ANEXO II

ESPECIFICACIONES TÉCNICAS

ADITIVO 1

Contratación de servicios de Protección de Aplicaciones Web y APIs (WAAP) y Content Delivery Network (CDN) - Cloudflare

1. OBJETO

Contratación de servicios de Protección de Aplicaciones Web y APIs (WAAP) y Content Delivery Network (CDN), provistos mediante la plataforma tecnológica de la marca Cloudflare, por un periodo de treinta y seis (36) meses, conforme a las condiciones, cantidades y requisitos establecidos en el presente documento.

2. CARACTERÍSTICAS TÉCNICAS

2.1. La solución deberá estar basada en la plataforma Cloudflare, operando sobre su red global Anycast, integrada de forma nativa en todos sus puntos de presencia y sin depender de servicios de terceros.

a) Content Delivery Network (CDN).
b) Web Application Firewall and API Protection (WAAP).
c) Protección contra ataques de denegación de servicio distribuido (DDoS) a nivel de capa 7 (L7), con una capacidad de red del fabricante igual o superior a 40 Tbps, distribuida de forma nativa en todos los puntos de presencia, sin depender de centros de depuración externos o diferenciados de la infraestructura de entrega de contenido
d) Integración nativa con sistemas de monitoreo y correlación de eventos de seguridad (SIEM).
e) Servicio de DNS autoritativo.
f) Servicios de SSL/TLS y gestión integral de certificados digitales.
g) Mitigación y gestión avanzada de bots.

2.2. La solución deberá contar con una **única plataforma de gestión web**, accesible sin requerir la instalación de equipamiento adicional, tales como appliances físicos o virtuales, en la infraestructura de la ITAIPU.

2.3. Los servicios de CDN y WAAP deberán implementarse mediante la infraestructura DNS gestionada por Cloudflare, incluyendo proxy reverso y aceleración desde su red global, contemplando la **migración, delegación y operación de 4 zonas DNS**, incluidos los subdominios de estos hacia la **plataforma adquirida**, la cual deberá asumir la provisión y gestión integral de dichos servicios.

2.4. Todo el tráfico deberá ser medido exclusivamente en base al tráfico legitimo efectivamente entregado a los usuarios finales, expresado en GB o TB. La métrica deberá ser declarada explícitamente en **el plan de implementación que deberá presentar el CONTRATISTA** y permanecer fija durante toda la vigencia del contrato, sin posibilidad de cambio unilateral

2.5. El servicio contratado deberá incluir una **capacidad de tráfico legítimo efectivamente entregado de hasta 6 (seis) TB (Terabytes) por mes**, de forma **agregada para la totalidad de los dominios mencionados** en el punto 2.3, durante un **período total de 36 (treinta y seis) meses** de vigencia contractual.

2.6. En ninguna circunstancia el **consumo de tráfico que supere el volumen mensual indicado** podrá generar **costos adicionales, cargos por sobreconsumo, recargos automáticos, ajustes**

tarifarios, penalidades, facturación posterior ni revisiones económicas para la ITAIPU Binacional, durante toda la vigencia del contrato.

2.7. No se aceptarán cláusulas de "fair use", uso razonable, limitaciones cualitativas o cuantitativas, ni condiciones comerciales o técnicas que habiliten al proveedor a:

a) Restringir, degradar o condicionar el servicio por volumen de tráfico.
b) Solicitar migraciones forzadas de plan.
c) Requerir renegociaciones contractuales ante incrementos de tráfico legítimos o derivados de eventos de seguridad (incluidos ataques DDoS).

2.8. El tráfico generado como consecuencia de eventos de seguridad, ataques de denegación de servicio (DDoS), actividad maliciosa o automatizada, deberá considerarse incluido dentro del servicio, sin impacto económico alguno para la ITAIPU Binacional.

2.9. El CONTRATISTA deberá detallar de forma clara y verificable la métrica de medición utilizada, demostrando su correspondencia directa con el volumen efectivamente entregado, conforme a lo establecido en el ítem 2.4. Dicha métrica deberá ser transparente, auditable y accesible para la ITAIPU BINACIONAL.

2.10. La métrica de medición aplicada por el CONTRATISTA deberá considerar exclusivamente el contenido legítimo efectivamente entregado a ITAIPU BINACIONAL. En ningún caso se aceptarán cargos, cómputos o imputaciones de tráfico derivados de:

a) Ataques de cualquier naturaleza (incluidos DDoS, floods o escaneos automatizados).
b) Tráfico malicioso o no autorizado.
c) Tráfico interno entre nodos, servidores o capas de la infraestructura CDN del CONTRATISTA.

2.11. El CONTRATISTA deberá implementar mecanismos de mitigación de accesos indebidos y tráfico malicioso en el origen o en el borde de la red, con el fin de evitar que dichos intentos sean contabilizados dentro del volumen mensual contratado, garantizando que únicamente el tráfico legítimo sea considerado a efectos de medición y facturación.

2.12. El CONTRATISTA deberá ofrecer un servicio de DNS autoritativo en la nube, integrado a la plataforma, con el objetivo de:

a) Acelerar la resolución de nombres de dominio.
b) Garantizar alta disponibilidad y resiliencia.
c) Proteger los servicios de ITAIPU BINACIONAL contra ataques dirigidos a la infraestructura DNS, incluyendo ataques de denegación de servicio y manipulación de consultas.

2.13. El servicio de DNS autoritativo deberá soportar e implementar DNSSEC (Domain Name System Security Extensions), conforme a las mejores prácticas de seguridad, para la totalidad

de los dominios de ITAIPU BINACIONAL, garantizando la integridad y autenticidad de las respuestas DNS y mitigando ataques de suplantación y envenenamiento de caché.

2.14. La solución deberá incluir un servicio de entrega y exportación de registros (logs) en tiempo casi real y baja latencia, que permita a ITAIPU BINACIONAL ejercer control total sobre los flujos de datos de registro, incluyendo, como mínimo, las siguientes capacidades:

2.14.1. Crear, editar, visualizar, habilitar, deshabilitar y eliminar **configuraciones de flujos de entrega de registros**, de forma autónoma desde la plataforma de gestión.

2.14.2. Recopilar, agrupar y transmitir **registros en formato bruto (raw logs)** hacia uno o más destinos seleccionados, permitiendo definir **ventanas temporales configurables**, políticas de entrega y reintentos ante fallos.

2.14.3. El servicio deberá habilitar **integración nativa** con, al menos, las siguientes plataformas de almacenamiento y análisis:

a) Amazon S3
b) Azure Storage
c) Google Cloud Storage
d) Splunk

2.14.4. El servicio de entrega de registros deberá **emitir alertas automáticas de notificación por correo electrónico** ante fallos en el envío de los logs, con el fin de facilitar la **detección y resolución temprana de incidentes**, tales como configuraciones de destino inválidas, errores de autenticación o tiempos de espera en la transmisión de datos.

2.14.5. El servicio deberá utilizar los mecanismos nativos de la plataforma Cloudflare (Logpush o equivalentes), sin intermediarios.

2.14.6. El servicio deberá exportar, como mínimo, los siguientes conjuntos de registros hacia el SIEM corporativo (Splunk): solicitudes HTTP/HTTPS, eventos de WAF, eventos de gestión de bots, eventos de protección de API, consultas DNS y pistas de auditoría administrativa (ítems 2.18.15 y 2.18.16) y retención de largo plazo garantizada mediante la exportación continua al SIEM.

2.14.7. El CONTRATISTA deberá brindar apoyo en la configuración y validación del parsing de estos registros en el SIEM, asegurando integridad, identificación de origen y utilidad analítica de los datos recibidos.

2.15. La plataforma ofertada deberá estar certificada por organismos independientes con mínimamente las siguientes certificaciones:

2.15.1. ISO/IEC 27001.

2.15.2. SOC 2 Tipo II- NO se acepta Tipo I como equivalente.

2.15.3. FedRAMP Moderate o High.

2.16. Características de acceso a la gestión de la herramienta:

a) Integración con el proveedor de identidad corporativo mediante SSO/SAML u OIDC, compatible con el entorno Microsoft Entra ID con PTA.
b) Autenticación multifactor obligatoria para todos los accesos administrativos

c) Control de acceso basado en roles (RBAC), con segregación mínima entre perfiles de lectura, operación y administración, atendiendo al principio de segregación de funciones (SoD).
d) Registro de auditoría de autenticación y de cambios de privilegios, exportable al SIEM corporativo.
e) Revisión periódica de cuentas y privilegios, con remoción oportuna de accesos de profesionales desvinculados.

2.17. CONTENT DELIVERY NETWORK (CDN)

2.17.1. El servicio de CDN deberá ser provisto a través de la red global de Cloudflare, con presencia distribuida mediante arquitectura Anycast, permitir el control a nivel de capa IP, incluyendo la liberación y bloqueo de direcciones IP individuales y rangos de direcciones, con propagación automática de dichas listas en toda la infraestructura global del proveedor.

2.17.2. Deberá soportar la creación y gestión de listas de bloqueo basadas en direcciones IP, subredes (CIDR) y Geolocalización.

2.17.3. La arquitectura del servicio deberá ser descentralizada, sin puntos únicos de fallo, con servidores distribuidos geográficamente, capaces de entregar contenido estático y dinámico, de forma cifrada mediante TLS/SSL, en todos los puntos de la red.

2.17.4. Cada POP (Punto de Presencia) deberá disponer de infraestructura suficiente para garantizar un SLA mínimo del 99,999 % de disponibilidad.

2.17.5. El CONTRATISTA de CDN deberá contar con Puntos de Presencia (POPs) con presencia confirmada y operativa en los territorios de Paraguay y del Brasil, los cuales deberán

formar parte activa de la red de entrega de contenido utilizada para los servicios de ITAIPU.

2.17.6. El servicio deberá contar con **mecanismos de enrutamiento dinámico e inteligente**, que permitan la redirección automática del tráfico en caso de indisponibilidad de cualquier POP, sin degradar el rendimiento del servicio.

2.17.7. Deberá disponer de un **entorno de pruebas o preproducción**, que permita aplicar y validar configuraciones de distribución de contenido y de seguridad antes de su publicación en producción.

