

*Visión: ser una institución técnica e independiente que desarrolle una gestión eficiente y creíble, basada en la excelencia de sus talentos y reconocida en el ámbito nacional e internacional, orientada a preservar el valor de la moneda y la eficacia, integridad y estabilidad del sistema financiero.*



## DICTAMEN TÉCNICO EN EL CUAL SE SUSTENTAN LAS ESPECIFICACIONES TÉCNICAS REQUERIDAS EN EL PROCEDIMIENTO DE CONTRATACIÓN

En cumplimiento del artículo 12 de la Resolución DNCP N° 453/24, en virtud del cual se solicita la emisión de dictamen técnico en el cual se sustenten las especificaciones técnicas requeridas en el procedimiento de contratación, refrendado por el responsable del área requirente o del técnico que las recomendó; se emite el siguiente dictamen en los siguientes términos:

### INFORMACIÓN BÁSICA DE LA CONVOCATORIA

- A. DENOMINACIÓN DE LA CONVOCATORIA:**  
**LICITACIÓN PÚBLICA NACIONAL N° 28/2024 – SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE CORTAFUEGOS DE APLICACIONES WEB – ID N° 443917**
- B. MONTO TOTAL DEL PAC:** **G. 1.300.000.000.**
- C. ÁREA TÉCNICA REQUIRENTE DEL PROCESO:** **Departamento de Ciberseguridad.**
- D. FUNCIONARIO/S RESPONSABLE/S DESIGNADO/S PARA LA ADMINISTRACION DEL CONTRATO, ENCARGADO/S DE LA CARGA EN EL SISTEMA DE INFORMACIÓN DE CONTRATACIONES PÚBLICAS DE LOS DOCUMENTOS CONTRACTUALES Y DE LOS INDICADORES DE CUMPLIMIENTO:**

#### TITULAR:

- Nombre y apellido: **Aditardo Vazquez**
- Cédula de Identidad: **1.624.369.**
- Fecha de nacimiento: **07/06/1983**
- Número telefónico de contacto: **(595 21) 619 2696**
- Cargo en el área requirente: **Director del Departamento de Ciberseguridad**

#### AUXILIAR:

- Nombre y apellido: **Miguel Toffoletti**
- Cédula de Identidad: **4.293.038.**
- Fecha de nacimiento: **16/07/1987**
- Número telefónico de contacto: **(595 21) 619 2294.**
- Cargo en el área requirente: **Jefe de División Operaciones de Ciberseguridad**

*Visión: ser una institución técnica e independiente que desarrolle una gestión eficiente y creíble, basada en la excelencia de sus talentos y reconocida en el ámbito nacional e internacional, orientada a preservar el valor de la moneda y la eficacia, integridad y estabilidad del sistema financiero.*



## E. MODALIDAD DE LA CONTRATACIÓN

...X... CONTRATO CERRADO

..... CONTRATO ABIERTO

### SECCIÓN I - DATOS DE LA CONVOCATORIA

➤ **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.*

...X... APLICA

..... NO APLICA

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

...X.. SI (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).

..... NO

➤ **Visita al sitio de ejecución del contrato:**

...X... NO APLICA

➤ **Autorización del Fabricante:**

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

...X... APLICA

REQUISITO: El oferente deberá presentar fotocopia simple del documento vigente que acredite fehacientemente que el mismo es Fabricante y/o Representante Oficial y/o Distribuidor y/o Sub-Distribuidor y/o Partner Autorizado para el Paraguay de la solución objeto del servicio de suscripción; 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.

➤ **Muestras:**

...X... NO APLICA

➤ **Periodo de validez de la Garantía de los bienes:**

...X... APLICA El periodo de validez de la Garantía de los bienes/servicios será el siguiente:

El proveedor deberá emitir una Garantía de Buen Servicio y Calidad, mediante una nota en carácter de declaración jurada a nombre del Banco Central del Paraguay, en virtud de la cual garantice, por todo el plazo de prestación del servicio de suscripción contratado, que correrá a su cargo, por cuenta propia y sin costo para la Convocante, las reposiciones, sustituciones, reparaciones y/o modificaciones que correspondan, cuando se observasen fallas y/o deficiencias, por causas que le fueran imputables.



