Fecha: 11 de noviembre de 2025 **Destinatario:** Presidencia de la mesa de contratación

N/R: INV25-0114

Asunto: Informe de la Comisión técnica para informar de las ofertas admitidas para el contrato de servicio de "**Servicio de CDN con control de ataques distribuidos y filtro de seguridad para las webs corporativas de la Autoridad Portuaria de Baleares**", expediente INV25-0114

En sesión celebrada por la mesa de contratación el 27 de octubre de 2025 relativa al expediente INV25-0114 fueron examinadas las proposiciones presentadas por las siguientes empresas:

- FLUMOTION SERVICES, S.A.
- NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.
- TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.

Y ha sido remitida la documentación presentada por dichas empresas a la Comisión técnica para el estudio del cumplimiento de los requisitos técnicos mínimos exigidos en el PPT, así como la justificación de la oferta económica de la empresa -FLUMOTION SERVICES, S.A..

Reunida la Comisión técnica, formada por D. Javier Segovia Mascaró, Jefe de Departamento de Desarrollo Tecnológico e Innovación, y por D. José Miguel Esteve Lledó, Responsable de Sistemas de Información e Infraestructuras TIC, se ha procedido a su estudio y valoración.

ESTA COMISIÓN INFORMA

Tras analizar y examinar las propuestas presentadas:

1. EN RELACIÓN AL CUMPLIMIENTO DE LOS REQUISITOS TÉCNICOS MÍNIMOS EXIGIDOS EN EL PPT DE LA SOLUCIÓN PROPUESTA:

Que la empresa **FLUMOTION SERVICES, S.A.** aporta documento con la descripción propuesta **cumpliendo íntegramente** con las características mínimas exigidas en el PPT, a continuación se detalla el análisis efectuado:

Características mínimas	Cumplimiento	Comentarios y justificación
Infraestructura		
Capacidad mínima CDN y cobertura - Soportar **≥6 TB/mes** de tráfico CDN y **≥50 millones peticiones/mes**, con **WAF** y mitigación **DDoS sin límite** de tráfico, *rate limiting* hasta **10 millones/mes**, servicio de soporte estándar, cubriendo **hasta 4 dominios** principales.	**Sí**	La oferta de Flumotion (Cloudflare) declara capacidad para >6 TB mensuales y >50 M peticiones/mes. Cloudflare cuenta con infraestructura global muy sobredimensionada (más de 330 centros de datos) incluyendo España, por lo que tráfico y peticiones máximas no serán problema (prácticamente tráfico ilimitado). Cubre al menos 4 dominios y es escalable a más.
Infraestructura de la plataforma CDN - El proveedor debe tener presencia de red en **>2 ciudades de España** (al menos 3 PoPs en España) y nodos en Europa, garantizando **baja latencia** y alineación con marcos/certificaciones exigibles.	**Sí**	Cloudflare propuesta de Flumotion tiene presencia masiva: 330+ PoPs globales con varios en España (Madrid, Barcelona, etc.). La red Cloudflare está en >320 ciudades y es la red más interconectada del mundo, situándose a <50ms del 95% de la población.
Plataforma unificada - La solución debe incluir **en una única plataforma integrada** los servicios de **DNS, CDN, WAF, mitigación DDoS y Rate Limiting**, con gestión centralizada.	**Sí**	Flumotion propone usar Cloudflare en modo Autoritativo (Full Setup), haciendo que Cloudflare gestione DNS y todos los servicios en una plataforma única. En dicha configuración, el panel de Cloudflare unifica la gestión de DNS, CDN, seguridad L7, etc., desde un solo interface.
Despliegue rápido de cambios - Cualquier cambio de configuración debe poder propagarse en la red en **<5 segundos**.	**Sí**	Cloudflare destaca por la rapidez en la propagación de cambios. En particular, señala que los cambios en reglas WAF se propagan en <10s, y además la mitigación DDoS tiene TTM ~3s. Aunque no menciona explícitamente "<5s para cualquier cambio", la arquitectura global de Cloudflare es conocida por su inmediatez al aplicar configuraciones.
Sin limitaciones de tráfico - La plataforma **no debe imponer limitaciones** de ancho de banda ni peticiones por segundo (tráfico ilimitado).	**Sí**	Cloudflare posee una capacidad de red enorme (tera-bps), sin imponer límites fijos al tráfico de un cliente. La oferta no fija tope alguno a ancho de banda ni solicitudes; por el contrario, enfatiza la robustez de la infraestructura. Los valores mínimos (6TB/50M) se cumplen con margen, y no se indica restricción superior, por lo que se asume tráfico ilimitado para APB dentro de la oferta.
Autenticación multifactor (MFA) - Debe ofrecer **MFA** para el acceso administrativo a la plataforma.	**Sí**	Cloudflare ofrece autenticación multifactor para el acceso al panel de control (es una plataforma orientada a seguridad). Aunque la oferta de