2.17.8. Dicho entorno de pruebas deberá contar con **las mismas funcionalidades que el entorno de producción**.

2.17.9. El sistema deberá permitir la **replicación directa de las configuraciones del entorno de pruebas al entorno de producción**, mediante la interfaz web de administración.

2.17.10. Toda configuración activa en producción deberá estar reflejada en el entorno de pruebas o permitir su **exportación/importación**, con el fin de realizar validaciones sin afectar el servicio productivo.

2.17.11. El servicio deberá utilizar **algoritmos inteligentes de selección de POP**, determinando el punto con mejores condiciones de entrega mediante técnicas de **redirección de tráfico a nivel de aplicación y/o DNS**.

2.17.12. Deberá permitir que todos los servidores de la red CDN reconozcan el **sitio de origen**, así como su contenido **estático y dinámico**, en todos los POPs del proveedor.

2.17.13. El CONTRATISTA deberá proporcionar **aceleración y protección** para la totalidad de los dominios mencionados en el ítem 2.3 a ITAIPU.

2.17.14. El servicio deberá garantizar la **disponibilidad del sitio web y tiempos de carga de página inferiores** a los obtenidos sin el uso de CDN, independientemente del número de usuarios concurrentes.

2.17.15. El proveedor deberá determinar, **en tiempo real y de forma automática**, qué servidor CDN ofrece las mejores condiciones de entrega para cada usuario.

2.17.16. Los cambios en listas de liberación y bloqueo deberán **propagarse en un plazo máximo de 3 minutos**, permitiendo una respuesta eficaz ante incidentes de seguridad.

2.17.17. El servicio deberá permitir la **expiración (purga) de contenido por URL**, incluyendo **comodines**, en toda la red, con un tiempo máximo de propagación de **1 minuto**.

2.17.18. La infraestructura deberá contar con **rutas redundantes** para el acceso y distribución del contenido, garantizando la continuidad del servicio y el acceso al origen.

2.17.19. El servicio deberá acelerar y distribuir cualquier aplicación basada en **HTTP y HTTPS**, balanceando la carga entre sus POPs para optimizar el rendimiento.

2.17.20. El CONTRATISTA deberá emitir, **sin coste adicional para ITAIPU**, los certificados digitales necesarios para la aceleración y distribución de servicios HTTPS.

2.17.21. Los certificados deberán configurarse de forma que alcancen, como mínimo, la **calificación "A+"** en las pruebas de **Qualys SSL Labs**.

2.17.22. Los certificados digitales SSL/TLS para servidores web deberán cumplir con las siguientes especificaciones:

a) Certificados SSL/TLS tipo A1, individuales por URL o de tipo comodín, válidos para subdominios del mismo dominio raíz.
b) El certificado raíz de la autoridad certificadora deberá estar reconocido por los principales navegadores y dispositivos del mercado (Firefox, Chrome, Edge, Safari, iOS, Android, Windows).
c) El CONTRATISTA deberá garantizar la validez continua de los certificados durante todo el período contractual.
d) El proceso de validación de certificados deberá realizarse en línea, por vía telefónica o mediante validación DNS.

2.17.23. El proveedor del servicio deberá permitir la configuración de las versiones de TLS y de los conjuntos de cifrado (cipher suites) utilizados para las conexiones HTTPS de los servicios de ITAIPU, conforme a buenas prácticas de seguridad y estándares internacionales.

2.17.24. El certificado digital deberá contar con validación de la organización emisora, incluyendo, cuando aplique, los datos identificatorios de ITAIPU en el propio certificado (validación de organización – OV).

2.17.25. El servicio deberá ser capaz de detectar fallos o indisponibilidad en uno o más enlaces del centro de datos de origen, garantizando la continuidad en la transmisión y entrega del contenido.

2.17.26. El servicio deberá permitir la configuración de orígenes de respaldo (standby) con failover automático ante fallo o indisponibilidad del origen principal.

2.17.27. Adicionalmente, la solución deberá incluir capacidad de balanceo de carga activo, con licenciamiento para un mínimo de 20 (veinte) orígenes en modo balanceo, entendidos como orígenes configurados simultáneamente dentro de un pool de balanceo con distribución activa de tráfico entre ellos. La solución deberá contemplar:

a) Distribución de tráfico entre los orígenes del pool mediante métodos configurables (round-robin, weighted, geográfico).
b) Monitorización continua del estado de salud de cada origen (health checks) con failover automático.
c) Gestión centralizada de los pools y orígenes desde el panel de administración de la plataforma.
d) El licenciamiento para los 20 orígenes en modo balanceo deberá estar incluido en el precio ofertado, sin costo adicional para ITAIPU durante toda la vigencia del contrato.

2.17.28. El servicio de CDN deberá ser sensible a mayúsculas y minúsculas (case-sensitive) en el almacenamiento y recuperación de objetos en caché.

2.17.29. El servicio deberá permitir la selección y control de parámetros de cadena de consulta (query string), cookies y headers para la generación de claves de caché, de modo que solicitudes con características equivalentes utilicen el mismo objeto almacenado.

2.17.30. Debe contar con los siguientes recursos para la gestión de caché:

a) Soporte para políticas de no almacenamiento en caché (No-Store).
b) Opción para bypass de caché, de modo que el contenido no sea almacenado por la CDN cuando así se configure.

2.17.31. El servicio deberá **identificar, analizar y tratar de forma individualizada** las solicitudes maliciosas dirigidas a los sitios web de origen, bloqueándolas antes de que alcancen la infraestructura de ITAIPU.

2.17.32. El servicio deberá permitir la creación de **políticas de caché avanzadas**, incluyendo:

a) Bypass de caché para solicitudes específicas.
b) Reenvío controlado de cookies hacia los servidores de origen.

2.17.33. El servicio deberá realizar inspección del cuerpo de las solicitudes HTTP/HTTPS, incluyendo formularios y cargas HTML, sin limitaciones funcionales que impidan la detección de ataques comunes.

2.17.34. El servicio deberá realizar análisis e inspección del contenido de las solicitudes, utilizando técnicas que no se limiten exclusivamente a firmas estáticas, incorporando análisis contextual y heurístico.

2.17.35. El servicio deberá soportar y procesar correctamente, como mínimo, los siguientes métodos HTTP: GET, HEAD, POST, PUT, PATCH, DELETE y OPTIONS.

2.17.36. El servicio deberá permitir la restricción de métodos HTTP por aplicación o sitio, bloqueando aquellos métodos que no estén explícitamente habilitados.

2.17.37. El servicio deberá permitir modificar, añadir o eliminar encabezados HTTP, tanto en las solicitudes enviadas al origen como en las respuestas entregadas a los clientes.

2.17.38. El servicio deberá proporcionar geolocalización a nivel de país, permitiendo la gestión de políticas de acceso y denegación basadas en la ubicación geográfica de las solicitudes.

2.17.39. El servicio deberá ser capaz de entregar cualquier tipo y formato de contenido utilizando, como mínimo, los protocolos HTTP/1.1, HTTP/2 y HTTP/3 (QUIC).

2.17.40. El servicio deberá proporcionar aceleración mediante compresión de datos, soportando al menos Gzip y Brotli, siempre que el navegador o dispositivo del usuario lo permita.

2.17.41. El servicio deberá ser capaz de identificar características de los dispositivos clientes, utilizando la información provista por el navegador (User-Agent, headers, reglas y mecanismos equivalentes).

2.17.42. El servicio deberá permitir la recuperación de objetos almacenados en caché desde otros nodos de la red CDN, evitando, cuando sea posible, la conexión directa con el centro de datos de origen.

2.17.43. El servicio deberá verificar que las solicitudes de acceso al contenido almacenado provienen de sitios web o aplicaciones autorizadas, aplicando controles de acceso a nivel de dominio, encabezados o tokens.

2.17.44. El servicio deberá contar con mecanismos de defensa activa e inmediata, de modo que las solicitudes que correspondan a un grupo de ataque definido con acción de

denegación sean automáticamente penalizadas o bloqueadas durante un período configurable.

2.17.45. El proveedor deberá proporcionar una infraestructura escalable, automática y en tiempo real, capaz de garantizar la correcta prestación de los servicios, independientemente del volumen de accesos simultáneos.

2.17.46. El panel de monitorización deberá permitir la visualización y consulta de métricas de tráfico, solicitudes HTTP y HTTPS, y caché (hits/misses), de forma individual por cada sitio web configurado, manteniendo un historial mínimo de 30 (treinta) días.

2.17.47. El panel de monitorización deberá permitir la **creación de filtros y reportes personalizados**, por sitio web y rango de fechas.

2.17.48. El panel de monitorización debe permitir monitorizar el número de solicitudes realizadas para cada sitio WEB en la CDN;

2.17.49. El panel de monitorización deberá proporcionar información detallada de seguridad, incluyendo al menos:

a) País de origen
b) Dirección IP
c) Regla o tipo de amenaza detectada
d) Método HTTP utilizado
e) Fecha y hora del evento

2.17.50. Incluyendo, como mínimo:

a) Identificación de los sitios web afectados.
b) Tipos de ataques o amenazas detectadas.

2.17.51. La información presentada en el panel de monitorización deberá estar disponible con un **retraso máximo de 5(cinco) minutos**, y conservar un **historial mínimo de 30 (treinta) días**.

2.17.52. El panel de monitorización deberá presentar, mediante **gráficos**, todas las solicitudes realizadas por los usuarios finales, **clasificadas por códigos de estado HTTP/HTTPS**, permitiendo identificar **picos de tráfico**.

2.17.53. El panel de monitorización deberá presentar y contabilizar, mediante **gráficos y API**, el **volumen de datos transferidos y el número de solicitudes** entre la CDN y los usuarios finales, diferenciados por códigos de estado HTTP/HTTPS.

2.17.54. El panel de monitorización deberá presentar y contabilizar, mediante **gráficos y API**, el **volumen de datos y solicitudes** atendidas desde el **origen** y desde los **servidores de borde (edge)** de la CDN.

2.17.55. El servicio deberá poner a disposición **registros (logs) de servidor**, permitiendo su descarga o exportación con un **retraso no superior a 15 (quince) minutos**.