## SECCIÓN II - REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN

### ➤ Experiencia requerida

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

- a. Demostrar una antigüedad mínima de 5 (cinco) años de existencia legal (inclusive para las firmas unipersonales).
- b. Demostrar experiencia en la prestación de servicios de suscripción a soluciones de protección de aplicaciones web y/o provisión de soluciones de ciberseguridad de protección de aplicaciones web, dentro del periodo comprendido entre los años 2019 a 2024, con la documentación requerida en los inc. b) y c) del siguiente apartado “Requisitos documentales para la evaluación de la experiencia”  
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 finalizado/s, y/o facturas, y/o recepción/es final/es de haber prestado servicios de suscripción a soluciones de protección de aplicaciones web y/o provisión de soluciones de ciberseguridad de protección de aplicaciones web, a Instituciones Públicas y/o Privadas, dentro del periodo comprendido entre los años 2019 a 2024, cuyos montos sumados representen un monto igual o superior al 50% del monto total ofertado en la presente licitación. Podrán presentarse la cantidad de fotocopia/s de contrato/s finalizado/s, y/o factura/s y/o recepciones finales que fueren necesarias para acreditar el monto solicitado, siempre y cuando dichas prestaciones de servicios y/o provisiones hayan sido realizadas dentro del periodo mencionado.
c) Fotocopia simple de referencias satisfactorias de clientes finales, como mínimo 3 (tres), formalizadas por documentos que contengan la debida identificación y suscripción del emisor, de haber prestado servicios de suscripción a soluciones de protección de aplicaciones web y/o en la provisión de soluciones de ciberseguridad de protección de aplicaciones web, dentro del periodo comprendido entre los años 2019 al 2024, 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:*

- El Oferente deberá contar con al menos dos técnicos certificados por la marca ofertada.

### ▪ Requisito documental para evaluar la capacidad técnica

a) Nota en carácter de Declaración Jurada en la cual el Oferente manifieste que cuenta con el personal técnico capacitado de acuerdo a lo establecido en las Especificaciones técnicas, a efectos de la instalación, configuración y actualización de la solución objeto del servicio de suscripción.
b) Fotocopia simple de documento emitido por el fabricante que acredite que al menos 2 (dos) técnicos propuestos poseen una certificación técnica de la marca objeto del servicio de suscripción.
c) Catálogos o impresos descriptivos de la solución objeto del servicio de suscripción, 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 esta.

*Visión: ser una institución técnica e independiente que desarrolle una gestión eficiente y creíble, basada en la excelencia de sus talentos y reconocida en el ámbito nacional e internacional, orientada a preservar el valor de la moneda y la eficacia, integridad y estabilidad del sistema financiero.*



d) Nota en carácter de declaración jurada en la cual se detallen las especificaciones técnicas de la solución objeto del servicio de suscripción, con la inclusión de las descripciones y demás requisitos exigidos en la Sección Especificaciones Técnicas y Suministros Requeridos.	i)
e) Garantía de Buen Funcionamiento y Calidad, mediante una nota en carácter de declaración jurada a nombre de la Convocante, en virtud de la cual el oferente garantice, por todo el plazo de prestación del servicio de suscripción contratado, que correrá a su cargo, por cuenta propia y sin costo para la Convocante, las reposiciones, sustituciones, reparaciones y/o modificaciones que correspondan, cuando se observasen fallas y/o deficiencias, por causas que le fueran imputables.	
f) Nota en carácter de Declaración jurada, por la cual el Oferente manifieste que se compromete a brindar la actualización y la garantía del fabricante de la solución objeto del servicio de suscripción durante todo el plazo de la prestación.	
g) Nota en carácter de Declaración jurada, por la cual el Oferente se compromete a asegurar el soporte y mantenimiento local (proveedor) y del fabricante durante todo el plazo de prestación del servicio de suscripción.	
h) Documento vigente que acredite fehacientemente que el Oferente es Fabricante y/o Representante Oficial y/o Distribuidor Oficial y/o Partner Autorizado por el mismo para el Paraguay de la solución objeto del servicio de suscripción, ya sea mediante documento emitido por la firma autorizante o mediante la presentación del Formulario incluido en la Sección Formularios debidamente suscripto por la firma autorizante.	
➤ <b>Otros criterios que la convocante requiera</b>	

