la capacidad de integrar al menos 300 tecnologías diferentes, sin licenciamiento adicional.	EXIGIDO	
5.1.1.5	La solución debe tener la capacidad de minimizar el impacto de un incidente.	EXIGIDO	
5.1.1.6	La solución debe poder centralizar los datos recibidos con el fin de contar con visibilidad de las amenazas y vulnerabilidades.	EXIGIDO	
5.1.1.7	La solución debe soportar expresiones regulares compatibles con Perl.	EXIGIDO	
5.1.1.8	La solución debe soportar operaciones booleanas como AND, OR y NOT.	EXIGIDO	
5.1.1.9	Debe utilizar un lenguaje de análisis de datos para consultas de eventos para su posterior análisis.	EXIGIDO	
5.1.1.10	La solución debe soportar dentro de la anatomía del lenguaje utilizado al menos los siguientes aspectos: búsquedas, filtros, elementos sintaxis como día y hora, operadores de comparación, funciones hash criptográfica, variables de expansión, histograma.	EXIGIDO	
5.1.1.11	La solución debe proveer la capacidad de asignar un nombre de clase genérico que se refiera a eventos, por ejemplo, proxies: Bluecoat, firewall: Palo Alto, etc.	EXIGIDO	
5.1.1.12	La solución debe incluir al menos los siguientes métodos de autenticación: local, Radius, LDAP, Active Directory, Sigle sign-on.	EXIGIDO	
5.1.1.13	La solución debe proporcionar un flujo de trabajo de incidentes para rastrear eventos.	EXIGIDO	

5.1.1.14	Para el tránsito de todos los datos, debe realizarse con un cifrado SSL/TLS.	EXIGIDO	
5.1.1.15	La solución debe soportar al menos tres formas de contactar al soporte: licencia de suscripción, chat de soporte, por el servicio de expertise on demand.	EXIGIDO	
5.1.1.16	La solución debe soportar una consola maestra de alertas, con capacidad de personalizar dashboards, búsquedas, y resultados de búsquedas.	EXIGIDO	
5.1.1.17	La solución debe soportar el uso de API para la administración, así como para integración de fuentes de datos, si así se requiere.	EXIGIDO	
5.1.1.18	Los indicadores deben ser cargados a través de archivos CSV o JSON.	EXIGIDO	
5.1.1.19	Los indicadores deben de incluir al menos los siguientes campos: Value, Notes, Risk, Type.	EXIGIDO	
5.1.1.20	La solución debe de soportar dos tipos de reglas: las creadas por el fabricante y las personalizadas.	EXIGIDO	
5.1.1.21	La solución debe mostrar un gráfico que muestre el porcentaje de las reglas habilitadas creadas por el fabricante que están siendo utilizadas y las que no.	EXIGIDO	
5.1.1.22	Las reglas deben contener al menos la siguiente información: riesgo, nombre, estatus, opción de deshabilitar y ver la regla.	EXIGIDO	
5.1.1.23	La solución debe permitir asignar una contraseña al reporte en formato pdf cuando éste sea enviado por correo electrónico.	EXIGIDO	
5.1.1.24	La solución debe contar con un dashboard que muestre información sobre: estadísticas de eventos por segundo, estado general del dispositivo, eficacia de los sensores.	EXIGIDO	
5.1.1.25	La solución debe mostrar en las tablas de alertas, al menos la siguiente información: riesgo, tipo, origen, primer evento, último evento, sumario, estado, hash.	EXIGIDO	

5.1.1.26	La solución debe soportar la personalización de tablas de alertas.	EXIGIDO	
5.1.1.27	La solución debe indicar el nivel de amenaza basado en la inteligencia que realice, tomando en consideración al menos los siguientes aspectos: el valor de un evento indeterminado, el valor de un evento benigno, el valor de un evento sospechoso, el valor de un evento malicioso.	EXIGIDO	
5.1.1.28	La solución debe poder asignar alertas a los usuarios como parte del proceso de escalamiento y gestión de incidentes.	EXIGIDO	
5.1.1.29	La solución debe incluir una vista sobre consejos de investigación, que permitan ofrecer mayor detalle a través de preguntas con consultas de búsqueda asociadas y así tener una mejor comprensión de la amenaza.	EXIGIDO	
5.1.1.30	La solución debe poder exportar alertas a formato tipo JSON o CSV.	EXIGIDO	
5.1.1.31	La solución debe soportar la búsqueda y descarga de transcripciones de PCAP.	EXIGIDO	
5.1.1.32	La solución debe soportar al menos los siguientes tipos de log; security log, sysmon log, system log, application log, appLocker log, PowerShell Log, defender log, IIS log.	EXIGIDO	
5.1.1.33	La solución debe soportar la identificación de actividad sospechosa a través del análisis del comportamiento indicado por detectores, incluyéndose al menos los siguientes: Beacon Detection, DNS Entropy Detection, DNS Fast-flux Detection, Geofeasibility Detection, Credential Misuse Detection, Unacknowledged Connection Detection, Anomalous Wsman Activity Detection, Port Scanning Detection, Port Probing Detection, Data Theft (outbound) exfiltration Detection, Inbound Connections Detection, Server outbound Connections Detection, VPN Compromised Account Detection.	EXIGIDO	
5.1.1.34	La solución debe ser compatible para procesar registros a través de los siguientes métodos: IETF, syslog, RFC5424, RFC3164.	EXIGIDO	

5.1.1.35	La solución debe permitir la detección, validación, e investigación de alertas/amenazas, para así reconstruir el killchain de un ataque.	EXIGIDO	
5.1.1.36	La solución debe proveer la capacidad de generar una puntuación de riesgo.	EXIGIDO	
5.1.1.37	La solución debe tener la capacidad de minimizar el impacto de un incidente de forma automática.	EXIGIDO	
5.1.1.38	La solución debe generar una investigación visual guiada con los detalles de una incidencia.	EXIGIDO	
5.1.1.39	La solución debe tener integrado playbooks que automatizan las acciones de respuesta a las amenazas.	EXIGIDO	
5.1.1.40	La solución debe crear correlaciones automáticamente, a partir de alertas, utilizando análisis estadístico.	EXIGIDO	
5.1.1.41	La solución debe soportar alertas de terceros de más de 600 fuentes.	EXIGIDO	
5.1.1.42	La solución debe ser una plataforma de operación SaaS que permita tomar control de incidentes desde la detección hasta la respuesta.	EXIGIDO	
5.1.1.43	La solución debe detectar incidentes correlacionando datos de múltiples herramientas.	EXIGIDO	
5.1.1.44	La solución debe asistir en la toma de decisiones a través de inteligencia contextual sobre amenazas.	EXIGIDO	
5.1.1.45	La solución debe permitir centralizar la infraestructura y los datos de seguridad.	EXIGIDO	
5.1.1.46	La solución debe tener la capacidad de mejorar la detección de amenazas y vulnerabilidades con análisis avanzados de comportamiento de los usuarios	EXIGIDO	
5.1.1.47	La solución debe incluir paneles que brinden descripción del estado de las operaciones de seguridad tales como: - Numero de amenaza	EXIGIDO	
5.1.1.48	- Puntaje de riesgo.	EXIGIDO	

5.1.1.49	- Matriz de MITRE ATT&CK.	EXIGIDO	
5.1.1.50	- Amenazas asignadas.	EXIGIDO	
5.1.1.51	- Uso de datos dentro del entorno.	EXIGIDO	
5.1.1.52	- Salud del entorno.	EXIGIDO	
5.1.1.53	- Coincidencias de inteligencia que muestran actores e indicadores.	EXIGIDO	
5.1.1.54	La solución debe permitir acciones para asignar, cerrar, suprimir, contener y exportar una alerta.	EXIGIDO	
5.1.1.55	La solución debe soportar acciones para remediar la amenaza.	EXIGIDO	
5.1.1.56	La solución debe ser capaz de proporcionar una representación visual de cada incidente y un resumen de lo que sucedió (vectores que estuvieron involucrados - como las alertas conectadas. entre sí).	EXIGIDO	
5.1.1.57	La solución debe proporcionar información de los activos (host - usuario) basados en: - Clasificación de riesgo	EXIGIDO	
5.1.1.58	- Etiquetarlos como activo VIP	EXIGIDO	
5.1.1.59	- Exportar a un archivo CSV o JSON.	EXIGIDO	
5.1.1.60	La solución debe permitir la integración para automatizar tareas frecuentes a través de playbooks proporcionados por: Azure, Cloudvisory, detección bajo de manda, serviceNow, VirusTotal.	EXIGIDO	
5.1.1.61	La solución debe contar con un portal que permita agregar conexiones a la nube, abarcando plataformas como: Amazon Web Services (AWS), Google Cloud Platform (GCP), GSuite, Microsoft Azure, Microsoft 365 y Microsoft Teams. También se admiten alertas de proveedores como MimeCast, Proofpoint, MS Defender, Sophos (AV), TrendMicro y CrowdStrike.	EXIGIDO	