2.17.56. El servicio deberá permitir la **monitorización del comportamiento de navegación de los usuarios**, incluyendo:

c) Monitorización mediante **inyección de JavaScript** para la recopilación de métricas de rendimiento y datos del cliente.
d) Supervisión del rendimiento de navegación mediante **recolección de balizas (beacons)** en navegadores modernos (Chrome, Firefox, Edge) y plataformas móviles principales (**Android e iOS**).

2.17.57. El servicio deberá permitir la monitorización en tiempo casi real de los datos de rendimiento recopilados mediante balizas (beacons / RUM), proporcionando visualización, como mínimo, de las siguientes características del usuario final:

a) Navegador
b) Tipo de dispositivo
c) Sistema operativo
d) Ubicación geográfica (país / región)

2.17.58. El servicio deberá poner a disposición interfaces de programación de aplicaciones (API) que permitan:

a) La consulta del estado y configuración de las políticas de caché y de seguridad.
b) La modificación y actualización de dichas configuraciones, garantizando su propagación automática y consistente en todos los servidores de borde de la plataforma CDN.

2.17.59. El servicio deberá incluir un mecanismo de gestión de afluencia de usuarios que permita controlar el acceso a los sitios web protegidos ante picos de tráfico elevado, evitando la degradación o caída del servicio de origen. La solución deberá incluir licenciamiento para un mínimo de 2 (dos) salas de esperas (waiting room) de tipo advanced waiting room activas simultáneamente, que sean utilizables indistintamente a nivel de cuenta de ITAIPU y aplicable según necesidad a cualquier dominio solicitado y contemplar:

a) Presentación automática de una página de espera personalizable a los usuarios en cola, con estimación del tiempo de espera y actualización en tiempo real.
b) Control configurable del número máximo de usuarios activos simultáneos admitidos en el sitio, con umbral ajustable por ITAIPU.
c) Incorporación automática de usuarios a la sesión activa a medida que se liberen plazas disponibles, sin intervención manual.
d) Capacidad de aplicar el mecanismo de forma selectiva por URL, ruta o dominio protegido.
e) Panel de monitorización en tiempo real del estado de la cola, incluyendo número de usuarios en espera, tiempo estimado y tasa de admisión.
f) Activación automática al superar los umbrales configurados, sin requerir intervención manual del equipo de ITAIPU.
g) El licenciamiento para las 2 salas de espera deberá estar incluido en el precio ofertado, sin costo adicional para ITAIPU durante toda la vigencia del contrato.

2.18. WEB APPLICATION FIREWALL (WAF)

2.18.1. El Web Application Firewall (WAF) deberá ser el servicio nativo de la plataforma Cloudflare, ejecutándose en todos los puntos de presencia de su red global. activo en todos los Puntos de Presencia (POPs) de la red, con el fin de prevenir actividades maliciosas a nivel de aplicación, incluyendo —como mínimo— la detección y mitigación de los siguientes tipos de ataques, sin limitarse a ellos:

a) Bloqueo a nivel de red, dirección IP y rangos de direcciones.
b) Políticas de seguridad basadas en geolocalización.
c) Uso de tokens de seguridad y mecanismos de validación de sesión.

d) Ataques de Cross-Site Scripting (XSS).
e) Remote File Inclusion (RFI).
f) Directory Traversal.
g) Inyección SQL (SQLi).
h) Control de tasa (Rate Limiting) para mitigación de ataques DoS a nivel de aplicación de manera avanzada.
i) Protección contra ataques de Slow POST / Slow HTTP.

2.18.2. El WAF deberá proporcionar protección efectiva contra las vulnerabilidades de aplicaciones web definidas en el OWASP Top 10, así como frente a nuevas vulnerabilidades que puedan publicarse durante la vigencia del contrato, incluyendo, como mínimo:

a) Inyecciones (SQL, NoSQL, OS, LDAP).
b) Fallos de autenticación y gestión de sesiones.
c) Cross-Site Scripting (XSS).
d) Referencias directas inseguras a objetos (IDOR).
e) Configuración de seguridad incorrecta.
f) Exposición de datos sensibles.
g) Fallos de control de acceso.
h) Cross-Site Request Forgery (CSRF).
i) Uso de componentes con vulnerabilidades conocidas.
j) Redirecciones y reenvíos no validados.

2.18.3. El WAF deberá operar de forma autónoma en el borde de la red, aplicando inspección y mitigación en el mismo punto de presencia que procesa la solicitud, sin requerir redirección de tráfico a centros de análisis centralizados externos a la infraestructura de entrega.

2.18.4. El proveedor deberá contar con un proceso de actualización de emergencia de reglas WAF, diferenciado del ciclo de actualización estándar, que permita el despliegue de reglas de mitigación ante vulnerabilidades críticas de aplicación web en el menor tiempo posible desde su divulgación pública.

2.18.5. Dicho proceso de emergencia deberá aplicarse de forma automática a todos los clientes sin requerir solicitud expresa, y el cliente deberá ser notificado del despliegue de nuevas reglas mediante un mecanismo oficial del fabricante.

2.18.6. El servicio deberá permitir la creación de reglas personalizadas, expresiones avanzadas, dentro del WAF, sin límites adaptadas a las características específicas de cada

aplicación o sistema publicado en la CDN, con soporte para despliegue centralizado y/o por sitio.

2.18.7. El WAF deberá incorporar **análisis de comportamiento y puntuación de riesgo**, no limitado a firmas estáticas.

2.18.8. El WAF deberá diferenciar tráfico legítimo de bots maliciosos.

2.18.9. El servicio deberá permitir exportación de eventos de seguridad hacia plataformas SIEM mediante API o streaming de logs.

2.18.10. El WAF deberá permitir **modo de aprendizaje o monitoreo** para reducir falsos positivos antes de bloquear.

2.18.11. El WAF deberá contar con mecanismos automáticos para detectar y mitigar ataques de fuerza bruta, credential stuffing y abuso de formularios de autenticación.

2.18.12. Deberá permitir la correlación de eventos y la aplicación de medidas progresivas (bloqueo, desafío, limitación de tasa) sin afectar a usuarios legítimos.

2.18.13. El WAF deberá permitir la mitigación inmediata de vulnerabilidades conocidas o de día cero mediante virtual patching, sin requerir cambios en la aplicación protegida.

2.18.14. Las reglas de mitigación deberán actualizarse de forma automática y continua durante la vigencia del contrato.

2.18.15. El servicio deberá registrar todas las acciones administrativas relacionadas con la configuración del WAF, incluyendo creación, modificación y eliminación de reglas.

2.18.16. Los registros de auditoría deberán estar disponibles para consulta y exportación, garantizando trazabilidad completa para fines de control y cumplimiento.

2.18.17. El servicio deberá permitir la administración centralizada de políticas y reglas de seguridad para múltiples aplicaciones o sitios web.

2.18.18. Deberá soportar despliegues consistentes por sitio, grupo de sitios o de forma global, facilitando la operación en entornos de gran escala.

2.19. PROTECCIÓN DE API

2.19.1. El servicio deberá ser capaz de proteger APIs expuestas por aplicaciones mediante los mecanismos nativos de protección de APIs de Cloudflare., incluyendo, como mínimo, los siguientes tipos y formatos:

a) APIs basadas en **SOAP**.
b) APIs basadas en **XML**.
c) APIs basadas en **JSON**.
d) APIs **RESTful** sobre HTTP/HTTPS.

2.19.2. El servicio deberá ser capaz de **inspeccionar tráfico cifrado** utilizando **TLS 1.2, TLS 1.3 o versiones superiores**, y realizar **análisis de comportamiento** para identificar patrones de uso anómalos o sospechosos.

2.19.3. El servicio deberá ser capaz de **proteger APIs asociadas a los sitios web protegidos por la plataforma**, aplicando políticas de seguridad coherentes entre aplicaciones web y APIs.

2.19.4. El servicio deberá permitir la **seguridad de APIs basada en archivos de especificación** (por ejemplo, **OpenAPI/Swagger**), generando automáticamente un **modelo de seguridad positivo**, que solo permita solicitudes que cumplan con el esquema definido.

2.19.5. El servicio deberá **detectar y bloquear solicitudes que intenten acceder a métodos, rutas u operaciones no definidas en la especificación de la API**, tratándolas como violaciones de seguridad.

2.19.6. El servicio deberá integrarse con los **mecanismos de análisis y correlación de eventos de seguridad del mismo fabricante**, permitiendo una visión unificada de incidentes.

2.19.7. El servicio deberá ser compatible con **plataformas de gestión de APIs** ampliamente utilizadas, tales como **AWS**, **Microsoft Azure** y **Red Hat 3scale**, sin requerir cambios en la lógica de las APIs protegidas.

2.19.8. El servicio deberá contar con **protección contra ataques de denegación de servicio (DDoS) a nivel de aplicación**, mediante **controles de velocidad (rate limiting)** y mitigación en el borde de la red.

2.19.9. El servicio deberá proporcionar protección frente a las vulnerabilidades definidas en el **OWASP API Security Top 10**, así como frente a **nuevas vulnerabilidades** que puedan publicarse durante la vigencia del contrato.

2.19.10. El servicio deberá detectar automáticamente **APIs y endpoints no documentados (shadow APIs)**.

2.19.11. Soporte para **mutual TLS (mTLS)** y validación de **JWT**.

2.19.12. Gestión centralizada por API, capacidad de aplicar políticas **por endpoint y método**, no solo por host.

2.20. PROTECCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO EN CAPA DE APLICACIÓN (ANTI-DDOS L7)

2.20.1. La solución deberá proveer un mecanismo nativo y permanentemente activo de protección contra ataques distribuidos de denegación de servicio (*Distributed Denial of Service* – DDoS) en capa de aplicación (Capa 7 del modelo OSI), destinado a la detección, análisis, mitigación y bloqueo automático de tráfico malicioso dirigido a aplicaciones web, APIs, portales corporativos, servicios DNS y demás activos publicados por medio de la plataforma contratada.

2.20.2. La protección deberá operar de forma integrada a la infraestructura global del prestador, utilizando mecanismos automáticos de identificación y mitigación de ataques,

sin exigir intervención manual para su activación durante eventos de denegación de servicio.