...X... NO APLICA

### SECCIÓN III- SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS

#### ➤ 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, de acuerdo a las necesidades de la Institución y con aprobación de la máxima autoridad. Los nombres de las personas requerientes de la contratación obran en los registros del BCP y en el Dictamen Técnico publicado en el SICP.

• La necesidad que se pretende satisfacer mediante la contratación realizada radica en:

El Banco Central del Paraguay es una entidad crítica para la economía del país y está expuesto a diversos riesgos de seguridad, incluyendo ataques de denegación de servicio, inyección de código malicioso y robo de datos. Uno de los principales riesgos de seguridad son las vulnerabilidades en las aplicaciones web que publica el Banco (página web institucional, RCF, SIVEF, SICEX, SEOG, etc.), y que pueden ser explotadas por los atacantes para acceder a datos sensibles internos y afectar la disponibilidad de los sistemas.

Para mitigar estos riesgos de seguridad, se propone la suscripción a una solución de cortafuegos de aplicaciones web (WAF). El WAF es una solución de seguridad que permite proteger las aplicaciones web contra diversos tipos de ataques.

• 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 especificaciones técnicas establecidas se justifican en las necesidades actuales de la Institución, en su infraestructura y en el conocimiento del área técnica.

#### ➤ Especificaciones técnicas

##### GENERALIDADES:

##### ▪ **MÓDULO DE OFERTAS ELECTRÓNICAS:**

*De acuerdo a lo establecido en la reglamentación de la DNCP vigente:*

▪ 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.

**Visión:** ser una institución técnica e independiente que desarrolle una gestión eficiente y creíble, basada en la excelencia de sus talentos y reconocida en el ámbito nacional e internacional, orientada a preservar el valor de la moneda y la eficacia, integridad y estabilidad del sistema financiero.



- 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.

▪ **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 Unidad Operativa de Contratación dispondrá las modificaciones de los aspectos establecidos en la convocatoria y/o en las bases de licitación y/o en el SICP cuando se refieran a fechas y/o a informaciones y/o a los documentos del llamado, suscribiendo, cuando corresponda, y difundiendo en el SICP la Adenda respectiva; con excepción de las modificaciones relativas a las especificaciones técnicas y al monto de los precios referenciales, las cuales deberán ser autorizadas por el Gerente General del BCP mediante adendas verificadas por el área técnica y/u otras instancias administrativas y a ser difundidas por la UOC.

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.

▪ **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.**

**ESPECIFICACIONES TECNICAS**

Requisito	Detalle y definiciones	Exigido	Ofrecido (Campo a ser completado por el oferente)
<b>ÍTEM N° 1 – SERVICIO DE SUSCRIPCIÓN A SOLUCIÓN DE CORTAFUEGOS DE APLICACIONES WEB</b>			
<b>1. Descripción</b>			
1.1	Indicar Marca	SI	
1.2	Indicar Solución / Modelo objeto del servicio de suscripción	SI	
<b>2. Generalidades</b>			
2.1	Debe proveer un servicio de suscripción a una solución unificada en la nube para DNS, WAF, Anti-DDOS, CDN desde una misma plataforma.	SI	
2.2	La solución deberá proveer aceleración de aplicaciones Web (CDN)	SI	
2.3	La solución deberá contar con gestión de DNS	SI	
2.4	La solución deberá contar con Web Application and API Protección (WAAP)	SI	

**Visión:** ser una institución técnica e independiente que desarrolle una gestión eficiente y creíble, basada en la excelencia de sus talentos y reconocida en el ámbito nacional e internacional, orientada a preservar el valor de la moneda y la eficacia, integridad y estabilidad del sistema financiero.