5.1.1.62	La solución debe permitir configurar notificaciones por correo electrónico.	EXIGIDO	
5.1.1.63	La solución debe mostrar información sobre cada táctica (Mitre ATT&CK) que se intentó durante el periodo de tiempo especificado.	EXIGIDO	
5.1.1.64	La solución debe mostrar el número de técnicas (Mitre ATT&CK) que se utilizaron en el intento de la táctica.	EXIGIDO	
5.1.1.65	La solución debe detallar el número de amenazas asociadas a cada técnica (Mitre ATT&CK).	EXIGIDO	
5.1.1.66	La solución debe proporcionar una comprensión del flujo de ataque a través de un gráfico que muestre los siguientes nodos: - Múltiples herramientas.	EXIGIDO	
5.1.1.67	- Múltiples fuentes.	EXIGIDO	
5.1.1.68	- Alertas múltiples.	EXIGIDO	
5.1.1.69	- Activos múltiples.	EXIGIDO	
5.1.1.70	- Múltiples artefactos.	EXIGIDO	
5.1.1.71	La solución debe tener la capacidad de agrupar una amenaza a través de una correlación o una alerta.	EXIGIDO	
5.1.1.72	La solución debe mostrar un gráfico de tabla que contenga al menos la siguiente información: riesgo, tipo, total de activos, total de eventos, primer evento, último evento, origen/destino, resumen (summary), asignación, estatus.	EXIGIDO	
5.1.1.73	La solución debe ser capaz de calcular el riesgo de un activo multiplicando la suma de los puntajes de riesgo de todas las alertas por el número de reglas para dividirse entre el total de alertas utilizando la siguiente escala o similar: 0-59: puntuación - severidad baja; 60-79: puntuación - severidad media; 80 - 99: puntuación - severidad alta; Mayor o igual a 100: puntuación - severidad crítica.	EXIGIDO	
5.1.1.74	La solución debe tener la capacidad de realizar las siguientes acciones relacionadas con la amenaza: - Contener	EXIGIDO	

5.1.1.75	- Eliminar	EXIGIDO	
5.1.1.76	- Asignar a un usuario	EXIGIDO	
5.1.1.77	- Cierre o suprimir	EXIGIDO	
5.1.1.78	La solución debe tener la capacidad de realizar las siguientes acciones relacionadas con la amenaza: - Activar un playbook	EXIGIDO	
5.1.1.79	- Realizar una reparación	EXIGIDO	
5.1.1.80	La solución debe mostrar una gráfica sobre las actividades playbooks ejecutadas en la organización.	EXIGIDO	
5.1.1.81	La solución debe permitir la visualización del diagrama de flujo que realiza el seguimiento de cada paso de la ejecución dentro del playbook.	EXIGIDO	
5.1.1.82	La solución debe permitir que el diagrama de flujo de la actividad del playbook y los detalles de la acción puedan ser exportados a formato JSON.	EXIGIDO	
5.1.1.83	La solución debe soportar la asignación de acciones de respuesta a los playbooks a través de artefactos relevantes como: hashes MD5, alertas, dominios, direcciones IP).	EXIGIDO	
5.1.1.84	La solución debe contar con la capacidad de que el fabricante cree paquetes de reglas dedicadas a tipos específicos de detección como: suplantación de identidad, para Windows, etc.	EXIGIDO	
5.1.1.85	La solución debe permitir visualizar la regla a través de una tabla la información donde se identifique: nombre, consulta (query), estatus, playbook, riesgo, creación.	EXIGIDO	
LOTE N° 6 - SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN FIREWALL DE APLICACIÓN WEB (WAF)			
ITEM N° 1 - Servicio de suscripción a Solución Firewall de Aplicación Web (WAF)			
6.1.1 Características principales de la Solución			

6.1.1.1	Se solicita el servicio de suscripción a solución firewall de aplicación web Barracuda 660 Vx implementado actualmente en el BCP, con soporte y mantenimiento del fabricante por 12 meses computados a partir de fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.	EXIGIDO	
6.1.1.2	La Solución debe contar con las siguientes características: Backend Servers Supported CPU Cores Allowed Throughput Response Control Outbound Data Theft Protection File Upload Control Vulnerability Scanner Integration Protection against Application DDoS Attacks Bot Defense/ Web Scraping Protection Network Firewall JSON Protection XML Firewall URL Encryption Adaptive Profiling AV for File Uploads Advanced Threat Protection Authentication and Authorization LDAP/RADIUS Load Balancing Caching and Compression Content Routing High Availability Advanced Routing	EXIGIDO	
LOTE N° 7 SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE DETECCIÓN Y RESPUESTA PARA NETWORKING - NDR			
ITEM N° 1 Servicio de suscripción a Solución de Detección y Respuesta para Networking - NDR			
7.1.1 Características principales de la Solución:			
7.1.1.1	Se solicita el servicio de suscripción a una Solución de ciberseguridad para la detección y respuesta a incidentes para networking, mediante el análisis de la metadatos del tráfico de red, para 300 fuentes, con el objetivo de realizar la medición e identificación de IoCs (indicadores de compromiso) a través de la técnica de detección continua de compromisos, con soporte y mantenimiento del fabricante por 24 meses, computados a partir de la fecha establecida al efecto en la orden de inicio que será emitida por el área administradora del contrato.	EXIGIDO	

7.1.1.2	La solución debe proporcionar, en modalidad de SaaS, la capacidad de medir el compromiso de la infraestructura tecnológica, en tiempo real, sin importar el formato enviado, siempre y cuando contenga la información necesaria.	EXIGIDO	
7.1.1.3	La solución debe tener la capacidad de recolectar, procesar y analizar las consultas DNS de la organización para identificar qué activos (estaciones de trabajo, servidores, equipos de red, etc.) están intentando comunicarse con potenciales atacantes.	EXIGIDO	
7.1.1.4	La solución debe tener la capacidad de recolectar, procesar y analizar los datos del Spambox para identificar quién y cómo están intentando atacar a la organización.	EXIGIDO	
7.1.1.5	La solución debe incluir agentes o colectores para al menos sistemas operativos Windows 10 o superior y Windows Server 2012 o superior.	EXIGIDO	
7.1.1.6	La solución debe poder ser implementada y debe tener la capacidad de realizar el proceso de recolección de datos sin la necesidad de hardware de propósito específico, tal como network taps u otros. El proceso de recolección de datos para medir compromiso debe estar basado en metadatos.	EXIGIDO	
7.1.1.7	El proceso de medición de compromiso debe estar basado en: consultas DNS, spambox, netflows, logs de proxy y/o firewall.	EXIGIDO	
7.1.1.8	La solución debe tener la capacidad de clasificar el resultado de la medición de compromiso. Ejemplo: Malware, C&C, Phishing.	EXIGIDO	
7.1.1.9	La solución debe almacenar datos de forma histórica de al menos 2 años.	EXIGIDO	
7.1.1.10	La solución debe tener la capacidad de realizar una revisión histórica o 'playback' de nuevos ataques para identificar compromiso histórico basado en nueva información.	EXIGIDO	
7.1.1.11	La solución debe identificar el origen del compromiso de manera precisa y sin la necesidad de la instalación de hardware de propósito específico.	EXIGIDO	

7.1.1.12	El proceso de análisis de los metadatos de la organización debe estar basado en: - Correlación contra más de 80 fuentes de ciberinteligencia.	EXIGIDO	
7.1.1.13	- Analizadores/algoritmos, supervisados o no, de machine learning e inteligencia artificial.	EXIGIDO	
7.1.1.14	La solución debe implementar la capacidad de adicionar nuevas fuentes de ciberinteligencia con conceptos tales como BYOTI "Bring your own threat intelligence".	EXIGIDO	
7.1.1.15	La solución debe proveer un portal web que sea accesible desde las últimas versiones estables de los navegadores Google Chrome, Firefox, Edge y Safari.	EXIGIDO	
7.1.1.16	La solución debe incluir al menos uno de los siguientes métodos de autenticación: local, Radius, LDAP, Active Directory, Single sign-on.	EXIGIDO	
7.1.2 Reportes y vistas			
7.1.2.1	El portal debe contener una vista que provea estadísticas de los indicadores de compromiso.	EXIGIDO	
7.1.2.2	La solución debe tener la opción de aplicar filtros predefinidos, como por fecha, ejemplo: Hoy, ayer, últimos 7 días, últimos 30 días.	EXIGIDO	
7.1.2.3	La solución debe tener la opción de aplicar filtros por un periodo de tiempo personalizado.	EXIGIDO	
7.1.2.4	La solución debe permitir agrupar los activos a través de etiquetas como: tipo de activos (estaciones de trabajo, servidores, equipos de red, etc.), grupos de usuarios, etc., de acuerdo con la necesidad de la organización.	EXIGIDO	
7.1.2.5	La solución debe incluir frecuencia del compromiso por día de la semana y hora del día. Asimismo, debe mostrar la distribución del ataque basado en etiquetas previamente configuradas (ejemplo: usuario remoto, oficina central, IOT), también debe contar con recursos relacionados con los compromisos y con unas guías (playbooks) para cada tipo de ataque detectado.	EXIGIDO	