2.20.3. La solución deberá contemplar, como mínimo, las siguientes capacidades:

a) a) detección y mitigación automática de ataques HTTP, HTTPS, HTTP/2, HTTP/3, WebSocket, APIs REST, GraphQL y demás protocolos de aplicación soportados por la plataforma.
b) b) identificación y mitigación de ataques de agotamiento de recursos (*resource exhaustion*), ataques por inundación de solicitudes (*request flood*), ataques distribuidos de capa de aplicación, abuso de APIs, conexiones abusivas y demás técnicas destinadas a la degradación o indisponibilidad de los servicios protegidos.
c) c) utilización de mecanismos de análisis comportamental, inteligencia de amenazas, reputación de direcciones IP, identificación de firmas de ataques y análisis estadístico de tráfico para diferenciar entre usuarios legítimos y tráfico malicioso.
d) d) mitigación automática en tiempo real, sin necesidad de redireccionamiento manual del tráfico ni alteración emergencial de configuraciones durante la ocurrencia del ataque.
e) e) capacidad de protección contra ataques distribuidos originados en redes de bots, dispositivos comprometidos, proxies anónimos, VPNs públicas, servicios de anonimización y demás fuentes frecuentemente utilizadas en campañas DDoS.
f) f) aplicación de desafíos adaptativos (*challenge mechanisms*), validación de clientes, limitación de tasa (*rate limiting*), bloqueo selectivo, mitigación basada en reputación y otros mecanismos destinados a preservar el acceso de los usuarios legítimos.
g) g) soporte para la definición de políticas diferenciadas por dominio, aplicación, URL, API, método HTTP, encabezado, origen geográfico, ASN, dirección IP, grupo de usuarios u otros atributos disponibles en la solución.
h) h) coordinación operacional entre los mecanismos de Anti-DDoS, Web Application Firewall (WAF), gestión de bots y demás controles de seguridad de la plataforma, a fin de proporcionar una respuesta integrada ante incidentes.

2.20.4. La solución deberá operar mediante infraestructura global distribuida, compuesta por una red de entrega de contenido (*Content Delivery Network* – CDN) y puntos de presencia geográficamente distribuidos, aptos para absorber, filtrar y mitigar tráfico malicioso antes de que este alcance los ambientes de ITAIPU.

2.20.5. La CONTRATADA deberá disponibilizar recursos de monitoreo y observabilidad que contengan, como mínimo:

a) visualización en tiempo real de los eventos de mitigación.
b) estadísticas de solicitudes legítimas y bloqueadas.
c) identificación de los vectores de ataque observados.
d) registros detallados de los eventos de mitigación.
e) historial de los incidentes ocurridos.
f) indicadores de tendencia y volumen de los ataques mitigados.

2.20.6. Los registros y métricas relacionados con los eventos de protección Anti-DDoS deberán permanecer disponibles para consulta y exportación por parte de ITAIPU durante todo el período de retención contratado.

2.20.7. Siempre que ocurra un incidente de denegación de servicio considerado relevante por ITAIPU, la CONTRATADA deberá disponibilizar un informe técnico que contenga, como mínimo:

a) fecha y hora de inicio y finalización del evento.
b) activos afectados.
c) vectores de ataque identificados.
d) volumen y características del tráfico mitigado.
e) medidas adoptadas automáticamente por la plataforma.
f) impactos observados.
g) recomendaciones de ajuste o fortalecimiento de la protección.

2.21. GESTIÓN DE ROBOTS (BOTS)

2.21.1. La plataforma deberá ser capaz de **detectar y clasificar automáticamente accesos realizados por robots (bots)** a los sistemas y sitios web de ITAIPU protegidos por la solución.

2.21.2. La plataforma deberá contar con una **base de datos dinámica de bots conocidos**, categorizados al menos en **bots legítimos (buenos)** y **bots maliciosos**, la cual deberá **actualizarse automáticamente** para incorporar nuevos bots y retirar aquellos obsoletos o inactivos.

2.21.3. La plataforma deberá ser capaz de **identificar bots falsos o suplantados**, diferenciando entre bots legítimos y aquellos que **simulan su identidad mediante encabezados HTTP (User-Agent)**.

2.21.4. La plataforma deberá ser capaz de **detectar bots desarrollados utilizando frameworks, bibliotecas y herramientas de automatización comunes**, incluyendo —pero no limitándose a—:

a) Frameworks y runtimes (Node.js, Ruby, Java, PHP)
b) Bibliotecas HTTP y clientes automatizados (OkHttp, cURL, Python requests)
c) Navegadores sin interfaz (headless) y motores de automatización (PhantomJS, Puppeteer, Playwright)
d) Rastreadores y herramientas de scraping

2.21.5. La plataforma deberá detectar accesos automatizados **analizando anomalías de comportamiento y del protocolo**, tales como:

a) Firmas incorrectas o inconsistentes de encabezados HTTP
b) Orden anómalo de cabeceras
c) Inconsistencias entre User-Agent, versión de navegador y capacidades TLS/HTTP

2.21.6. La plataforma deberá permitir la **creación de categorías personalizadas de bots**, posibilitando la inclusión y gestión de bots específicos definidos por ITAIPU.

2.21.7. La plataforma deberá permitir la aplicación de **acciones de seguridad diferenciadas sobre el tráfico de bots**, incluyendo como mínimo:

a) Monitorización y registro del tráfico de bots.

b) Permitir el acceso (allow).
c) Bloquear el acceso devolviendo un código HTTP 403.
d) Bloquear el acceso devolviendo un mensaje o respuesta personalizada.
e) Desafíos gestionados o invisibles para validar tráfico legítimo sin afectar la experiencia del usuario.

2.21.8. La plataforma deberá asignar una puntuación de probabilidad de automatización a cada solicitud, permitiendo diferenciar de forma granular entre tráfico humano y automatizado, y aplicar políticas de seguridad basadas en dicha puntuación.

2.21.9. La plataforma deberá permitir identificar, permitir, restringir o bloquear bots asociados a inteligencia artificial, incluyendo rastreadores utilizados para entrenamiento de modelos, respetando políticas configurables por el propietario del contenido.

2.21.10. La plataforma deberá permitir aplicar políticas de gestión de bots de forma granular, por:

a) URL o ruta
b) Aplicación
c) API o endpoint específico
d) Método HTTP

2.21.11. La plataforma deberá proporcionar paneles y APIs de analítica avanzada de bots, permitiendo visualizar:

a) Volumen de tráfico por tipo de bot
b) Tendencias y picos de automatización
c) Acciones aplicadas (permitido, bloqueado, desafiado)
d) Impacto en aplicaciones y APIs

2.22. DNS AUTORITATIVO Y GESTIÓN DE CERTIFICADOS DIGITALES

2.22.1. El servicio deberá basarse en el sistema DNS autoritativo de Cloudflare, altamente disponible y distribuida geográficamente, para la gestión de los dominios de ITAIPU, capaz de operar a gran escala y de absorber incrementos significativos de tráfico

mediante **mecanismos de escalado automático**, sin degradación del servicio ni interrupciones operativas.

2.22.2. El servicio DNS autoritativo deberá **soportar e implementar DNSSEC (Domain Name System Security Extensions)**, incluyendo la **firma criptográfica de zonas**, gestión de claves y cadena de confianza.

2.22.3. El servicio deberá disponer de **puntos de presencia (PoPs) para resolución DNS en Brasil y Paraguay**, garantizando baja latencia y resiliencia regional.

2.22.4. El servicio deberá garantizar **disponibilidad 24x7x365**, con un **SLA mínimo de 99,999%** para el servicio DNS autoritativo.

2.22.5. El servicio DNS deberá operar sobre una **red Anycast global**, distribuida en los puntos de presencia definidos en este documento, permitiendo **enrutamiento automático al PoP más cercano** y tolerancia a fallos.

2.22.6. El servicio deberá proporcionar **mecanismos de aceleración de resolución DNS**, incluyendo optimización de rutas, baja latencia de respuesta y propagación eficiente de cambios.

2.22.7. El proveedor deberá permitir la **implementación del servicio DNS como primario y/o secundario**, posibilitando el **reemplazo o la coexistencia con la infraestructura DNS actual de ITAIPU**.

2.22.8. El servicio DNS autoritativo deberá proporcionar, como mínimo:

a) Aceleración de la resolución DNS.
b) Protección contra ataques dirigidos al servicio DNS.
c) Alta disponibilidad y continuidad operativa del servicio DNS.

2.22.9. El servicio deberá proporcionar interfaces de gestión mediante portal web y APIs, permitiendo la integración con herramientas y flujos de automatización de ITAIPU.

2.22.10. El servicio debería proporcionar métricas y analítica avanzada del tráfico DNS, incluyendo volumen, latencia, errores y eventos de seguridad.

2.22.11. El servicio debería incluir mitigación automática contra ataques de amplificación, reflection y NXDOMAIN floods, sin impacto en el SLA.

2.22.12. El proveedor deberá ofrecer un servicio integrado de gestión de certificados digitales TLS/SSL, que permita proteger las comunicaciones HTTP y otros servicios publicados por ITAIPU, garantizando confidencialidad, integridad y autenticidad de la información.

2.22.13. El proveedor deberá proveer los certificados digitales necesarios para los dominios gestionados, sin requerir la adquisición externa por parte de ITAIPU, incluyendo su emisión, instalación, renovación y revocación, de forma automatizada y transparente.

2.22.14. El servicio deberá soportar, como mínimo, los siguientes tipos de certificados:

a) Certificados DV (Domain Validation).
b) Certificados OV (Organization Validation).
c) Certificados EV (Extended Validation), cuando aplique.
d) Certificados Wildcard.
e) Certificados SAN / Multi-dominio.

2.22.15. El proveedor deberá permitir la renovación automática de certificados, sin intervención manual y sin impacto en la disponibilidad de los servicios, asegurando la continuidad operativa y evitando vencimientos no deseados.

2.22.16. El servicio deberá soportar algoritmos criptográficos y longitudes de clave alineados con las mejores prácticas de la industria y estándares vigentes, permitiendo la actualización de dichos algoritmos conforme evolucionen los requisitos de seguridad.