2.5	La solución deberá contar con red de entrega de contenidos (CDN)	SI	
2.6	La solución deberá contar con protección contra robots (BOTS)	SI	
2.7	La solución debe tener una red global con topología Anycast.	SI	
2.8	El fabricante de la solución ofertada deberá contar con al menos 200 puntos de presencia (PoPs) a nivel global y al menos 15 puntos de presencia en Latinoamérica, incluyendo al menos un punto de presencia en Paraguay	SI	
2.9	La solución debe contar con APIs para cambios de configuración y para monitoreo	SI	
2.10	La plataforma debe aplicar modificaciones en un tiempo máximo de 30 segundos	SI	
2.11	La plataforma debe soportar tráfico mensual a ser controlado por la solución de al menos 100Gb	SI	
2.12	Debe soportar HTTP/2, IPv4, IPv6	SI	
2.13	Se debe asegurar al menos 1 (uno) dominio principal y 20 (veinte) subdominios	SI	
<b>3. Reglas</b>			
3.1	La plataforma debe permitir al menos 100 reglas que permitan hacer ajustes a las consultas o respuestas web.	SI	
3.2	Debe soportar Rewrite URL rules	SI	
3.3	Debe permitir la modificación de HTTP request header	SI	
3.4	Debe permitir la modificación de HTTP response header	SI	
3.5	Debe permitir URL normalization	SI	
3.6	Debe permitir URL forwarding (Single and Bulk)	SI	
3.7	Debe contar con reglas de acceso con las opciones de IP, rango de IP, País, ASN	SI	
<b>4. SSL</b>			
4.1	Debe incluir el certificado para dominio raíz y el primer nivel de subdominios	SI	
4.2	Debe permitir utilizar certificado SSL propio.	SI	
4.3	Debe soportar TLS 1.0, 1.1, 1.2 y 1.3	SI	
4.4	Debe ser compatible con los cipher suites de TLS 1.3, TLS_AES_256_GCM_SHA384 y TLS_AES_128_GCM_SHA256.	SI	
4.5	Debe ser compatible con los cipher suites de TLS 1.2, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 y TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.	SI	
4.6	Debe ser compatible con los cipher suites de TLS 1.1, incluidos los más seguros, como ECDHE-RSA-AES128-SHA y AES256-SHA.	SI	
4.7	Debe ser compatible con los cipher suites de TLS 1.0, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA y TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	SI	
<b>5. WAF</b>			
5.1	Debe de disponer de reglas dinámicas preestablecidas para bloquear amenazas encontradas en la OWASP top 10.	SI	
5.2	Debe permitir la creación de por lo menos 1000 reglas WAF	SI	
5.3	Debe permitir la utilización de expresiones regulares	SI	
5.4	Debe permitir crear reglas de limitación de velocidad, al menos 50	SI	
5.5	Debe permitir utilizar CAPTCHA o JavaScript para validar que los visitantes utilicen un navegador legítimo	SI	
5.6	Debe permitir la mitigación avanzada de Bots utilizando Análisis de comportamiento, Machine Learning y Fingerprinting	SI	
5.7	Debe de disponer reglas pre establecidas para tener protección inmediata. Estas reglas deben ser actualizadas regularmente y debe ofrecer protección contra amenazas de día 0.	SI	
5.8	Debe tener la función de verificación automatizada de credenciales robadas	SI	
5.9	Debe proporcionar reglas de seguridad contra SQL Injection	SI	
5.10	Debe proporcionar reglas de seguridad contra Cross-site Scripting	SI	
5.11	Debe tener la función de bloquear, generar logs, de agregar un header HTTP, un reto interactivo, si se detecta que se utiliza una credencial robada	SI	
<b>6. DNS</b>			
6.1	La solución debe garantizar a través de DNSSEC que el tráfico sea dirigido de manera segura a los servidores correctos.	SI	
6.2	Debe poder utilizarse como DNS autoritativo	SI	
6.3	Debe proporcionar la publicación del servicio DNS global por medio de Anycast	SI	
6.4	Debe permitir la gestión de una cantidad ilimitada de registros DNS, con los siguientes tipos: A, CNAME, MX, TXT, SPF, AAAA, NS, SRV, LOC y CAA.	SI	
6.5	Debe permitir realizar análisis al servicio de DNS considerando lo siguiente: Datos históricos de las consultas realizadas al DNS con un periodo de al menos 30 días atrás. Filtrar las consultas de DNS a través de: código de respuesta, centro de datos, tipo de consulta, día de la semana o tiempo de respuesta medio. Visualización del origen de las consultas DNS válidas y no válidas	SI	
6.6	Debe poder utilizarse como DNS no autoritativo utilizando registros CNAME	SI	