		Flumotion no lo menciona textualmente, es sabido que Cloudflare soporta MFA/2FA y SSO para sus cuentas.
Seguridad web (WAF)		
Visibilidad de seguridad completa - Debe proporcionar **panel de control en tiempo real** con métricas claras de tráfico, ataques y rendimiento.	**Sí**	Flumotion provee a APB acceso al dashboard en tiempo real de Cloudflare, con visibilidad total de tráfico, rendimiento y ataques. De hecho, Cloudflare incluye incluso monitorización de usuario real (*Real User Monitoring*) y métricas Web Vitals en su panel, enriqueciendo la visibilidad.
Protección OWASP y reglas gestionadas - Debe cubrir ataques típicos (OWASP Top 10) y exploits emergentes, y disponer de **conjuntos de reglas de seguridad gestionadas actualizadas**.	**Sí**	Cloudflare cubre todas las vulnerabilidades conocidas: su WAF incluye reglas gestionadas creadas por el equipo de seguridad de Cloudflare, abarcando ataques típicos (RCE, SQLi, XSS, etc.) y el estándar OWASP Top 10. También dispone de aprendizaje automático para detectar patrones de ataque nuevos.
Evaluación de riesgo en tiempo real (0-day) - Debe evaluar en tiempo real el riesgo de los ataques para **mitigar amenazas desconocidas (0-day)**.	**Sí**	Cloudflare WAF tiene capacidades de evaluación en tiempo real de ataques nuevos (0-day). Además, Flumotion incluye en su propuesta la funcionalidad *Super Bot Fight Mode*, que emplea machine learning e IA para distinguir tráfico malicioso desconocido.
Inspección de tráfico HTTPS cifrado - Capacidad de **inspeccionar HTTPS** sin comprometer privacidad ni rendimiento.	**Sí**	Cloudflare intercepta y analiza tráfico HTTPS en sus data centers sin afectar rendimiento ni privacidad. La oferta afirma que inspecciona tráfico cifrado sin comprometer rendimiento. Cloudflare utiliza certificados propios y optimizaciones para asegurar mínima latencia. APB se beneficiará de inspección SSL a nivel global sin impacto perceptible.
Reglas de seguridad personalizadas - Posibilidad de definir **reglas WAF personalizadas** por aplicación, subdominio o servicio.	**Sí**	Cloudfare permite definir reglas WAF personalizadas fácilmente. En la oferta se menciona que los operadores de APB pueden crear reglas propias para bloquear tráfico no deseado (por IP, país, patrones específicos) utilizando el potente motor de reglas de Cloudflare. Además, se incluye la posibilidad de reglas personalizadas por área/subdominio (hasta 2 por cada, ampliables) durante la implantación.
Clasificación de peticiones con IA - La solución debe usar **Machine Learning/AI** para clasificar en tiempo real las peticiones HTTP según su riesgo potencial.	**Sí**	Cloudfare utiliza el Super Bot Fight Mode, clasifica el tráfico automatizado con una puntuación de 1 bot a 100 humano en tiempo real. Esta clasificación basada en ML/IA evalúa cada petición o sesión por su probabilidad de ser