2.22.17. El proveedor deberá permitir la gestión centralizada de certificados, incluyendo visibilidad del estado, fechas de expiración y configuración por dominio o servicio.

2.22.18. Deberá permitirse, de forma opcional, el uso de certificados provistos por ITAIPU o por una Autoridad Certificadora externa, manteniendo compatibilidad con el servicio de gestión del proveedor.

2.23. REVERSIBILIDAD Y TRANSICIÓN DE LOS SERVICIOS

2.23.1. Al término de la vigencia contractual, por cualquier motivo, inclusive rescisión, denuncia o no renovación, la CONTRATADA deberá asegurar la plena reversibilidad de la solución contratada, sin interrupción indebida de los servicios y sin ningún costo adicional para ITAIPU.

2.23.2. Para tal fin, la CONTRATADA deberá:

a) disponibilizar a ITAIPU la exportación integral de las zonas DNS bajo su administración en formato estándar compatible con la RFC 1035 (*zone file*), preservando todos los registros, configuraciones y metadatos necesarios para su migración y reutilización.
b) proporcionar la documentación completa y actualizada de las configuraciones implementadas en la solución, incluyendo, pero sin limitarse a, políticas y reglas de Web Application Firewall (WAF), reglas personalizadas, listas de excepción, firmas, perfiles de protección, políticas de gestión y mitigación de bots, listas de bloqueo y permiso (*blocklists* y *allowlists*), configuraciones de seguridad, balanceo y demás parametrizaciones en uso.
c) entregar los archivos de configuración, informes, logs exportables y demás informaciones necesarias para la migración de los servicios a otro proveedor o a un ambiente administrado directamente por ITAIPU.
d) prestar soporte técnico especializado durante el proceso de transición por un período mínimo de 90 (noventa) días, contado desde la solicitud formal de ITAIPU o desde el cierre del contrato, lo que ocurra en último lugar, incluyendo aclaraciones, orientación técnica y apoyo a las actividades de migración.
e) promover la devolución formal e integral del control administrativo y operacional de los dominios, zonas DNS, certificados, credenciales, cuentas y demás activos vinculados a los servicios contratados, asegurando que ITAIPU mantenga plena autonomía sobre dichos recursos.
f) remover, luego de la confirmación de la conclusión de la migración por parte de ITAIPU, cualquier vínculo administrativo que impida o dificulte la gestión de los servicios por parte del nuevo operador.

2.23.3. La CONTRATADA no podrá imponer restricciones técnicas, comerciales o contractuales que dificulten la migración a otro proveedor, constituyendo una obligación esencial del

contrato la adopción de mecanismos que eviten el aprisionamiento tecnológico (*vendor lock-in*).

2.23.4. El cumplimiento de las obligaciones previstas en esta cláusula será realizado sin cobro adicional de licencias, tasas, servicios profesionales o cualquier otro valor distinto de aquellos ya previstos en el contrato.

2.24. PROTECCIÓN DEL LADO DEL CLIENTE (CLIENT-SIDE PROTECTION)

2.24.1. La solución deberá disponer de un mecanismo de protección del lado del cliente (client-side protection), destinado a la detección, monitoreo y control de scripts de terceros ejecutados en el navegador del usuario final durante la interacción con los sitios web y aplicaciones protegidos.

2.24.2. El mecanismo deberá proveer, como mínimo, las siguientes capacidades:

a) inventario automático de scripts de terceros cargados en las páginas monitoreadas, incluyendo origen, dominio de procedencia.
b) alertas ante la inclusión de nuevos scripts o dominios de destino, en tiempo casi real
c) visibilidad sobre las conexiones salientes iniciadas por el navegador del usuario hacia dominios de terceros.

2.24.3. El mecanismo debería, adicionalmente, permitir la detección de modificaciones o comportamiento anómalo de scripts existentes, así como la detección y bloqueo de intentos de exfiltración no autorizada de datos ingresados por el usuario. Estas capacidades podrán ser activadas por ITAIPU durante la vigencia o en la renovación del contrato, mediante el módulo correspondiente de la plataforma.

2.24.4. Esta capacidad tiene por objeto la visibilidad y control de la cadena de suministro de scripts de terceros (third-party script supply chain), en línea con las referencias de mercado vigentes en la materia.

3. PLANIFICACIÓN E IMPLEMENTACIÓN DE LA SOLUCIÓN

3.1. El CONTRATISTA deberá implementar de forma integral la solución adquirida mediante el presente documento, incluyendo la **migración de configuraciones**, **ajustes técnicos**, **pruebas**, **validación** y **puesta en producción**, garantizando su **correcta integración con el entorno tecnológico de ITAIPU** y su funcionamiento conforme a los requisitos establecidos.

3.2. La implementación deberá contemplar, como mínimo, las siguientes **etapas**:

a) Planificación
b) Ejecución
c) Homologación (validación y aceptación)
d) Entrega

3.3. El **CONTRATISTA** será responsable de la **operación completa de la infraestructura** donde se aloje la solución, debiendo adoptar todas las medidas necesarias para garantizar:

a) Disponibilidad
b) Integridad
c) Confidencialidad
d) Seguridad del entorno

3.4. El CONTRATISTA deberá disponer de servicios profesionales del fabricante de la solución o de técnicos debidamente certificados por dicho fabricante, responsables de la ejecución de los servicios contratados, así como deberá acreditar su condición de partner autorizado de Cloudflare, mediante certificación oficial vigente emitida por el fabricante.

3.5. Cualquier gasto relacionado con transporte, alimentación y alojamiento, si es necesario, para los profesionales responsables de la ejecución de los servicios, será asumido por el CONTRATISTA, sin ninguna carga para ITAIPU.

3.6. El CONTRATISTA deberá analizar el acceso a Internet, sitios remotos, servicios de red ofrecidos a empleados y usuarios externos.

3.7. El CONTRATISTA deberá configurar la solución adquirida en estricta conformidad con los requisitos definidos en este documento.

3.8. Toda la configuración deberá realizarse de acuerdo con las mejores prácticas recomendadas por el fabricante de la solución ofertada.

3.9. Cualquier actividad adicional que, aun no estando explícitamente descrita en el presente documento, resulte necesaria para el correcto funcionamiento de la solución, deberá ser ejecutada por el CONTRATISTA sin coste adicional para ITAIPU.

3.10. La solución debe configurarse para garantizar la plena operatividad con el entorno informático de ITAIPU y optimizarse para disfrutar de las mejores condiciones en términos de rendimiento y disponibilidad;

3.11. Todos los servicios abajo deberán ser realizados por personal técnico experimentado y certificado por el fabricante de la solución:

a) Despliegue
b) Configuración
c) Migración
d) Pruebas
e) Revisión Periódica de la Solución (Health-Check)

3.12. La ITAIPU podrá, antes del inicio de la implementación:

a) Solicitar evidencia documental de dichas certificaciones
b) Aceptar o requerir la sustitución del profesional asignado si no cumple los requisitos exigidos

3.13. Antes del inicio de la implementación, el CONTRATISTA deberá firmar un acuerdo de confidencialidad, comprometiéndose a:

a) Utilizar la información recibida exclusivamente para la ejecución del contrato
b) No divulgar información confidencial a terceros sin autorización expresa y escrita de ITAIPU

3.14. Los servicios de implementación, configuración, migración y pruebas deberán incluir, como mínimo, las siguientes actividades:

3.14.1. Definir, junto con ITAIPU, los **FQDN (Fully Qualified Domain Names)** que serán protegidos por la solución WAAP, así como el **orden de implementación**.

3.14.2. Las FQDN pueden agruparse para la implementación simultánea de la solución, por definición junto con la ITAIPU.

3.14.3. Configurar, para cada FQDN seleccionado:

a) CDN
b) Políticas WAF
c) Protección de APIs
d) Gestión de bots
e) Certificados SSL y DNS

3.14.4. Configurar la **recopilación de registros (logs)** para todos los recursos de la solución asociados a los FQDN implementados.

3.14.5. Presentar y configurar, de acuerdo con ITAIPU, los **paneles de monitorización** disponibles.

3.14.6. Configurar perfiles y usuarios para la autenticación en la solución;

3.14.7. Configurar correos electrónicos para enviar alertas e informes relacionados con la solución;

3.14.8. Preparación de la documentación del entorno tal como se implementó y entregó a ITAIPU;

3.14.9. Realizar la **validación funcional** y la **entrega formal de la solución** al equipo técnico de ITAIPU.

3.14.10. Completar todo el proceso de implementación y entrega conforme a los **plazos definidos en la Tabla 4 del punto 7** de este documento.

3.15. Además de las actividades anteriores, el CONTRATISTA deberá realizar, junto con ITAIPU, un **estudio detallado de los requisitos**, formalizando un **PLAN DE IMPLEMENTACIÓN**, que abarque las fases de:

a) Planificación
b) Ejecución
c) Homologación
d) Entrega

3.16. **ETAPA DE PLANIFICACIÓN**

3.16.1. El CONTRATISTA, directamente o con apoyo del fabricante, deberá coordinar reuniones (preferentemente remotas) con el equipo técnico de ITAIPU, dentro de los

plazos establecidos en la Tabla 4 del punto 7, con el fin de preparar el PLAN DE IMPLEMENTACIÓN.

3.16.2. El CONTRATISTA, directamente o con apoyo del fabricante, deberá realizar una presentación técnica de la solución, demostrando sus funcionalidades y evidenciando el cumplimiento de los requisitos técnicos establecidos en este documento.

3.16.3. Deberá presentarse un plan preliminar de ejecución, que incluya:

a) Actividades que realizar
b) Recursos humanos involucrados
c) Calendario estimado

3.16.4. El CONTRATISTA, directamente o con apoyo del fabricante, deberá identificar y documentar los requisitos previos que ITAIPU deberá proporcionar para el inicio de los servicios.

3.16.5. El CONTRATISTA deberá proponer las configuraciones recomendadas, alineadas con las necesidades de ITAIPU y las mejores prácticas del fabricante, quedando su implementación sujeta a la aprobación expresa de ITAIPU.