**Visión:** ser una institución técnica e independiente que desarrolle una gestión eficiente y creíble, basada en la excelencia de sus talentos y reconocida en el ámbito nacional e internacional, orientada a preservar el valor de la moneda y la eficacia, integridad y estabilidad del sistema financiero.



<b>7. Balanceo de carga</b>			
7.1	Debe poder balancear la carga de al menos cuatro (4) servidores (Origin), estos deben de poder organizarse en grupos (Pools)	SI	
7.2	Debe permitir el monitoreo de los servicios utilizando las opciones de protocolos HTTP, HTTPS, TCP, ICMP, SMTP	SI	
7.3	Debe poder monitorear la disponibilidad del servicio por "path" y por puerto	SI	
7.4	El intervalo de monitoreo de servicios debe ser de 10 segundos o menos	SI	
<b>8. DDOS</b>			
8.1	Debe proveer protección contra Ataques volumétricos de capa 3/4/7 del modelo OSI	SI	
8.2	Debe ofrecer mitigación de ataques DDoS ilimitada	SI	
8.3	Debe disponer de un grupo de reglas preconfiguradas para evitar ataques DDoS conocidos de capa 3 y 4 del modelo OSI	SI	
8.4	Debe proveer protección contra vectores de ataque como: TCP SYN floods, TCP SYN-ACK reflection attack, ACK floods, ICMP flood attack, SNMP flood attack, Out of state TCP attacks, DNS amplification attack, DNS NXDOMAIN flood, DNS flood attack, UDP flood attack, Mirai, Variantes de Mirai de capa 3/4, entre otros.	SI	
8.5	Debe proteger contra vectores de ataque de capa 7 (HTTP/HTTPS) como: HTTP flood attack, HULK, Slowloris, LOIC, Mirai, ataques HTTP variantes Mirai, entre otros.	SI	
8.6	Debe soportar reglas de limitaciones de velocidad para proteger contra ataques de fuerza bruta	SI	
<b>9. Rendimiento</b>			
9.1	Debe contar con CDN con punto de presencia (PoP) en Paraguay	SI	
9.2	Debe proveer almacenamiento en caché del contenido estático	SI	
9.3	Debe proporcionar disponibilidad de las partes estáticas del contenido del sitio web, incluso cuando éste se encuentre sin disponibilidad por un tiempo	SI	
9.4	Debe soportar un TTL mínimo configurable a 1 segundo	SI	
9.5	Debe tener la capacidad de definir rangos de direcciones IP prioritarias	SI	
9.6	Debe proveer enrutamiento basado en geolocalización	SI	
9.7	Debe proveer limpieza de todo el caché almacenado en la red de entrega de contenidos o depuración de un archivo específico en menos de 30 segundos por medio de consola de administración de usuario o por medio de AP	SI	
9.8	Debe tener la capacidad de adaptar el tamaño de las imágenes a diferentes tipos de dispositivos	SI	
<b>10. Administración</b>			
10.1	Debe disponer de un panel de control Web	SI	
10.2	Debe permitir utilizar autenticación de doble Factor	SI	
10.3	Debe soportar el almacenamiento de logs por al menos 30 días.	SI	
10.4	Debe permitir generar reportes en línea que incluyan: análisis de tráfico, solicitudes web y amenazas detectadas hacia los distintos sitios web gestionados y con una periodicidad mínima de recolección de datos de 1 minuto.	SI	
10.5	Debe permitir la configuración desde el Dashboard o vía API	SI	
10.6	Integración con soluciones SIEM implementadas actualmente.	SI	
10.7	Debe soportar el manejo de roles de usuarios	SI	
<b>11. Certificaciones</b>			
11.1	El fabricante de la solución ofertada deberá contar mínimamente con las siguientes certificaciones: PCI-DSS nivel 1 SOC 2 ISO/IEC 27001:2013 (Gestión de seguridad de la información) ISO 27701:2019 (Gestión de privacidad de la información)	SI	
<b>12. Soporte</b>			
12.1	Debe incluir el soporte técnico del tipo 24/7 tanto por parte del fabricante como por parte del Proveedor durante 24 meses	SI	
12.2	El Proveedor deberá contar con al menos 2 técnicos con una antigüedad mínima de 6 meses en la empresa, los cuales deberán estar certificados por la marca de la solución ofertada.	SI	
12.3	Se debe incluir soporte telefónico para casos de Emergencia	SI	
12.4	Debe cumplir con SLA de respuesta técnica: -Crítico: El soporte debe asistir al cliente en un tiempo menor a 2 horas ya sea de forma presencial o remota de acuerdo a la necesidad de la contratante. -No Crítico: El soporte debe asistir al cliente en un tiempo menor a 4 horas ya sea de forma presencial o remota de acuerdo a la necesidad de la contratante. La definición respecto al nivel de criticidad será determinada exclusivamente por el BCP en la solicitud de soporte. El Proveedor facilitará el nombre, número telefónico y correo electrónico del contacto para gestionar los incidentes críticos y no críticos.	SI	