		maliciosa, permitiendo aplicar umbrales de seguridad dinámicos. Es exactamente el enfoque de clasificación inteligente de tráfico que el pliego pretendía.
Funcionalidad de Rate Limiting - Debe incluir **limitación de tasas** de peticiones por usuario/IP en cierto periodo (para mitigar abusos).	**Sí**	La propuesta de Flumotion incluye explícitamente el servicio Rate Limiting avanzado de Cloudflare. La oferta detalla que el *Rate Limiter* se puede aplicar a tráfico definido muy granularmente, contando peticiones y definiendo acciones al exceder el límite.
Protección frente tráfico automatizado (Bots) - Debe incluir protección nativa contra **bots maliciosos**, con despliegue sencillo y **sin necesidad de agentes** en clientes.	**Sí**	Cloudflare cuenta con Bot Management nativo que no requiere agentes. *Super Bot Fight Mode* detecta bots avanzados y evasivos en el tráfico de APB sin necesidad de nada en el cliente. Emplea huellas de reputación global y ML para distinguir bots humanos. La oferta explica que se pueden bloquear bots automáticamente con esa funcionalidad. También admite listas blancas para no interferir con tráfico legítimo.
Propagación ágil de reglas WAF - Los cambios en reglas WAF deben propagarse en **<10 segundos** en la red.	**Sí**	La propuesta de Flumotion señala que los cambios en reglas WAF se propagan en menos de 10 segundos globalmente. Se remarca que es "de las tecnologías más rápidas" en aplicar cambios, manteniendo la seguridad lo más actualizada posible.
Protección de APIs - Debe ofrecer funcionalidades específicas para proteger **APIs** (validación de esquemas, tokens, autenticación reforzada, etc.).	**Sí**	Incluye Cloudflare API Shield en su propuesta, lo que proporciona descubrimiento y protección de APIs expuestas. Cloudflare API Shield permite definir políticas basadas en esquemas, así como autenticación mutua mTLS para clientes API. Estas funciones brindan visibilidad de las APIs en uso y control granular, exactamente conforme a lo exigido.
Detección de credenciales comprometidas (ATO) - Debe poder identificar **credenciales comprometidas** de la APB para prevenir **tomas de control de cuentas.**	**Sí**	Cloudflare dispone de un sistema específico de identificación de credenciales comprometidas de usuarios. La oferta menciona que, mediante ese sistema, se ayuda a prevenir tomas de control de cuentas.
Gestión de certificados		
Gestión de certificados (manual) - Posibilidad de **emitir y renovar manualmente ~200 certificados** por dominio, con hasta **50 SANs por certificado**.	**Sí**	La oferta de Flumotion especifica claramente que puede generar y gestionar al menos 200 certificados SSL para APB, con hasta 50 subdominios adicionales (SAN) por certificado. En la oferta se detalla que Cloudflare emite certificados (firmados por CAs reconocidas