3.16.6. Toda la información generada en esta etapa deberá consolidarse en la versión definitiva del PLAN DE IMPLEMENTACIÓN, que deberá ser entregada y aprobada antes del cierre de la etapa de planificación.

3.16.7. El PLAN DE IMPLEMENTACIÓN deberá incluir, como mínimo:

a) Descripción de la solución y sus componentes
b) Alcance y servicios que prestar
c) Cronograma por etapas, con responsables y fechas
d) Condiciones de ejecución
e) Puntos de contacto de ambas partes
f) Matriz de responsabilidades
g) Plan de gestión de cambios
h) Riesgos y exclusiones
i) Documentación que entregar
j) Plazo y criterios de aceptación

3.16.8. El documento deberá contar con la conformidad de ambas partes.

3.16.9. El CONTRATISTA deberá designar un director de proyecto y, al menos, un técnico responsable de la implementación, debidamente capacitado y con experiencia en la solución ofrecida.

3.16.10. ITAIPU se reserva el derecho de solicitar la sustitución del personal técnico asignado, previa justificación, en caso de no cumplir con los requisitos de cualificación.

3.16.11. La planificación deberá dar lugar a un documento de alcance, que incluya como mínimo:

a) Mapeo de los sitios y aplicaciones de ITAIPU expuestos externamente
b) Definición de las configuraciones a implementar
c) Estrategia de despliegue
d) Análisis de riesgos y medidas de mitigación
e) Cronograma de ejecución con fechas de inicio y finalización

3.17. ETAPA DE EJECUCIÓN

3.17.1. Todas las actividades de esta etapa deben realizarse en una fecha y hora acordadas entre ITAIPU y el CONTRATISTA.

3.17.2. Una vez realizada la migración de los servicios DNS y la implementación de la solución para cada FQDN (o grupo de FQDN), y con la solución en producción, el CONTRATISTA deberá **monitorizar y asistir la operación durante un periodo mínimo de 12 (doce) horas**, en una ventana acordada con ITAIPU, con el objetivo de:

a) Verificar la estabilidad operativa.
b) Detectar y corregir incidencias o inconformidades.

3.17.3. Finalizado el periodo anterior, la solución deberá ser **monitorizada durante al menos 1 (un) día hábil adicional**, durante el horario laboral, por el mismo técnico que participó en la migración, para:

a) Corrección de eventuales incidencias.
b) Verificación de rendimiento.
c) Análisis de bloqueos o comportamientos anómalos ante aumentos de carga o situaciones imprevistas.

3.17.4. Los periodos de seguimiento establecidos no afectarán el **cronograma general definido en el PLAN DE IMPLEMENTACIÓN**.

3.17.5. ITAIPU designará un **equipo técnico de acompañamiento**, responsable de:

a) Supervisar la ejecución.
b) Proveer la información necesaria.
c) Autorizar los accesos requeridos para la configuración de la solución.

3.17.6. En caso de ser necesarias actividades que puedan impactar el entorno productivo, las mismas deberán ejecutarse exclusivamente en **ventanas de mantenimiento previamente acordadas con ITAIPU**, conforme al proceso formal de gestión de cambios de ITAIPU:

a) registro de solicitud de cambio con evaluación de riesgo.
b) reducción programada del TTL antes de la ventana.
c) plan de retorno (*rollback*) probado y documentado.
d) criterios objetivos de éxito verificables.
e) comunicación a las partes interesadas.
f) copia de seguridad de las zonas antes de la migración y exportación periódica de las configuraciones durante toda la vigencia.

3.18. ETAPA DE APROBACIÓN

3.18.1. Concluida la etapa de ejecución, ITAIPU dispondrá de un **plazo de hasta 7 siete) días** para verificar que la solución:

a) Funciona conforme a lo esperado.
b) Cumple con todos los requisitos establecidos en el presente documento.

3.18.2. Durante este periodo, ITAIPU comunicará al CONTRATISTA cualquier **incidencia, desviación o fallo detectado**, incluidos problemas de integración con el entorno de red, para su **corrección sin coste adicional**.

3.19. ETAPA DE ENTREGA

3.19.1. El CONTRATISTA deberá entregar un **informe técnico final "tal como se construyó" (as-built)**, redactado en **español o portugués**, que permita la correcta operación y mantenimiento de la solución.

3.19.2. El informe deberá incluir, como mínimo:

a) Mapeo actualizado de las aplicaciones y sitios web de ITAIPU publicados por CDN.
b) Detalle de las configuraciones implementadas.
c) Usuarios, accesos y parámetros relevantes.
d) Procedimientos operativos y rutinas de mantenimiento recomendadas por el fabricante.

3.19.3. La documentación deberá ser entregada en un **plazo máximo de 10 (diez) días** tras la finalización del periodo de aprobación.

3.19.4. Una vez concluido el periodo de aprobación y corregidas todas las observaciones, ITAIPU emitirá el **acta o confirmación formal de aceptación**, cerrando el proceso de implementación.

3.19.5. La aceptación final y la correspondiente **autorización de pago por los servicios de implementación** estarán condicionadas a:

a) El funcionamiento correcto y estable de la solución.
b) El cumplimiento de los requisitos definidos en la etapa de planificación.
c) La validación de la documentación y de la transferencia de conocimiento.
d) El cumplimiento íntegro de las especificaciones de este documento.

3.20. ETAPA DE TRANSFERENCIA DE CONOCIMIENTO Y CAPACITACIÓN TÉCNICA

3.20.1. La CONTRATADA deberá realizar un programa formal de transferencia de conocimiento sobre la solución suministrada, con el objetivo de capacitar a los equipos técnicos de ITAIPU para la operación, administración, monitoreo, configuración y soporte de los servicios contratados.

3.20.2. Para el cumplimiento de esta obligación, la CONTRATADA deberá observar los siguientes requisitos mínimos:

a) realizar capacitación con una carga horaria mínima de 24 (veinticuatro) horas, pudiendo ser distribuida en módulos teóricos y prácticos.
b) disponibilizar grupos destinados a los equipos de Seguridad de la Información, Infraestructura y Desarrollo, contemplando en hasta 8 participantes indicados por ITAIPU, adecuando las necesidades operacionales definidas por ITAIPU.
c) proporcionar material didáctico completo, actualizado y en formato digital, redactado en portugués o español, abarcando aspectos conceptuales, operacionales y administrativos de la solución.
d) realizar actividades prácticas en ambiente de pruebas u homologación disponibilizado para el contrato, incluyendo obligatoriamente el ambiente previsto en el ítem 2.17.7, permitiendo a los participantes ejecutar procedimientos de configuración, administración, monitoreo, análisis de eventos, creación de políticas y demás funcionalidades relevantes de la solución.

3.20.3. Abordar, como mínimo, los siguientes temas:

a) administración y operación de la plataforma.
b) gestión de dominios y DNS.
c) configuración y gestión de WAF.
d) creación y mantenimiento de reglas personalizadas.
e) políticas de mitigación y gestión de bots.
f) monitoreo y análisis de eventos de seguridad.
g) generación de informes.
h) procedimientos de contingencia, recuperación y reversibilidad de la solución.
i) buenas prácticas de seguridad y operación.

3.20.4. Registrar formalmente la participación de los capacitados por medio de listas de presencia, registros electrónicos equivalentes o certificados de conclusión, conteniendo identificación de los participantes, carga horaria realizada y contenido impartido.

3.20.5. Someter, al término de cada grupo, un término de aceptación o documento equivalente para validación de la ejecución de la transferencia de conocimiento por parte de ITAIPU.

3.20.6. Como alternativa o complemento a la capacitación descrita en esta cláusula, la CONTRATADA podrá proporcionar créditos oficiales de capacitación del fabricante de la solución, en cantidad suficiente para atender al público objetivo definido por ITAIPU. En esta hipótesis, las capacitaciones deberán contemplar contenidos equivalentes o superiores a los requisitos establecidos en esta cláusula, ser impartidas por instructores acreditados o por plataforma oficial del fabricante y permitir la emisión de comprobantes o certificados de participación.

3.20.7. Todos los costos relacionados con la preparación, instrucción, material didáctico, laboratorios, ambientes de capacitación, certificación de participación y demás recursos necesarios para la ejecución de las actividades de transferencia de conocimiento estarán incluidos en el valor del contrato, no admitiéndose ningún cobro adicional.

3.21. REVISIÓN PERIÓDICA DE LA SOLUCIÓN (HEALTH CHECK)

3.21.1. La CONTRATADA deberá realizar revisión técnica periódica de la solución contratada, con periodicidad mínima semestral o anual, conforme lo defina ITAIPU, abarcando el análisis de la arquitectura implementada, configuraciones, políticas de seguridad, desempeño operacional, niveles de protección y adherencia a las recomendaciones vigentes del fabricante.

3.21.2. Las revisiones deberán ser conducidas por profesionales calificados y contemplar, como mínimo, los componentes de DNS, CDN, WAF, protección contra bots, gestión de tráfico, certificados digitales, autenticación, control de acceso, monitoreo, registros de auditoría y demás funcionalidades contratadas.

3.21.3. Al final de cada revisión, la CONTRATADA deberá entregar un informe técnico que contenga, como mínimo:

a) descripción del alcance, metodología utilizada y ambiente analizado.
b) inventario de las principales configuraciones evaluadas.

c) identificación de los hallazgos, vulnerabilidades, desvíos de configuración, riesgos operacionales, oportunidades de mejora e ítems en desacuerdo con las recomendaciones del fabricante.
d) clasificación de los hallazgos por nivel de severidad, como mínimo en las categorías Crítico, Alto, Medio y Bajo, acompañada de la respectiva justificación técnica.
e) comparación de las configuraciones y prácticas adoptadas por ITAIPU con las mejores prácticas, guías de seguridad, recomendaciones operacionales y arquitecturas de referencia disponibilizadas por el fabricante de la solución.
f) evaluación de la efectividad de las políticas de protección implementadas, incluyendo reglas de WAF, mitigación de bots, políticas de acceso, mecanismos de autenticación, protección contra amenazas y demás controles de seguridad disponibles.
g) plan de acción que contenga las recomendaciones de corrección o mejora, los respectivos responsables de la ejecución, dependencias identificadas, impactos previstos y prioridades de tratamiento.
h) cronograma propuesto para la implementación de las acciones correctivas y evolutivas acordadas entre las partes, conteniendo plazos estimados y marcos de seguimiento.