**Visión:** ser una institución técnica e independiente que desarrolle una gestión eficiente y creíble, basada en la excelencia de sus talentos y reconocida en el ámbito nacional e internacional, orientada a preservar el valor de la moneda y la eficacia, integridad y estabilidad del sistema financiero.



12.5	En cuanto a los acuerdos de nivel de servicio (ANSs) se deberá tener una disponibilidad del servicio del 100%.	SI	
12.6	El BCP debe recibir alertas, mensajes o noticias sobre las actualizaciones del servicio durante el periodo contratado.	SI	
<b>13. Documentación y entrenamiento</b>			
13.1	El fabricante deberá proveer acceso a documentación en línea	SI	
13.2	El fabricante deberá proveer acceso a talleres de formación en línea para al menos 5 personas del contratante	SI	
<b>14. Suscripción</b>			
14.1	Se debe incluir la suscripción a la solución para cumplir con lo requerido por un periodo de 24 meses.	SI	
<b>15. Implementación y capacitación</b>			
15.1	Se debe incluir la implementación, configuración y monitoreo de la solución; así como la capacitación al personal designado por el área técnica administradora del Contrato del BCP para la gestión de la herramienta.	SI	

**CONDICIONES GENERALES:**

**Compromiso de Confidencialidad:** el personal contratado 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 de la Sección Formularios Adicionales. 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 los mismos.