7.1.2.6	La solución debe permitir mostrar los IoCs por cada compromiso detectado y se debe poder descargar directamente de la plataforma, en formato CSV.	EXIGIDO	
7.1.2.7	La solución debe tener una vista de incidentes que permita gestionar incidentes abiertos, cerrar incidentes y silenciar incidentes llevando registro de las acciones tomadas en los mismos.	EXIGIDO	
7.1.2.8	La solución debe incluir información del spambox como: volumen de correos analizados, destinatarios que reciben más spam, tendencias de ataques, días y horas de la semana en la que se recibe más correos maliciosos y correlación del spambox con respecto a la comunicación efectiva realizada hacia el potencial atacante.	EXIGIDO	
7.1.2.9	La solución debe enviar reportes vía correo electrónico con información de resultados de la evaluación de compromiso.	EXIGIDO	
7.1.2.10	La solución debe enviar notificación al correo electrónico del administrador de la plataforma o a los usuarios definidos en caso de la existencia de un indicador de compromiso detectado.	EXIGIDO	
7.1.2.11	La solución debe tener la opción de configurar la periodicidad de las notificaciones, tales como: envío de correo con las alertas de la última hora o de las últimas 4 horas, etc.	EXIGIDO	
7.1.2.12	La solución debe incluir en las notificaciones, el análisis de cada incidente basado en la matriz MITRE ATT&CK.	EXIGIDO	
7.1.2.13	La solución debe permitir configurar la periodicidad de los reportes. Ejemplo: diario, semanal, bisemanal y mensual	EXIGIDO	
7.1.3 Características y alertas			
7.1.3.1	La solución debe poder responder de forma automática, conectándose vía API a la infraestructura tecnológica para ajustar las políticas de bloqueo pertinentes, ante la detección de un compromiso.	EXIGIDO	

7.1.3.2	La solución debe incorporar capacidades automáticas de bloqueo con los fabricantes más reconocidos de la industria, tales como: Palo Alto Networks, Fortinet, Checkpoint, Cisco, entre otros.	EXIGIDO	
7.1.3.3	La solución debe proporcionar una API de forma tal que la organización pueda construir la integración que requiera para propósitos de defensa o gestión de incidentes.	EXIGIDO	
7.1.3.4	La solución debe tener la capacidad de realizar la descarga de información de amenazas en formato STIX.	EXIGIDO	
7.1.3.5	La solución debe proporcionar el contexto de cada compromiso con referencias internas y externas para entender la naturaleza del mismo.	EXIGIDO	
7.1.3.6	La solución debe permitir el direccionamiento del tráfico DNS a un DNS publico ofrecido por el proveedor.	EXIGIDO	
7.1.3.7	La solución debe permitir consumir metadatos de plataformas de VPN para medición de compromiso de dispositivos remotos en modo full tunnel y split tunnel.	EXIGIDO	
7.1.3.8	La solución debe proporcionar una API abierta para consumir metadatos, de forma que la organización pueda utilizarla para propósitos específicos.	EXIGIDO	
7.1.3.9	La solución debe soportar colectores o su equivalente para los hipervisores VirtualBox, Hyper-V y VMware.	EXIGIDO	
7.1.4 Calidad y capacidad del Talento Humano			
7.1.4.1	El proveedor debe ofrecer la gestión de los incidentes generados en la solución en modalidad 7x24.	EXIGIDO	
7.1.4.2	El alcance de la gestión de incidentes debe entregar al equipo de la organización la guía necesaria para la mitigación de estos, identificados por la solución.	EXIGIDO	
7.1.4.3	El proveedor debe proporcionar el apoyo necesario para el despliegue de la solución.	EXIGIDO	
7.1.4.4	El proveedor debe proporcionar resolución de dudas sobre la forma de mitigación de los compromisos detectados.	EXIGIDO	

7.1.4.5	El proveedor debe disponibilizar entrenamiento/capacitación de la solución ofrecida para traspaso de conocimiento al personal para asegurar la correcta operación.	EXIGIDO	
7.1.4.6	El proveedor debe incluir un plan de implementación, actualización u optimización, además del acompañamiento continuo a lo largo de la duración de la prestación del servicio.	EXIGIDO	

Equipos y dispositivos existentes en el BCP:

Tipo	Descripción	Cantidad
Server	Total de Servidores Físicos	50
Storage	IBM, Dell	7
Hipervisores	ESXi 5, 6	34
Hipervisores	HyperV	2
Server	CentOS Linux	39
Server	RedHat	18
Server	Generic Linux	13
Server	Microsoft Windows Server Otros	54
Server	Microsoft Windows Server 2012	60
Server	Microsoft Windows Server 2016	3
MBD	MS SQL	5
MBD	PostgreSQL	1
MBD	MySQL	4

MBD	Sybase	4
MBD	Oracle	6
Server	Servidor de archivos	5
Server	Servidor Exchange	2
Firewall	Checkpoint	3
Firewall	Cisco FTD	2
Firewall	Cisco ASA	5
LB	Citrix	2
Router	Cisco IOS	3
Switch	Cisco IOS	70
Switch	Cisco NX-OS	15
Wireless	Cisco WLAN Controller	3
Wireless	Cisco AP	50
Proxy	Forcepoint	2
Usuarios	Estaciones de trabajo (PCs, Notebooks)	900
Usuarios	Dispositivos móviles (Android/iOS)	70

CONDICIONES GENERALES

Administración del Contrato: la administración del contrato estará a cargo del Departamento de Ciberseguridad del Banco Central del Paraguay.

Compromiso de Confidencialidad: el personal interviniente del Proveedor deberá firmar un Compromiso de Confidencialidad de la Información, dado que podría acceder a información confidencial de la contratante, en los términos del Formulario incluido en la Sección Formularios. La firma del Compromiso de Confidencialidad se realizará al momento de la suscripción del Contrato. El Departamento de Ciberseguridad será el responsable de gestionar la firma de dicha documentación. En caso de que se incorpore nuevo personal del Proveedor se deberá gestionar la firma del Compromiso de Confidencialidad por parte de estos.

Área Técnica Administradora del Contrato: la administración del contrato estará a cargo del Departamento de Ciberseguridad.

Acuerdo de Nivel de Servicio: El Proveedor deberá suscribir un Acuerdo de Nivel de Servicio, bajo los siguientes términos:

Tiempo de respuesta a incidentes que afectan la disponibilidad del servicio:

Crítico: 2 (dos) horas desde la comunicación del incidente.

En caso de no cumplir con el plazo establecido, el Proveedor deberá comunicarlo por escrito mediante nota dirigida al DCS, indicando los motivos técnicos de su atraso. En estos casos, el Proveedor está obligado a proporcionar y mantener funcionando el servicio de respaldo/contingencia mientras dure la reparación y puesta a punto del servicio.

No crítico: 4 (cuatro) horas desde la comunicación del incidente.

El Proveedor facilitará el nombre, número telefónico y correo electrónico del contacto para gestionar los incidentes críticos y no críticos.

Informes y Actas: El Proveedor deberá elaborar de manera mensual un informe técnico de cumplimiento que contemple las actividades desarrolladas respecto al servicio que fuera adjudicado (deberá contener como mínimo fecha de la actividad, tareas realizadas, participantes, entre otros datos relacionados), así como un acta de conformidad por los trabajos mensuales que será suscrito en conjunto con el área administradora del contrato.

Lugar y Horario de Trabajo: la prestación de los servicios se realizará de manera presencial en las oficinas del Banco Central, sito en Av. Federación Rusa y Augusto Roa Bastos. Para casos excepcionales y previo acuerdo con la contraparte técnica administradora del contrato (Departamento de Ciberseguridad del BCP), se podrá realizar de manera remota, a través de herramientas tecnológicas tales como Microsoft Teams, acceso VPN a través de herramientas SDP o similares.

Plazo de vigencia del Contrato: el plazo de vigencia será a partir de la fecha que se establezca al efecto en la Orden de Inicio del Servicio, la cual será emitida dentro del plazo de 10 (diez) días hábiles desde la suscripción del Contrato, hasta el cumplimiento total de las obligaciones contractuales.

Plazo de prestación/ejecución de los servicios:

Para los Lotes 1, 2, 3, 4, 5 y 7: el plazo de prestación total de los servicios será de 24 (veinticuatro) meses contados a partir de la fecha que se establezca al efecto en la Orden de Inicio del Servicio, la cual será emitida dentro del plazo de 10 (diez) días hábiles, desde la suscripción del Contrato.

Para el Lote 6: el plazo de prestación total de los servicios será de 12 (doce) meses contados a partir de la fecha que se establezca al efecto en la Orden de Inicio del Servicio, la cual será emitida dentro del plazo de 10 (diez) días hábiles, desde la suscripción del Contrato.

Identificación de la unidad solicitante y justificaciones

•El presente llamado a ser publicado ha sido solicitado por: el Departamento de Ciberseguridad del Banco Central del Paraguay.

•La necesidad que se pretende satisfacer mediante la contratación realizada radica en: mantener y fortalecer las capacidades defensivas en materia de ciberseguridad de la Institución, y mejorar las capacidades técnicas y tecnológicas que le permitan ejecutar las operaciones de ciberseguridad esenciales, principalmente, en la detección, prevención, respuesta y recuperación de los eventos e incidentes de ciberseguridad, de la manera más automatizada posible, lo cual incluye: herramientas, personas, procesos y soporte externo especializado, desde un contexto centralizado, sin que se vean afectados los recursos humanos destinados a los procesos estratégicos o misionales del BCP.