3.21.4. Después de la presentación del informe, la CONTRATADA deberá realizar una reunión de revisión ejecutiva y técnica para presentación de los resultados, aclaración de los hallazgos y validación conjunta del plan de acción.

3.21.5. Las correcciones, ajustes y mejoras aprobados por ITAIPU deberán ser acompañados por la CONTRATADA hasta su implementación o hasta la formalización de la decisión de ITAIPU respecto al tratamiento del riesgo identificado.

3.21.6. Los servicios de revisión periódica previstos en esta cláusula constituyen una obligación contractual autónoma y no podrán ser contabilizados ni descontados del banco de horas, franquicia de servicios profesionales o cualquier mecanismo contractual destinado a la atención de demandas operacionales, incidentes, solicitudes de servicio o actividades de sustentación de la solución.

3.21.7. Todos los costos relacionados con la ejecución de las revisiones periódicas, elaboración de los informes, reuniones de presentación, recomendaciones técnicas y seguimiento de los planes de acción estarán íntegramente incluidos en el valor contratado, no admitiéndose ningún cobro adicional.

3.21.8. ITAIPU podrá solicitar, en cualquier momento, una revisión extraordinaria de la solución como consecuencia de incidentes de seguridad, alteraciones relevantes de arquitectura, cambios significativos de configuración o publicación de vulnerabilidades críticas relacionadas con la plataforma contratada, debiendo la CONTRATADA realizar dicha evaluación sin perjuicio de las revisiones periódicas obligatorias previstas en esta cláusula.

4. SOPORTE TÉCNICO

4.1. El servicio de soporte técnico deberá prestarse por un plazo mínimo de treinta y seis (36) meses, contados a partir de la Orden de Inicio de Servicio (OIS).

4.2. El CONTRATISTA deberá ofrecer soporte técnico continuo 24x7x365, garantizando la disponibilidad, operación estable y uso integral de la solución, a fin de atender solicitudes, incidentes, eventos y consultas técnicas de ITAIPU.

4.3. El soporte deberá brindarse preferentemente en idioma español o portugués. De manera excepcional y cuando la complejidad técnica lo requiera, podrá prestarse en idioma inglés, con la debida coordinación.

4.4. Durante toda la vigencia del contrato, el CONTRATISTA deberá proporcionar, sin costo adicional para ITAIPU, todas las actualizaciones de software, incluyendo parches de seguridad, correcciones, mejoras funcionales y nuevas versiones liberadas por el fabricante.

4.5. El soporte se prestará principalmente de forma remota, siendo el CONTRATISTA plenamente responsable de la atención, diagnóstico, seguimiento y resolución de los incidentes.

4.6. El mantenimiento preventivo y correctivo de la solución será responsabilidad integral del CONTRATISTA, sin que ello implique cargos adicionales para ITAIPU.

4.7. El CONTRATISTA deberá analizar los comunicados, boletines y avisos emitidos por el fabricante, evaluar su impacto sobre el entorno de ITAIPU y emitir recomendaciones técnicas documentadas, orientadas a la reducción de riesgos, continuidad operativa y mejora del desempeño.

4.8. El soporte deberá cubrir toda la operación de la solución, incluyendo:

a) Configuración y ajustes
b) Resolución de fallos, errores o defectos
c) Asistencia técnica relacionada con parámetros, rendimiento y estabilidad

4.9. El CONTRATISTA deberá guiar, apoyar y dar seguimiento a las solicitudes de ITAIPU, incluyendo como mínimo:

a) Uso, configuración e implementación de la solución
b) Instalación y configuración de extensiones o complementos compatibles
c) Integración con otros sistemas de ITAIPU
d) Diagnóstico y resolución de problemas
e) Automatización de tareas y correcciones temporales
f) Adecuación a mejores prácticas del fabricante
g) Optimización de rendimiento y configuraciones
h) Actualización o reversión de versiones
i) Preparación de informes operativos y de gestión
j) Interpretación de documentación técnica
k) Recuperación del entorno ante incidentes
l) Gestión y seguimiento de llamadas con el fabricante, cuando aplique

4.10. Las intervenciones remotas se realizarán **previa autorización de ITAIPU**, utilizando exclusivamente los accesos, credenciales y mecanismos de seguridad habilitados por la propia ITAIPU.

4.11. El CONTRATISTA deberá disponer de **canales oficiales de soporte**, incluyendo al menos:

a) Teléfono
b) Correo electrónico
c) Portal electrónico

4.12. El **CONTRATISTA** deberá incluir, durante toda la vigencia del contrato, **soporte premium del fabricante (marca)** de la solución, con acceso directo a los equipos especializados del proveedor original.

4.13. Dicho soporte premium deberá contemplar, como mínimo:

a) Atención prioritaria de incidentes críticos
b) Acceso a ingenieros especializados del fabricante
c) Escalamiento directo a niveles avanzados (Tier 2 / Tier 3)
d) Acceso anticipado a correcciones, parches o mitigaciones cuando estén disponibles
e) Acompañamiento técnico en incidentes de alta complejidad

4.14. El **CONTRATISTA** será responsable de **coordinar y gestionar** todas las interacciones con el fabricante, actuando como punto único de contacto para ITAIPU.

4.15. ACUERDO DE NIVEL DE SERVICIO (SLA) Y CRITERIOS DE MEDICIÓN

4.15.1. La CONTRATADA deberá garantizar los niveles mínimos de servicio establecidos en esta cláusula durante toda la vigencia contractual, observando los criterios de disponibilidad, atención, respuesta y resolución definidos por ITAIPU.

4.15.2. La solución deberá presentar una disponibilidad mensual mínima de 99,99%, calculada sobre el período integral de medición, comprendiendo los servicios contratados de DNS, CDN, WAF, protección Anti-DDoS, gestión de bots y demás componentes integrantes de la solución.

4.15.3. La disponibilidad será calculada mediante la siguiente fórmula:

$$\text{Disponibilidad (\%)} = [(\text{Tiempo Total del Período} - \text{Tiempo de Indisponibilidad}) \div \text{Tiempo Total del Período}] \times 100$$

4.15.4. Para fines de cálculo, será considerada como indisponibilidad cualquier interrupción, degradación severa o falla que impida total o parcialmente la utilización normal de los servicios por parte de ITAIPU.

4.15.5. La medición de los indicadores de SLA será realizada mensualmente, mediante la utilización de los registros y métricas de la propia plataforma contratada, complementados, cuando corresponda, por registros de ITAIPU.

4.15.6. En caso de divergencia entre los registros de las partes, prevalecerán los datos obtenidos mediante análisis conjunto de los eventos, logs, informes de monitoreo y evidencias técnicas disponibles.

4.15.7. La CONTRATADA deberá disponibilizar paneles e informes que permitan a ITAIPU acompañar el cumplimiento de los niveles de servicio en tiempo real y de forma histórica.

4.15.8. No serán computados como indisponibilidad para fines de SLA los períodos derivados de:

a) mantenimientos programados previamente aprobados por ITAIPU.
b) indisponibilidades causadas exclusivamente por fallas de los sistemas, aplicaciones, redes o infraestructuras bajo responsabilidad de ITAIPU.
c) interrupciones derivadas de caso fortuito o fuerza mayor debidamente comprobados.
d) indisponibilidades provocadas por actos u omisiones de la propia ITAIPU o de terceros contratados por ella.

4.15.9. No serán consideradas exclusiones válidas los eventos derivados de:

e) a) fallas de capacidad de la infraestructura de la CONTRATADA.
f) b) errores operacionales de la CONTRATADA.
g) c) fallas de actualización, configuración o mantenimiento de la solución.
h) d) ataques cibernéticos que deberían haber sido absorbidos o mitigados por las funcionalidades contratadas de protección DDoS, WAF o mecanismos equivalentes.

4.15.10. Los llamados serán clasificados conforme su criticidad y la CONTRATADA deberá observar los siguientes tiempos máximos:

Severidad	Descripción	Inicio de la atención	Cierre del llamado
S0	Indisponibilidad total, compromiso de la seguridad o impacto severo a servicios esenciales	30 minutos	6 horas
S1	Degradación significativa o falla con elevado impacto operacional	2 horas	12 horas
S2	Falla sin impacto crítico o funcionalidad afectada parcialmente	4 horas	24 horas
S3	Dudas, ajustes operacionales, solicitudes de servicio o consultas técnicas	8 horas	48 horas

Tabla 1: Acuerdo de Nivel de Servicio (SLA) – Soporte Técnico

4.15.11. Para incidentes críticos (S0), la CONTRATADA deberá mantener seguimiento continuo hasta la normalización del servicio, inclusive mediante escalamiento a especialistas del fabricante.

4.15.12. La CONTRATADA deberá disponibilizar un informe mensual que contenga, como mínimo:

a) porcentaje de disponibilidad obtenido.
b) cantidad de incidentes registrados.
c) clasificación de los llamados por severidad.
d) tiempos de respuesta y atención observados.
e) ocurrencia de violaciones de SLA.
f) descripción de los incidentes relevantes.
g) acciones correctivas adoptadas.
h) plan de mejora continua cuando corresponda.

4.15.13. Todo incidente clasificado como crítico (S0) o que resulte en incumplimiento del SLA deberá generar un informe de análisis de causa raíz (*Root Cause Analysis* – RCA), a ser entregado en hasta 5 (cinco) días hábiles, conteniendo:

a) descripción detallada del incidente.
b) causa identificada.
c) activos afectados.
d) cronología de los eventos.
e) acciones correctivas adoptadas.
f) acciones preventivas para evitar recurrencia.
g) responsables y cronograma de implementación.

4.16. INFORMES DE SOPORTE

4.16.1. El CONTRATISTA deberá permitir la emisión de informes periódicos, que incluyan al menos:

a) Número del llamado o ticket.
b) Prioridad
c) Descripción del problema y solución
d) Procedimientos realizados
e) Fechas de apertura y cierre
f) Técnico responsable

4.17. BASE DE CONOCIMIENTO

4.17.1. Deberá proporcionarse acceso a la base de conocimientos del fabricante, incluyendo documentación, parches, guías técnicas y soporte especializado.