**Soporte Técnico:** El Proveedor deberá disponer de los canales de solicitud habilitados para el soporte, consistentes en dos números de contacto y cuentas de correo electrónico para la gestión de los reclamos o cambios requeridos. En ese sentido, el Proveedor una vez adjudicado, deberá detallar los siguientes datos: Nombres y apellidos, cargos, correos corporativos y números de teléfono de línea fija y móvil de los responsables del servicio de soporte técnico incluyendo una matriz de escalamiento. El BCP designará el equipo de trabajo que acompañará la implementación y/o soporte de la solución

Ante cada notificación por parte de la contratante, el Proveedor deberá realizar y presentar al BCP un informe que contendrá como mínimo la siguiente información: descripción detallada del problema, su causa y solución propuesta, personal que se asignó a la resolución de éste, problemas que se presentaron durante la resolución, documentación de los cambios realizados, recomendaciones, fecha y hora de resolución. El proveedor deberá garantizar durante la vigencia del contrato, que la solución se encuentre actualizada en su última versión estable y con los últimos parches de seguridad aplicados correctamente.

**Planificación y documentación del Proyecto:** el Proveedor deberá presentar una documentación con diagramas, configuraciones necesarias y otros detalles relevantes, además de un cronograma de trabajo para su implementación antes del inicio de los trabajos. Una vez finalizada la implementación, el proveedor deberá presentar un documento en el cual se detalle todos los datos necesarios como diagrama de implementación, URLs, direcciones IP, credenciales de usuario y de sistema, configuraciones y otros.

**Informes:** 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).

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

**Lugar y Horario de la prestación de los servicios y/o soportes:** se podrá realizar de forma remota, a través de herramientas tecnológicas tales como Microsoft Teams, o similares; o de forma presencial en el Edificio BCP, sito en la Av. Federación Rusa y Av. Augusto Roa Bastos, cuando el área administradora del contrato (Departamento de Ciberseguridad del BCP) lo requiera; preferentemente en el horario de lunes a viernes de 08:00 a 16:00 horas. En caso de necesidad la convocante podrá solicitar asistencia fuera del horario ordinario de trabajo o en días no laborables.

➤ **Plan de entrega de los bienes:** NO APLICA

➤ **Plan de entrega de los servicios:** APLICA

➤

Ítems	Descripción del servicio	Cantidad	Unidad de medida	Lugar y horario de prestación de los servicios	Plazo de prestación/ejecución de los servicios	Plazo de vigencia del Contrato
De acuerdo a la Lista de Precios publicada	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	La prestación de los servicios y/o soportes se podrán realizar de forma remota, a través de herramientas tecnológicas tales como Microsoft Teams, o	El plazo total de prestación del servicio será de 24 meses, contados a partir de la fecha a ser consignada al efecto en la Orden de Inicio del Servicio, que	El plazo de vigencia del Contrato será a partir de la fecha a ser consignada en la Orden de Inicio del Servicio que será emitida por el área

**Visión:** ser una institución técnica e independiente que desarrolle una gestión eficiente y creíble, basada en la excelencia de sus talentos y reconocida en el ámbito nacional e internacional, orientada a preservar el valor de la moneda y la eficacia, integridad y estabilidad del sistema financiero.



en el SICP				similares; o de forma presencial cuando el área administradora del contrato (Departamento de Ciberseguridad del BCP) lo requiera en el Edificio BCP, sito en la Av. Federación Rusa y Av. Augusto Roa Bastos, preferentemente en el horario de lunes a viernes de 08:00 a 16:00 horas.	será emitida por el área administradora del Contrato dentro de los 10 (diez) días hábiles siguientes a la suscripción del Contrato.	administradora del Contrato dentro de los 10 (diez) días hábiles siguientes a la suscripción del Contrato hasta el cumplimiento total de las obligaciones contractuales.
---------------	--	--	--	--	---	--

➤ **Otras aclaraciones:**

a) FORMA DE PAGO ESPECÍFICA.

...X... APLICA.

Los pagos se realizarán de la siguiente forma:

- ...X... APLICA. Detallar: MENSUAL

.....NO APLICA.

b) ANTICIPO.

..... APLICA. Detallar porcentaje y justificación: .....

...X....NO APLICA.

c) COMPROMISO DE CONFIDENCIALIDAD:

...X... APLICA.

.....NO APLICA.

**FIRMA DEL RESPONSABLE DEL ÁREA TÉCNICA:**