•Con relación a la planificación, se indica que: se trata de un llamado periódico, sucesivo ya que la necesidad es continua.

•Las especificaciones técnicas establecidas se justifican en: las necesidades actuales de la Institución, en su infraestructura, conocimiento del área técnica, entre otros.

Plan de entrega de los bienes

La entrega de los bienes se realizará de acuerdo al plan de entrega y cronograma de cumplimiento, indicado en el presente apartado. Así mismo, de los documentos de embarque y otros que deberá suministrar el proveedor indicado a continuación:

NO APLICA.

Plan de entrega de los servicios

Ítems	Descripción del servicio	Cantidad	Unidad de medida	Lugar donde los servicios serán prestados	Plazo de prestación/ejecución de los servicios	Plazo de vigencia del Contrato
De acuerdo a la Lista de Precios publicada en el SICP	De acuerdo a la Lista de Precios publicada en el SICP	De acuerdo a la Lista de Precios publicada en el SICP	De acuerdo a la Lista de Precios publicada en el SICP	Los servicios correspondientes a todos los lotes deberán ser realizados en el Banco Central del Paraguay, sito en Av. Federación Rusa y Augusto Roa Bastos o de manera remota para casos excepcionales y previo acuerdo con la contraparte técnica administradora del contrato (Departamento de Ciberseguridad del BCP). La comunicación se realizará a través de herramientas tecnológicas tales como Microsoft Teams o similares.	Lotes 1, 2, 3, 4, 5 y 7: El plazo de prestación total de los servicios será de 24 (veinticuatro) meses contados a partir de la fecha que se establezca al efecto en la Orden de Inicio del Servicio, la cual será emitida dentro del plazo de 10 (diez) días hábiles, desde la suscripción del Contrato. Lote 6: El plazo de prestación total de los servicios será de 12 (doce) meses contados a partir de la fecha que se establezca al efecto en la Orden de Inicio del Servicio, la cual será emitida dentro del plazo de 10 (diez) días hábiles, desde la suscripción del Contrato.	El plazo de vigencia será a partir de la fecha que se establezca al efecto en la Orden de Inicio del Servicio, la cual será emitida dentro del plazo de 10 (diez) días hábiles, desde la suscripción del Contrato, hasta el cumplimiento total de las obligaciones contractuales.

Planos y diseños

Para la presente contratación se pone a disposición los siguientes planos o diseños:

No Aplica

Embalajes y documentos

El embalaje, la identificación y la documentación dentro y fuera de los paquetes serán como se indican a continuación:

No Aplica

Inspecciones y pruebas

Las inspecciones y pruebas serán como se indica a continuación:

La Contratante fiscalizará la ejecución del Contrato a través del área administradora del Contrato. Se verificará que lo ejecutado cumpla a cabalidad con lo establecido en la Sección Suministros Requeridos Especificaciones técnicas y en la Lista de Precios; y se adecuen al Plan de Entrega de los Bienes o Servicios del presente PBC.

1. El proveedor realizará todas las pruebas y/o inspecciones de los Bienes, por su cuenta y sin costo alguno para la contratante.
2. Las inspecciones y pruebas podrán realizarse en las instalaciones del Proveedor o de sus subcontratistas, en el lugar de entrega y/o en el lugar de destino final de entrega de los bienes, o en otro lugar en este apartado.
Cuando dichas inspecciones o pruebas sean realizadas en recintos del Proveedor o de sus subcontratistas se le proporcionarán a los inspectores todas las facilidades y asistencia razonables, incluso el acceso a los planos y datos sobre producción, sin cargo alguno para la Contratante.
3. La Contratante o su representante designado tendrá derecho a presenciar las pruebas y/o inspecciones mencionadas en la cláusula anterior, siempre y cuando éste asuma todos los costos y gastos que ocasione su participación, incluyendo gastos de viaje, alojamiento y alimentación.
4. Cuando el proveedor esté listo para realizar dichas pruebas e inspecciones, notificará oportunamente a la contratante indicándole el lugar y la hora. El proveedor obtendrá de una tercera parte, si corresponde, o del fabricante cualquier permiso o consentimiento necesario para permitir a la contratante o a su representante designado presenciar las pruebas o inspecciones.
5. La Contratante podrá requerirle al proveedor que realice algunas pruebas y/o inspecciones que no están requeridas en el contrato, pero que considere necesarias para verificar que las características y funcionamiento de los bienes cumplan con los códigos de las especificaciones técnicas y normas establecidas en el contrato. Los costos adicionales razonables que incurra el Proveedor por dichas pruebas e inspecciones serán sumados al precio del contrato, en cuyo caso la contratante deberá justificar a través de un dictamen fundado en el interés público comprometido. Asimismo, si dichas pruebas y/o inspecciones impidieran el avance de la fabricación y/o el desempeño de otras obligaciones del proveedor bajo el Contrato, deberán realizarse los ajustes correspondientes a las Fechas de Entrega y de Cumplimiento y de las otras obligaciones afectadas.
6. El proveedor presentará a la contratante un informe de los resultados de dichas pruebas y/o inspecciones.

7. La contratante podrá rechazar algunos de los bienes o componentes de ellos que no pasen las pruebas o inspecciones o que no se ajusten a las especificaciones. El proveedor tendrá que rectificar o reemplazar dichos bienes o componentes rechazados o hacer las modificaciones necesarias para cumplir con las especificaciones sin ningún costo para la contratante. Asimismo, tendrá que repetir las pruebas o inspecciones, sin ningún costo para la contratante, una vez que notifique a la contratante.
8. El proveedor acepta que ni la realización de pruebas o inspecciones de los bienes o de parte de ellos, ni la presencia de la contratante o de su representante, ni la emisión de informes, lo eximirán de las garantías u otras obligaciones en virtud del contrato.

Indicadores de Cumplimiento

El documento requerido para acreditar el cumplimiento contractual, será:

Nota/Formulario de conformidad del área técnica.

Planificación de indicadores de cumplimiento:

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
Documentos de solicitud de los bienes/ servicios al Proveedor, si correspondiere, y Conformidad del área técnica administradora del contrato.	<ul style="list-style-type: none">Documentos de solicitud de los bienes/servicios al Proveedor emitidos por el área administradora del contrato, si correspondiere.Nota / Formulario / Providencia / Memorando de conformidad del área técnica administradora del contrato.	En el marco de la ejecución contractual, de acuerdo con el plazo establecido en el Plan de Entrega de los bienes o servicios del presente PBC, el área administradora del contrato emitirá los documentos de solicitud al Proveedor, si correspondiere, y posteriormente, el/la Nota/Formulario/Providencia/Memorando de conformidad, exigida/o para el/los pago/s correspondiente/s.

De manera a establecer indicadores de cumplimiento, a través del sistema de seguimiento de contratos, la convocante deberá determinar el tipo de documento que acredite el efectivo cumplimiento de la ejecución del contrato, así como planificar la cantidad de indicadores que deberán ser presentados durante la ejecución. Por lo tanto, la convocante en este apartado y de acuerdo al tipo de contratación de que se trate, deberá indicar el documento a ser comunicado a través del módulo de Seguimiento de Contratos y la cantidad de los mismos.

Criterios de Adjudicación

La convocante adjudicará el contrato al oferente cuya oferta haya sido evaluada como la más baja y cumpla sustancialmente con los requisitos de las bases y condiciones, siempre y cuando la convocante determine que el oferente está calificado para ejecutar el contrato satisfactoriamente.

1. La adjudicación en los procesos de contratación en los cuales se aplique la modalidad de contrato abierto, se efectuará por las cantidades o montos máximos solicitados en el llamado, sin que ello implique obligación de la convocante de requerir la provisión de esa cantidad o monto durante de la vigencia del contrato, obligándose sí respecto de las cantidades o montos mínimos establecidos.
 2. En caso de que la convocante no haya adquirido la cantidad o monto mínimo establecido, deberá consultar al proveedor si desea ampliarlo para el siguiente ejercicio fiscal, hasta cumplir el mínimo.
 3. Al momento de adjudicar el contrato, la convocante se reserva el derecho a disminuir la cantidad de Bienes requeridos, por razones de disponibilidad presupuestaria u otras razones debidamente justificadas. Estas variaciones no podrán alterar los precios unitarios u otros términos y condiciones de la oferta y de los documentos de la licitación.
- En aquellos llamados en los cuales se aplique la modalidad de contrato abierto, cuando la Convocante deba disminuir cantidades o montos a ser adjudicados, no podrá modificar el monto o las cantidades mínimas establecidas en las bases de la contratación.