4.18. 4.16) COMUNICACIONES DEL FABRICANTE

4.18.1. El CONTRATISTA deberá remitir periódicamente:

a) Alertas de seguridad
b) Nuevas versiones
c) Parches
d) Avisos de fin de vida útil (EOL/EOS)
e) Recomendaciones de actualización

4.19. CERTIFICACIÓN DEL PERSONAL DE SOPORTE

4.19.1. El CONTRATISTA deberá garantizar que los profesionales asignados a la prestación del soporte técnico cuenten con la formación y certificación técnica adecuada, acorde a la criticidad y complejidad de la solución provista.

4.19.2. Como requisito mínimo, el personal técnico responsable del soporte deberá poseer con al menos 2 (dos) profesionales con certificaciones oficiales vigentes emitidas por el fabricante de la solución, que acrediten su capacidad para administrar, operar, configurar y dar soporte especializado a la plataforma ofertada.

4.19.3. Adicionalmente, el CONTRATISTA deberá contar, dentro de su equipo de soporte, con profesionales que posean certificaciones reconocidas en seguridad de la información y/o redes: CISSP y CEH.

4.19.4. El CONTRATISTA deberá garantizar la vigencia de dichas certificaciones durante toda la duración del contrato, así como la actualización del personal ante cambios relevantes en la tecnología o versiones de la solución.

4.19.5. En un plazo máximo de diez (10) días a la firma de la OIS(Orden de Inicio de Servicio), ITAIPU podrá solicitar, en cualquier momento, la acreditación documental de las certificaciones del personal asignado al servicio, así como la sustitución de recursos que no cumplan con los requisitos establecidos.

4.20. SOPORTE TÉCNICO REMOTO Y SOPORTE LOCAL – BANCO DE HORAS

4.20.1. El CONTRATISTA deberá disponer de un banco de horas de soporte local (on-site), con un total de setecientas veinte (720) horas, destinado a la prestación de servicios de

soporte técnico relacionados con customizaciones, modificaciones, adecuaciones, ajustes y reconfiguraciones de la solución, conforme a los requerimientos de ITAIPU.

4.20.2. El servicio debe ser prestado en la Central Hidroeléctrica de ITAIPU en Foz do Iguaçu (Brasil) o Hernandarias (Paraguay).

4.20.3. La utilización del banco de horas no implica obligación de consumo ni garantía de facturación, quedando su ejecución sujeta a la solicitud expresa, programación y aprobación previa de ITAIPU, de acuerdo con sus necesidades operativas.

4.20.4. Las horas del banco podrán ser utilizadas de forma flexible, en cualquier cantidad y en cualquier momento durante la vigencia del contrato, en función de la demanda de ITAIPU, sin establecerse consumos mínimos por intervención.

4.20.5. El Soporte Técnico Remoto comprenderá las asistencias necesarias para mantener el funcionamiento regular del entorno, incluyendo, entre otras, las siguientes actividades:

a) diagnóstico, análisis y tratamiento de incidentes, fallos, errores o comportamientos anómalos de la solución.
b) apoyo en la identificación y resolución de problemas relacionados con la configuración de los servicios contratados.
c) aclaración de dudas técnicas y suministro de orientaciones relacionadas con la operación de la plataforma.
d) análisis de alertas, eventos y registros relacionados con los servicios contratados;
e) apoyo en la investigación de problemas relacionados con WAF, protección de APIs, mitigación DDoS, gestión de bots, CDN, DNS y demás funcionalidades que formen parte del alcance contratado.
f) corrección u orientación para la corrección de configuraciones relacionadas con incidentes o problemas operativos.
g) apoyo en la aplicación o adecuación de las configuraciones necesarias para garantizar la continuidad y el restablecimiento de los servicios.
h) interacción con el soporte del FABRICANTE, cuando resulte necesaria para la resolución del incidente o problema.

4.20.6 Las actividades caracterizadas como Soporte Técnico Remoto serán remuneradas mediante el ítem 4 de la Planilla de Precios y no podrán, en ninguna circunstancia, ocasionar el consumo del Banco de Horas, independientemente del nivel de complejidad o del tiempo empleado para su resolución.

4.20.7 La recurrencia de una determinada asistencia o la necesidad de involucrar a un profesional especializado del CONTRATISTA o del FABRICANTE no constituirá, por sí sola, fundamento para su caracterización como servicio sujeto al Banco de Horas.

4.21. CONTROL Y REPORTE DE SERVICIOS

4.21.1. Al finalizar cada intervención de soporte local, el CONTRATISTA deberá presentar a ITAIPU un informe de servicio, en hasta 5 (cinco) días, que incluya como mínimo:

a) Fecha y horario de ejecución

b) Tipo de soporte local prestado
c) Actividades realizadas
d) Cantidad de horas consumidas del banco
e) Técnico(s) responsable(s)

4.21.2. La facturación de las horas consumidas solo podrá realizarse una vez que dicho informe haya sido revisado y aprobado expresamente por ITAIPU.

4.22. CRITERIOS DE CONSUMO DEL BANCO DE HORAS (SOPORTE LOCAL)

4.22.1. El consumo del banco de horas se realizará conforme a la siguiente equivalencia, en función del horario de prestación del servicio local:

TIPO DE SOPORTE	UNIDAD	CANTIDAD	EQUIVALENCIA
Remoto (Independiente del horário)	Horas	1	0,5
Local on-site (horário comercial)	Horas	1	1
Local on-site (fuera del horário comercial)	Horas	1	1,5
Local on-site (fin de semana y feriados)	Horas	1	2

Tabla 3: Métricas para el uso del banco de horas – Soporte Local.

4.22.2. ITAIPU se reserva el derecho de **autorizar, rechazar, priorizar o reprogramar** cualquier solicitud de consumo del banco de horas, así como de verificar la correcta imputación y utilización de las horas consumidas.

4.22.3. Para contabilizar el consumo de horas, se deberá tener en cuenta el calendario interno de ITAIPU – Área Industrial para los feriados, y el horario de expediente de 7:00 a 11:30 y de 13:30 a 17:00.

4.23. COSTOS ASOCIADOS AL SOPORTE LOCAL

4.23.1. Todos los costos asociados a la prestación del soporte local (on-site), incluyendo —sin limitarse a— pasajes, transporte, traslados, alojamiento, viáticos, alimentación, seguros, impuestos y cualquier otro gasto logístico o personal, serán de exclusiva responsabilidad del CONTRATISTA.

4.23.2. Dichos costos se considerarán íntegramente incluidos dentro de los valores contractuales y/o del banco de horas correspondiente, no pudiendo ser facturados ni reclamados adicionalmente a ITAIPU, bajo ningún concepto.

4.23.3. ITAIPU no asumirá gastos derivados de la movilización del personal del CONTRATISTA, independientemente del lugar de origen, duración de la intervención o modalidad de ejecución del servicio.

5. SEGURIDAD DE LA INFORMACIÓN

5.1. ITAIPU podrá exigir al CONTRATISTA la firma de un acuerdo de confidencialidad respecto de toda la información a la que tenga acceso, cuyas obligaciones se mantendrán vigentes durante y después de la ejecución del contrato.

5.2. El CONTRATISTA deberá cumplir estrictamente la Política de Seguridad de la Información de ITAIPU y aplicar las mejores prácticas de seguridad para la mitigación de riesgos.

5.3. El CONTRATISTA será responsable por cualquier pérdida, daño, alteración, reproducción indebida o manipulación no autorizada de datos o documentos, estando sujeto a sanciones legales y contractuales.

5.4. Toda información, datos, documentos y metadatos de ITAIPU o de terceros deberán mantenerse estrictamente confidenciales y no podrán ser divulgados ni utilizados para fines distintos a los previstos en el contrato.

5.5. Queda prohibida la divulgación o publicidad del objeto del contrato sin autorización previa y expresa de ITAIPU.

5.6. El CONTRATISTA no podrá acceder, tratar ni manipular datos sin autorización previa y deberá notificar de inmediato cualquier incidente de seguridad o uso indebido del que tenga conocimiento.

5.7. Toda información, datos, documentos y metadatos de ITAIPU o de terceros deberán mantenerse estrictamente confidenciales y no podrán ser divulgados ni utilizados para fines distintos a los previstos en el contrato.

6. CONDICIONES DE SUMINISTRO Y ACEPTACIÓN

6.1. ITAIPU supervisará y evaluará la ejecución del contrato para asegurar su correcto cumplimiento e identificar posibles incumplimientos.

6.2. En un plazo máximo de diez (10) días a la firma de la OIS(Orden de Inicio de Servicio), el CONTRATISTA deberá acreditar ser partner autorizado de Cloudflare mediante certificación oficial vigente.

6.3. Dentro de los diez (10) días posteriores a la firma de la OIS (Orden de Inicio de Servicio), el CONTRATISTA deberá designar un responsable y su sustituto como interlocutores técnicos, legales y administrativos ante ITAIPU.

6.4. Cualquier sustitución de personal asignado al proyecto deberá ser informada a ITAIPU en un plazo máximo de cinco (5) días, acompañada de la documentación que acredite su idoneidad.

6.5. Las reuniones se realizarán preferentemente de forma remota, permitiéndose reuniones presenciales solo cuando sea estrictamente necesario.

6.6. Todos los servicios deberán ser ejecutados exclusivamente por técnicos certificados por el fabricante.

6.7. El personal del CONTRATISTA no mantendrá vínculo laboral alguno con ITAIPU, aun cuando esté sujeto a sus normas de seguridad y disciplina.

7. PROGRAMA DE ACTIVIDADES

DESCRIPCIÓN DE LOS SERVICIOS A REALIZAR	UNIDAD	CANTIDAD	PLAZOS
Fase de planificación	Días	7	De OIS.
Etapa de ejecución	Días	30	Después de la fase de planificación.
Etapa de homologación	Días	7	Después del paso de la ejecución.
Etapa de Entrega	Días	10	Tras la fase de aprobación y la entrega de la documentación requerida.

Tabla 4: Programa de actividades