Notificaciones

La comunicación de la adjudicación a los oferentes será como sigue:

1. Dentro de los cinco (5) días corridos de haberse resuelto la adjudicación, la convocante comunicará a través del Sistema de Información de Contrataciones Públicas, copia del informe de evaluación y del acto administrativo de adjudicación, los cuales serán puestos a disposición pública en el referido sistema. Adicionalmente el sistema generará una notificación a los oferentes por los medios remotos de comunicación electrónica pertinentes, la cual será reglamentada por la DNCP.
2. En sustitución de la notificación a través del Sistema de Información de Contrataciones Públicas, las convocantes podrán dar a conocer la adjudicación por cédula de notificación a cada uno de los oferentes, acompañados de la copia íntegra del acto administrativo y del informe de evaluación. La no entrega del informe en ocasión de la notificación, suspende el plazo para formular protestas hasta tanto la convocante haga entrega de dicha copia al oferente solicitante.
3. En caso de la convocante opte por la notificación física a los oferentes participantes, deberá realizarse únicamente con el acuse de recibo y en el mismo con expresa mención de haber recibido el informe de evaluación y la resolución de adjudicación.
4. Las cancelaciones o declaraciones desiertas deberán ser notificadas a todos los oferentes, según el procedimiento indicado precedentemente.
5. Las notificaciones realizadas en virtud al contrato, deberán ser por escrito y dirigirse a la dirección indicada en el contrato.

Audiencia Informativa

Una vez notificado el resultado del proceso, el oferente tendrá la facultad de solicitar una audiencia a fin de que la convocante explique los fundamentos que motivan su decisión.

La solicitud de audiencia informativa no suspenderá ni interrumpirá el plazo para la interposición de protestas.

La misma deberá ser solicitada dentro de los dos (2) días hábiles siguientes en que el oferente haya tomado conocimiento de los términos del Informe de Evaluación de Ofertas.

La convocante deberá dar respuesta a dicha solicitud dentro de los dos (2) días hábiles de haberla recibido y realizar la audiencia en un plazo que no exceda de dos (2) días hábiles siguientes a la fecha de respuesta al oferente.

Documentación requerida para la firma del contrato

Luego de la notificación de adjudicación, el proveedor deberá presentar en el plazo establecido en las reglamentaciones vigentes, los documentos indicados en el presente apartado.

1. Personas Físicas / Jurídicas
<ul style="list-style-type: none">• Certificado de no encontrarse en quiebra o en convocatoria de acreedores expedido por la Dirección General de Registros Públicos;
<ul style="list-style-type: none">• Certificado de no hallarse en interdicción judicial expedido por la Dirección General de Registros Públicos;
<ul style="list-style-type: none">• Constancia de no adeudar aporte obrero patronal expedida por el Instituto de Previsión Social.
<ul style="list-style-type: none">• Certificado laboral vigente expedido por la Dirección de Obrero Patronal dependiente del Viceministerio de Trabajo, siempre que el sujeto esté obligado a contar con el mismo, de conformidad a la reglamentación pertinente - CPS
<ul style="list-style-type: none">• En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación.
<ul style="list-style-type: none">• Certificado de cumplimiento tributario vigente a la firma del contrato.
2. Documentos. Consorcios
<ul style="list-style-type: none">• Cada integrante del Consorcio que sea una persona física o jurídica deberá presentar los documentos requeridos para oferentes individuales especificados en los apartados precedentes.
<ul style="list-style-type: none">• Original o fotocopia del Consorcio constituido
<ul style="list-style-type: none">• Documentos que acrediten las facultades del firmante del contrato para comprometer solidariamente al consorcio.

- En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación.

CONDICIONES CONTRACTUALES

Esta sección constituye las condiciones contractuales a ser adoptadas por las partes para la ejecución del contrato.

Interpretación

Interpretación

1. Si el contexto así lo requiere, el singular significa el plural y viceversa; y "día" significa día calendario, salvo que se haya indicado expresamente que se trata de días hábiles.

2. Condiciones prohibidas, inválidas o inejecutables

Si cualquier provisión o condición del contrato es prohibida o resultase inválida o inejecutable, dicha prohibición, invalidez o falta de ejecución no afectará la validez o el cumplimiento de las otras provisiones o condiciones del contrato.

3. Limitación de Dispensas:

a) Toda dispensa a los derechos o facultades de una de las partes en virtud del contrato, deberá ser documentada por escrito, indicar la fecha, estar firmada por un representante autorizado de la parte que otorga dicha dispensa y deberá especificar la obligación que está dispensando y el alcance de la dispensa.

b) Sujeto a lo indicado en el inciso precedente, ningún retraso, prórroga, demora o aprobación por cualquiera de las partes al hacer cumplir algún término y condición del contrato o el otorgar prórrogas por una de las partes a la otra, perjudicará, afectará o limitará los derechos de esa parte en virtud del contrato. Asimismo, ninguna prórroga concedida por cualquiera de las partes por un incumplimiento del contrato, servirá de dispensa para incumplimientos posteriores o continuos del contrato.

Subcontratación

El porcentaje permitido para la subcontratación será de:

No Aplica

La subcontratación del contrato deberá ser realizada conforme a las disposiciones contenidas en la Ley, el Decreto Reglamentario y la reglamentación que emita para el efecto la DNCP.

Derechos Intelectuales

1. Los derechos de propiedad intelectual de todos los planos, documentos y otros materiales conteniendo datos e información proporcionada a la contratante por el proveedor, seguirán siendo salvo prueba en contrario de propiedad del proveedor. Si esta información fue suministrada a la contratante directamente o a través del proveedor por terceros, incluyendo proveedores de materiales, los derechos de propiedad intelectual de dichos materiales seguirá siendo de propiedad de dichos terceros.

2. Sujeto al cumplimiento por parte de la contratante del párrafo siguiente, el proveedor indemnizará y liberará de toda responsabilidad a la contratante, sus empleados y funcionarios en caso de pleitos, acciones o procedimientos administrativos, reclamaciones, demandas, pérdidas, daños, costos y gastos de cualquier naturaleza, incluyendo gastos y honorarios por representación legal, que la contratante tenga que incurrir como resultado de la transgresión o supuesta transgresión de derechos de propiedad intelectual como patentes, dibujos y modelos industriales registrados, marcas registradas, derechos de autor u otro derecho de propiedad intelectual registrado o ya existente en la fecha del contrato debido a:

- a) La instalación de los bienes por el proveedor o el uso de los bienes en la República del Paraguay; y
- b) La venta de los productos producidos por los bienes en cualquier país.

Dicha indemnización no procederá si los bienes o una parte de ellos fuesen utilizados para fines no previstos en el Contrato o para fines que no pudieran inferirse razonablemente del Contrato. La indemnización tampoco cubrirá cualquier transgresión que resultara del uso de los bienes o parte de ellos, o de cualquier producto producido como resultado de asociación o combinación con otro equipo, planta o materiales no suministrados por el proveedor en virtud del Contrato.

3. Si se entablara un proceso legal o una demanda contra la contratante como resultado de alguna de las situaciones indicadas en la cláusula anterior, la Contratante notificará prontamente al proveedor y éste por su propia cuenta y en nombre de la Contratante responderá a dicho proceso o demanda, y realizará las negociaciones necesarias para llegar a un acuerdo de dicho proceso o demanda.

4. Si el proveedor no notifica a la contratante dentro de treinta (30) días a partir del recibo de dicha comunicación de su intención de proceder con tales procesos o reclamos, la contratante tendrá derecho a emprender dichas acciones en su propio nombre.

5. La contratante se compromete, a solicitud del proveedor, a prestarle toda la asistencia posible para que el proveedor pueda contestar las citadas acciones legales o reclamaciones. La Contratante será reembolsada por el proveedor por todos los gastos razonables en que hubiera incurrido.

6. La contratante deberá indemnizar y eximir de culpa al proveedor y a sus empleados, funcionarios y subcontratistas, por cualquier litigio, acción legal o procedimiento administrativo, reclamo, demanda, pérdida, daño, costo y gasto, de cualquier naturaleza, incluyendo honorarios y gastos de abogado, que pudieran afectar al proveedor como resultado de cualquier transgresión o supuesta transgresión de patentes, modelos de aparatos, diseños registrados, marcas registradas, derechos de autor, o cualquier otro derecho de propiedad intelectual registrado o ya existente a la fecha del contrato, que pudieran suscitarse con motivo de cualquier diseño, datos, planos, especificaciones, u otros documentos o materiales que hubieran sido suministrados o diseñados por la contratante o a nombre suyo.

Transporte

La responsabilidad por el transporte de los bienes será según se establece en los Incoterms.

Si no está de acuerdo con los Incoterms, la responsabilidad por el transporte deberá ser como sigue:

El transporte de los bienes, será responsabilidad del Proveedor.

Confidencialidad de la información

1. No deberá darse a conocer información alguna acerca del análisis, aclaración y evaluación de las ofertas ni sobre las recomendaciones relativas a la adjudicación, después de la apertura en público de las ofertas, a los oferentes ni a personas no involucradas en el proceso de evaluación, hasta que haya sido dictada la Resolución de Adjudicación cuando se trate de un solo sobre. Cuando se trate de dos sobres la confidencialidad de la primera etapa será hasta la emisión del acto administrativo de selección de ofertas técnicas, reanudándose la confidencialidad después de la apertura en público de las

ofertas económicas hasta la emisión de la resolución de adjudicación.

2. La contratante y el proveedor deberán mantener confidencialidad y en ningún momento divulgarán a terceros, sin el consentimiento de la otra parte, documentos, datos u otra información que hubiera sido directa o indirectamente proporcionada por la otra parte en conexión con el Contrato, antes, durante o después de la ejecución del mismo. No obstante, el proveedor podrá proporcionar a sus subcontratistas los documentos, datos e información recibidos de la contratante para que puedan cumplir con su trabajo en virtud del contrato. En tal caso, el proveedor obtendrá de dichos subcontratistas un compromiso de confidencialidad similar al requerido al proveedor en la presente cláusula.

3. La contratante no utilizará dichos documentos, datos u otra información recibida del proveedor para ningún uso que no esté relacionado con el contrato. Así mismo el proveedor no utilizará los documentos, datos u otra información recibida de la contratante para ningún otro propósito diferente al de la ejecución del contrato.

4. La obligación de las partes arriba mencionadas, no aplicará a la información que:

- a) La contratante o el proveedor requieran compartir con otras instituciones que participan en el financiamiento del contrato;
 - b) Actualmente o en el futuro se hace de dominio público sin culpa de ninguna de las partes;
 - c) Puede comprobarse que estaba en posesión de esa parte en el momento que fue divulgada y no fue previamente obtenida directa o indirectamente de la otra parte; o
 - d) Que de otra manera fue legalmente puesta a la disponibilidad de esa parte por un tercero que no tenía obligación de confidencialidad.
5. Las disposiciones precedentes no modificarán de ninguna manera ningún compromiso de confidencialidad otorgado por cualquiera de las partes a quien esto compete antes de la fecha del contrato con respecto a los suministros o cualquier parte de ellos.
6. Las disposiciones de esta cláusula permanecerán válidas después del cumplimiento o terminación del contrato por cualquier razón.

Obligatoriedad de declarar información del personal del contratista en el SICP

1. El proveedor deberá proporcionar los datos de identificación de sus subproveedores, así como de las personas físicas por medio de las cuales propone cumplir con las obligaciones del contrato, dentro de los treinta días posteriores a la obtención del código de contratación, y con anterioridad al primer pago que vaya a percibir en el marco de dicho contrato, con las especificaciones respecto a cada una de ellas. A ese respecto, el contratista deberá consignar dichos datos en el Formulario de Información del Personal (FIP) y en el Formulario de Informe de Servicios Personales (FIS), a través del SIPE.

2. Cuando ocurra algún cambio en la nómina del personal o de los subcontratistas propuestos, el proveedor o contratista está obligado a actualizar el FIP.

3. Como requerimiento para efectuar los pagos a los proveedores o contratistas, la contratante, a través del procedimiento establecido para el efecto por la entidad previsional, verificará que el proveedor o contratista se encuentre al día en el cumplimiento con sus obligaciones para con el Instituto de Previsión Social (IPS).

4. La Contratante podrá realizar las diligencias que considere necesarias para verificar que la totalidad de las personas que prestan servicios personales en relación de dependencia para la contratista y eventuales subcontratistas se encuentren debidamente individualizados en los listados recibidos.

5. El proveedor o contratista deberá permitir y facilitar los controles de cumplimiento de sus obligaciones de aporte obrero patronal, tanto los que fueran realizados por la contratante como los realizados por el IPS y por funcionarios de la DNCP. La negativa expresa o tácita se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.

6. En caso de detectarse que el proveedor o contratista o alguno de los subcontratistas, no se encontraran al día con el cumplimiento de sus obligaciones para con el IPS, deberán ser emplazados por la contratante para que en diez (10) días hábiles cumplan con sus obligaciones pendientes con la previsional. En el caso de que no lo hiciera, se considerará incumplimiento del

contrato por causa imputable al proveedor o contratista.

Formas y condiciones de pago

El adjudicado para solicitar el pago de las obligaciones deberá presentar la solicitud acompañada de los siguientes documentos:

1. Documentos Genéricos:

1. Nota de remisión u orden de prestación de servicios según el objeto de la contratación;
2. La factura de pago, con timbrado vigente, la cual deberán expresar claramente por separado el Impuesto al Valor Agregado (IVA) de conformidad con las disposiciones tributarias aplicables. En ningún caso el valor total facturado podrá exceder el valor adjudicado o las adendas aprobadas;
3. REPSE (registro de prestadores de servicios) todos los que son prestadores de servicios;
4. Certificado de Cumplimiento Tributario;
5. Constancia de Cumplimiento con la Seguridad Social;
6. Formulario de Informe de Servicios Personales (FIS).

Otras formas y condiciones de pago al proveedor en virtud del contrato serán las siguientes:

El adjudicado para solicitar el pago de las obligaciones deberá presentar la solicitud acompañada de los siguientes documentos:

1. Documentos Genéricos:

- a) Nota de remisión u orden de prestación del servicio, cuando corresponda;
- b) La factura de pago, con timbrado vigente, la cual deberán expresar claramente por separado el Impuesto al Valor Agregado (IVA) de conformidad con las disposiciones tributarias aplicables. En ningún caso el valor total facturado podrá exceder el valor adjudicado o las adendas aprobadas;
- c) Certificado de Cumplimiento Tributario;
- d) Constancia de Cumplimiento con la Seguridad Social;
- e) Formulario de informe de servicios personales (FIS),

2. Otros documentos:

- a) En la solicitud de pago, el Proveedor deberá incluir los siguientes datos:

- El número de cuenta habilitada en una entidad sujeta a las disposiciones de la Ley No. 861 General de Bancos, Financieras y Otras Entidades de Crédito, en la cual se depositarán los fondos del pago correspondiente.

- La dirección de correo electrónico (e-mail) de la empresa, a los efectos de que la Contratante comunique y/o informe cualquier cuestión atinente a la relación contractual.

En caso de que se hubiere establecido más de un pago en el marco de la contratación, el Proveedor deberá presentar los datos citados en la solicitud de pago de la primera factura, los que se mantendrán invariables para los pagos posteriores, debiendo el proveedor comunicar por escrito cualquier modificación/actualización que hubiere en los mismos.

La Contratante abonará al Proveedor en Guaraníes, en un plazo máximo de 30 (treinta) días contados a partir de la presentación de la factura correspondiente y del otorgamiento de la conformidad por parte del área técnica encargada del control y fiscalización.

En caso de constatare alguna deficiencia en la documentación presentada, la UOC reclamará al proveedor a través del correo electrónico (email) indicado en su oferta y el plazo para el pago será computado desde la presentación en forma satisfactoria del último documento requerido.

El/los precio/s facturado/s por el Proveedor no deberá/n diferir del/los que hubiese cotizado en su oferta (Lista de Precios), con excepción de los ajustes de precios de acuerdo a lo establecido en el presente PBC.

Se retendrá el equivalente a cero punto cinco por ciento (0.5%) sobre el importe de la factura, deducidos los impuestos correspondientes, conforme lo establecido en el Art. 41 de la Ley 3439/07, que modifica a la Ley 2051/03 de Contrataciones Públicas y en el Art. 278 de la Ley N° 7050/23.

En caso de que la contratación sea plurianual, los pagos correspondientes a cada ejercicio fiscal, estarán sujetos a su

aprobación presupuestaria correspondiente.

En el mes de enero y la quincena de febrero, al no contar con Plan Financiero, la presentación de las facturas que correspondan a los efectos del pago, podrán presentarse en la segunda quincena del mes de febrero, una vez que la contratante cuente con las reglamentaciones presupuestarias. Por lo tanto, en estas fechas no corresponde la aplicación de intereses a las facturas presentadas.

MULTAS:

Si la Contratante observare atrasos, deficiencias y/o incumplimientos, imputables al Proveedor, en la ejecución de lo contratado en los plazos o formas establecidos por el área administradora del contrato o en el Pliego de Bases y Condiciones, el Contrato o sus eventuales prórrogas, salvo casos fortuitos o de fuerza mayor justificada, será pasible de una multa equivalente al cero coma trescientos treinta y tres por ciento (0,333%) del valor total de la factura correspondiente al mes en que se produjo el atraso, la deficiencia y/o incumplimiento, por cada día de atraso y/o por cada deficiencia y/o incumplimiento.

La Contratante queda autorizada a deducir estas multas, en forma automática y sin interpelación judicial, de la factura del servicio correspondiente, o de la Garantía que el Proveedor deberá presentar. La contratante podrá rescindir administrativamente el contrato cuando el valor de las multas supere el monto de la Garantía de Cumplimiento de Contrato. En caso de no rescindir el contrato se seguirán aplicando las multas que fueron establecidas.

La aplicación de multas no libera al proveedor del cumplimiento de sus obligaciones contractuales.

2. La Contratante efectuará los pagos, dentro del plazo establecido en este apartado, sin exceder sesenta (60) días después de la presentación de una factura por el proveedor, y después de que la contratante la haya aceptado. Dicha aceptación o rechazo, deberá darse a más tardar en quince (15) días posteriores a su presentación.

3. De conformidad a las disposiciones del Decreto N° 7781/2006, del 30 de Junio de 2006 y modificatoria, en las contrataciones con Organismos de la Administración Central, el proveedor deberá habilitar su respectiva cuenta corriente o caja de ahorro en un Banco de plaza y comunicar a la Contratante para que ésta gestione ante la Dirección General del Tesoro Público, la habilitación en el Sistema de Tesorería (SITE).

Solicitud de suspensión de la ejecución del contrato

Si la mora en el pago por parte de la contratante fuere superior a sesenta (60) días, el proveedor, consultor o contratista, tendrá derecho a solicitar por escrito la suspensión de la ejecución del contrato por causas imputables a la contratante.

La solicitud deberá ser respondida por la contratante dentro de los 10 (diez) días calendario de haber recibido por escrito el requerimiento. Pasado dicho plazo sin respuesta se considerará denegado el pedido, con lo que se agota la instancia administrativa quedando expedita la vía contencioso administrativa.

Solicitud de Pago de Anticipo

El plazo dentro del cual se solicitará el anticipo será (en días corridos) de:

NO APLICA.

Con relación al Anticipo para las MIPYMES contemplado en el Art. 188 de la Ley de Presupuesto N° 7050/23, conforme a lo citado en la nota de comunicación del llamado a la DNCP, se indica que no se otorgará anticipo a ningún adjudicado.

1. El anticipo es la suma de dinero que se entrega al proveedor, consultor o contratista destinada al financiamiento de los costos en que este debe incurrir para iniciar la ejecución del objeto contractual. El mismo no constituye un pago por adelantado; debe estar amparado con una garantía correspondiente al cien por ciento de su valor y deberá ser amortizado durante la ejecución del contrato y durante la ejecución de contrato demostrar el debido uso. La Garantía de Anticipo deberá mantener su vigencia hasta su total amortización.

Los recursos entregados en calidad de anticipo no podrán destinarse a fines distintos a los relacionados con el objeto del contrato.

En caso de extensión de la Garantía de Anticipo, la misma deberá cubrir el saldo pendiente de amortización.

2. Si se establece en el SICP el otorgamiento de anticipos, no podrá superar en ningún caso el porcentaje establecido en la legislación vigente.

3. La solicitud de pago del anticipo deberá ser presentada por escrito, con la factura, el plan de inversiones y la Garantía de Anticipo.

4. El proveedor podrá remitir una comunicación por escrito a la contratante, en la cual informe que rechaza el anticipo previsto en el PBC. La falta de solicitud de anticipo en el plazo previsto en el PBC será considerado como un rechazo del mismo. En estos casos podrá darse inicio al cómputo de la ejecución contractual en las condiciones establecidas en el pliego de bases y condiciones.

5. El Pago del Anticipo debe ser total. En el caso que se realizare el pago de un porcentaje inferior al 100% del mismo, el proveedor podrá rechazarlo en el plazo de cinco (5) días hábiles mediante una nota de reclamo remitida a la Contratante. Transcurrido dicho plazo, se considerará que el Anticipo ha sido aceptado por el proveedor y podrá darse inicio al cronograma de ejecución contractual en las condiciones establecidas en el pliego de bases y condiciones.

6. En el caso de que el proveedor haya solicitado el anticipo en las condiciones establecidas en la presente cláusula y la convocante no ha procedido al pago, el oferente no está obligado a iniciar la ejecución del contrato hasta tanto el pago se haya efectuado de forma total o de acuerdo a lo dispuesto en el punto 5.

7. La amortización del anticipo se realizará de acuerdo con lo establecido en el contrato, en la proporción que éste indique.

8. Para la ejecución de esta garantía, especialmente cuando sea instrumentada a través de Póliza de Seguro de caución, será requisito que previamente el proveedor sea notificado del incumplimiento y la intimación de que se hará efectiva la ejecución del monto asegurado.

9. A menos que se indique otra cosa en este apartado, la Garantía de Anticipo será liberada por la contratante y devuelta al proveedor, a requerimiento de parte, a más tardar treinta (30) días contados a partir de la fecha de cumplimiento de las obligaciones del proveedor en virtud del contrato, pudiendo ajustarse por el saldo adeudado.

10. En el caso de rescisión o terminación anticipada del contrato, los proveedores o contratistas deberán reintegrar a la contratante el saldo por amortizar.

Reajuste

El precio del contrato estará sujeto a reajustes. La fórmula y el procedimiento para el reajuste serán los siguientes:

A solicitud por escrito del Proveedor, el precio de la oferta será reajutable en el siguiente caso:

Los precios ofertados estarán sujetos a reajustes (a petición de parte y por escrito), siempre y cuando: La inflación acumulada del Índice de Precios al Consumidor (IPC) desde el inicio del contrato o desde la fecha del último ajuste de precio sea igual o mayor al 15%. La fórmula de reajuste a ser utilizada en este caso es la siguiente:

$$\pi = (\text{IPC}(T) - \text{IPC}(T-n) / \text{IPC}(T-n)) \times 100$$

Donde

π = inflación acumulada desde el inicio del contrato o desde la fecha del último ajuste de precio.

$\text{IPC}(T)$ = IPC del mes anterior a la fecha en que se solicita el ajuste de precio.

$\text{IPC}(T-n)$ = IPC del mes en que se inició el contrato o del mes correspondiente al último ajuste de precio.

Los precios reajustados, solo tendrán incidencia sobre lo aun no ejecutado y no tendrán efecto retroactivo respecto a lo que haya sido ejecutado con anterioridad a la verificación del reajuste.

El Proveedor deberá solicitar el reajuste contractual por escrito a la Contratante como máximo dentro del mes siguiente al cual se produjo la variación. En caso que el pedido sea posterior, el reajuste será reconocido a partir de la fecha de

presentación de dicho pedido.

La Contratante dará curso al reajuste previa verificación de los requisitos exigidos y si dispone de suficiente disponibilidad presupuestaria.

No se reconocerán reajustes de precios si el servicio se encuentra con incumplimientos que impidan la ejecución contractual.

Porcentaje de multas

El valor del porcentaje de multas que será aplicado por el atraso en la entrega de los bienes, prestación de servicios será de:

0,333 %

La contratante podrá deducir en concepto de multas una suma equivalente al porcentaje del precio de entrega de los bienes atrasados, por cada día de atraso indicado en este apartado. La contratante podrá rescindir administrativamente el contrato cuando el valor de las multas supere el monto de la Garantía de Cumplimiento de Contrato.

La aplicación de multas no libera al proveedor del cumplimiento de sus obligaciones contractuales.

Tasa de interés por Mora

En caso de que la contratante incurriera en mora en los pagos, se aplicará una tasa de interés por cada día de atraso, del:

0,01

La mora será computada a partir del día siguiente del vencimiento del pago y no incluye el día en el que la contratante realiza el pago.

Si la Contratante no efectuara cualquiera de los pagos al proveedor en las fechas de vencimiento correspondiente o dentro del plazo establecido en la presente cláusula, la Contratante pagará al proveedor interés sobre los montos de los pagos morosos a la tasa establecida en este apartado, por el período de la demora hasta que haya efectuado el pago completo, ya sea antes o después de cualquier juicio.

Impuestos y derechos

En el caso de bienes de origen extranjero, el proveedor será totalmente responsable del pago de todos los impuestos, derechos, gravámenes, timbres, comisiones por licencias y otros cargos similares que sean exigibles fuera y dentro de la República del Paraguay, hasta el momento en que los bienes contratados sean entregados al contratante

En el caso de origen nacional, el proveedor será totalmente responsable por todos los impuestos, gravámenes, comisiones por licencias y otros cargos similares incurridos hasta el momento en que los bienes contratados sean entregados a la contratante.

El proveedor será responsable del pago de todos los impuestos y otros tributos o gravámenes con excepción de los siguientes:

No Aplica

Convenios Modificatorios

La Contratante podrá acordar modificaciones al contrato conforme al artículo N° 63 de la Ley N° 2051/2003.

1. Cuando el sistema de adjudicación adoptado sea de abastecimiento simultáneo las ampliaciones de los contratos se regirán por las disposiciones contenidas en la Ley N° 2051/2003, sus modificaciones y reglamentaciones, que para el efecto emita la DNCP.
2. Tratándose de contratos abiertos, las modificaciones a ser introducidas se regirán atendiendo a la reglamentación vigente.
3. La celebración de un convenio modificatorio conforme a las reglas establecidas en el artículo N° 63 de la Ley 2051/2003, que constituyan condiciones de agravación del riesgo cuando la Garantía de Cumplimiento de Contrato sea formalizada a través de póliza de caución, obliga al proveedor a informar a la compañía aseguradora sobre las modificaciones a ser realizadas y en su caso, presentar ante la contratante los endosos por ajustes que se realicen a la póliza original en razón al convenio celebrado con la contratante.

Limitación de responsabilidad

Excepto en casos de negligencia grave o actuación de mala fe, el proveedor no tendrá ninguna responsabilidad contractual de agravio o de otra índole frente a la contratante por pérdidas o daños indirectos o consiguientes, pérdidas de utilización, pérdidas de producción, o pérdidas de ganancias o por costo de intereses, estipulándose que esta exclusión no se aplicará a ninguna de las obligaciones del proveedor de pagar a la contratante las multas previstas en el Contrato.

Responsabilidad del proveedor

El proveedor deberá suministrar todos los bienes o servicios de acuerdo con las condiciones establecidas en el pliego de bases y condiciones.

Fuerza mayor

El proveedor no estará sujeto a la ejecución de su Garantía de Cumplimiento, liquidación por daños y perjuicios o terminación por incumplimiento en la medida en que la demora o el incumplimiento de sus obligaciones en virtud del contrato sea el resultado de un evento de Fuerza Mayor.

1. Para fines de esta cláusula, "Fuerza Mayor" significa un evento o situación fuera del control del proveedor que es imprevisible, inevitable y no se origina por descuido o negligencia del mismo. Tales eventos pueden incluir sin que éstos sean los únicos actos de la autoridad en su capacidad soberana, guerras o revoluciones, incendios, inundaciones, epidemias, pandemias, restricciones de cuarentena, y embargos de cargamentos.
2. El proveedor deberá demostrar el nexo existente entre el caso notorio y la obligación pendiente de cumplimiento. La fuerza mayor solamente podrá afectar a la parte del contrato cuyo cumplimiento imposible fue probado.
3. No se considerarán casos de Fuerza Mayor los actos o acontecimientos que hagan el cumplimiento de una obligación únicamente más difícil o más onerosa para la parte correspondiente.
4. Si se presentara un evento de Fuerza Mayor, el proveedor notificará por escrito a la contratante sobre dicha condición y causa, en el plazo de siete (7) días calendario a partir del día siguiente en que el proveedor haya tenido conocimiento del evento o debiera haber tenido conocimiento del evento. Transcurrido el mencionado plazo, sin que el proveedor o contratista haya notificado a la convocante la situación que le impide cumplir con las condiciones contractuales, no podrá invocar caso fortuito o fuerza mayor. Excepcionalmente, la convocante bajo su responsabilidad, podrá aceptar la notificación del evento de caso fortuito en un plazo mayor, debiendo acreditar el interés público comprometido.
5. La fuerza mayor debe ser invocada con posterioridad a la suscripción del contrato y con anterioridad al vencimiento del plazo de cumplimiento de las obligaciones contractuales.
6. A menos que la contratante disponga otra cosa por escrito, el proveedor continuará cumpliendo con sus obligaciones en virtud del contrato en la medida que sea razonablemente práctico, y buscará todos los medios alternativos de cumplimiento que no estuviesen afectados por la situación de fuerza mayor existente.

Causales de terminación del contrato

1. Terminación por Incumplimiento

a) La contratante, sin perjuicio de otros recursos a su disposición en caso de incumplimiento del contrato, podrá terminar el contrato, en cualquiera de las siguientes circunstancias:

- i. Si el proveedor no entrega parte o ninguno de los bienes dentro del período establecido en el contrato, o dentro de alguna prórroga otorgada por la contratante; o
- ii. Si el proveedor no cumple con cualquier otra obligación en virtud del contrato; o
- iii. Si el proveedor, a juicio de la contratante, durante el proceso de licitación o de ejecución del contrato, ha participado en actos de fraude y corrupción;
- iv. Cuando las multas por atraso superen el monto de la Garantía de Cumplimiento de Contrato;
- v. Por suspensión de los trabajos, imputable al proveedor o al contratista, por más de sesenta días calendarios, sin que medie fuerza mayor o caso fortuito;
- vi. En los demás casos previstos en este apartado.

2. Terminación por Insolvencia o quiebra

La Contratante podrá rescindir el contrato mediante comunicación por escrito al proveedor si éste se declarase en quiebra o en estado de insolvencia.

3. Terminación por conveniencia

a) La contratante podrá en cualquier momento terminar total o parcialmente el contrato por razones de interés público debidamente justificada, mediante notificación escrita al proveedor. La notificación indicará la razón de la terminación así como el alcance de la terminación con respecto a las obligaciones del proveedor, y la fecha en que se hace efectiva dicha terminación.

b) Los bienes que ya estén fabricados y estuviesen listos para ser enviados a la contratante dentro de los treinta (30) días siguientes a la fecha de recibo de la notificación de terminación del contrato deberán ser aceptados por la contratante de acuerdo con los términos y precios establecidos en el contrato. En cuanto al resto de los bienes la contratante podrá elegir entre las siguientes opciones:

- i. Que se complete alguna porción y se entregue de acuerdo con las condiciones y precios del contrato; y/o
- ii. Que se cancele la entrega restante y se pague al proveedor una suma convenida por aquellos bienes que hubiesen sido

parcialmente completados y por los materiales y repuestos adquiridos previamente por el proveedor.

Otras causales de terminación del contrato

Además de las ya indicadas en la cláusula anterior, otras causales de terminación de contrato son:

No Aplica

Resolución de Conflictos a través del Arbitraje

Las partes se someterán a Arbitraje:

No

En caso que la Convocante adopte el arbitraje como mecanismo de resolución de conflicto, la cláusula arbitral que regirá a las partes es la siguiente:

"Todas las controversias que deriven del presente contrato o que guarden relación con éste serán resueltas definitivamente por arbitraje, conforme con las disposiciones de la ley N° 2051/03 "De Contrataciones Públicas", de la ley N° 1879/02 "De arbitraje y mediación" y las condiciones del Contrato. El procedimiento arbitral se llevará a cabo ante el Centro de Arbitraje y Mediación del Paraguay (en adelante, "CAMP"). El tribunal estará conformado por tres árbitros designados de la lista del cuerpo arbitral del CAMP, que decidirá conforme a derecho, siendo el laudo definitivo y vinculante para las partes. Se aplicará el reglamento respectivo y demás disposiciones que regule dicho procedimiento al momento de ser requerido, declarando las partes conocer y aceptar los vigentes, incluso en orden a su régimen de gastos y costas, considerándolos parte integrante del presente Contrato. Para la ejecución del laudo arbitral, o para dirimir cuestiones que no sean arbitrables, las partes se someterán a la jurisdicción de los tribunales de la ciudad de Asunción, República del Paraguay".

Fraude y Corrupción

1. La Convocante exige que los participantes en los procedimientos de contratación, observen los más altos niveles éticos, ya sea durante el proceso de licitación o de ejecución de un contrato. La Convocante actuará frente a cualquier hecho o reclamación que se considere fraudulento o corrupto.
2. Si se comprueba que un funcionario público, o quien actúe en su lugar, y/o el oferente o adjudicatario propuesto en un proceso de contratación, hayan incurrido en prácticas fraudulentas o corruptas, la Convocante deberá:
 - (i) En la etapa de oferta, se descalificará cualquier oferta del oferente y/o rechazará cualquier propuesta de adjudicación relacionada con el proceso de adquisición o contratación de que se trate; y/o
 - (ii) Durante la ejecución del contrato, se rescindirá el contrato por causa imputable al proveedor
 - (iii) Se remitirán los antecedentes del oferente o proveedor directamente involucrado en las prácticas fraudulentas o corruptivas, a la Dirección Nacional de Contrataciones Públicas, a los efectos de la aplicación de las sanciones previstas.
 - (iv) Se presentará la denuncia penal ante las instancias correspondientes si el hecho conocido se encontrare tipificado en

la legislación penal.

Fraude y corrupción comprenden actos como:

- (i) Ofrecer, dar, recibir o solicitar, directa o indirectamente, cualquier cosa de valor para influenciar las acciones de otra parte;
- (ii) Cualquier acto u omisión, incluyendo la tergiversación de hechos y circunstancias, que engañen, o intenten engañar, a alguna parte para obtener un beneficio económico o de otra naturaleza o para evadir una obligación;
- (iii) Perjudicar o causar daño, o amenazar con perjudicar o causar daño, directa o indirectamente, a cualquier parte o a sus bienes para influenciar las acciones de una parte;
- (iv) Colusión o acuerdo entre dos o más partes realizado con la intención de alcanzar un propósito inapropiado, incluyendo influenciar en forma inapropiada las acciones de otra parte.
- (v) Cualquier otro acto considerado como tal en la legislación vigente.

3. Los oferentes deberán declarar que por sí mismos o a través de interpósita persona, se abstendrán de adoptar conductas orientadas a que los funcionarios o empleados de la convocante induzcan o alteren las evaluaciones de las propuestas, el resultado del procedimiento u otros aspectos que les otorguen condiciones más ventajosas con relación a los demás participantes (Declaratoria de Integridad).

MODELO DE CONTRATO

Este modelo de contrato, constituye la proforma del contrato a ser utilizado una vez adjudicado al proveedor y en los plazos dispuestos para el efecto por la normativa vigente.

EL MODELO DE CONTRATO SE ENCUENTRA EN UN ARCHIVO ANEXO A ESTE DOCUMENTO.

FORMULARIOS

Los formularios dispuestos en esta sección son los estándar a ser utilizados por los potenciales oferentes para la preparación de sus ofertas.

ESTA SECCIÓN DE FORMULARIOS SE ENCUENTRA EN UN ARCHIVO ANEXO A ESTE DOCUMENTO, DEBIENDO LA CONVOCANTE MANTENERLO EN FORMATO EDITABLE A FIN DE QUE EL OFERENTE LO PUEDA UTILIZAR EN LA PREPARACION DE SU OFERTA.