		como Google Trust/Let's Encrypt) con validez configurable y que cubren hasta 50 SANs. Esto confirma expresamente el cumplimiento de las cifras requeridas (200 certs/50 SAN).
Gestión de certificados (automática) - Emisión y renovación automática de certificados SSL/TLS para todos los subdominios protegidos, **sin limitación**.	**Sí**	La propuesta de Flumotion señala que la solución presenta generación y gestión automática de certificados SSL para las propiedades web de APB. Cloudflare emite y renueva automáticamente certificados (dual RSA/ECDSA) para todos los subdominios proxificados, sin límite práctico.
Cifrado resistente cuántico - Soporte de algoritmos criptográficos **post-quantum** (resistentes a computación cuántica) en el intercambio de claves TLS.	**Sí**	Flumotion destaca que Cloudflare ya soporta cifrado post-cuántico: siempre que el cliente lo permita, Cloudflare negociará TLS usando algoritmos post-cuánticos (ej. Kyber híbrido con X25519). Esto asegura resiliencia criptográfica futura. La propuesta de Flumotion ofrece explícitamente esta capacidad de vanguardia.
Visibilidad y control		
Panel de control en tiempo real - Disponibilidad de un **dashboard** en vivo, con métricas claras de tráfico, ataques y rendimiento.	**Sí**	Como indicado, APB dispondrá del panel Cloudflare con datos en tiempo real. La oferta describe que Cloudflare proporciona paneles analíticos avanzados en tiempo real para monitorizar sus servicios. Además, incluye monitores activos que actualizan el estado al instante en el panel.
Analítica avanzada con filtrado - Acceso a **paneles analíticos avanzados**, con filtros por hostname, IP, código, URL, y análisis por rangos temporales específicos.	**Sí**	El panel de Cloudflare permite filtrar y segmentar datos por multitud de parámetros. Si bien la oferta no enumera cada filtro, sí menciona visibilidad de APIs, tráfico por servicios, etc. y la disponibilidad de analíticas web detalladas. Dado que Cloudflare expone incluso consultas via GraphQL API para datos históricos, es evidente que APB podrá filtrar por rango temporal, por dominio, tipo de tráfico, etc.
Actualización en tiempo real - Los paneles deben **actualizarse en tiempo real** sin recarga manual.	**Sí**	Los paneles de Cloudflare son interactivos y se actualizan en tiempo real sin intervención manual. La oferta describe "tiempo real mediante paneles analíticos avanzados", implicando actualización continua. Adicionalmente, Cloudflare envía notificaciones push (correo, 829webhook) que reflejan eventos en el panel automáticamente.
Integración con SIEM - La plataforma debe ser integrable con los **SIEM** existentes de la APB.	**Sí**	La propuesta de Flumotion satisface este requisito. La oferta indica que Cloudflare permite exportar logs por múltiples medios (API,

		Syslog, conectores SIEM) hacia plataformas externas como Splunk. Es decir, APB podrá integrar fácilmente los eventos en su SIEM existente, ya sea consumiendo vía Syslog directo o mediante los conectores nativos que ofrece Cloudflare.
Alertas configurables - Soporte de **alertas por email o webhook** ante eventos de seguridad o indisponibilidad.	**Sí**	La solución propuesta de Flumotion resalta que Cloudflare genera notificaciones configurables por email o webhook ante diversos eventos de seguridad. Se menciona la capacidad de enviar alertas a los operadores de APB cuando ocurre un evento de seguridad (ej. ataque DDoS). También en la sección de monitorización se especifica que fallos en *health checks* pueden disparar alertas por correo o webhook según preferencia del cliente.
Reportes periódicos automáticos - Capacidad de generar y enviar **informes periódicos** con métricas clave de seguridad y cumplimiento.	**Si**	La oferta de Flumotion no detalla explícitamente el envío de informes periódicos programados, pero dado el ecosistema Cloudflare, es posible con Analytics. Cloudflare permite extraer datos vía API/GraphQL para generar informes personalizados, y con las notificaciones y panel histórico APB podría obtener reportes regulares.
Mitigación DDoS		
Mitigación DDoS L3/L4 - Protección a nivel de red (capas **L3 y L4**) contra ataques volumétricos y de protocolo.	**Sí**	Cloudfare ofrece protección DDoS integral en todas las capas. Cloudflare tiene uno de los sistemas DDoS más robustos del mercado, con mitigación distribuida a nivel de red (L3/L4) automática. La oferta indica explícitamente que el sistema DDoS de Cloudflare cubre ataques de red volumétricos y de protocolo, con un Tiempo de Mitigación ~3 segundos.
Mitigación DDoS L7 - Protección a nivel **aplicación (L7)** contra ataques dirigidos a vulnerabilidades web o recursos lógicos.	**Sí**	Una vez el tráfico llega a Cloudflare, se analiza y filtra también a nivel L7. La oferta señala que tras el cambio DNS, todo tráfico web de APB pasará por Cloudflare donde se mitigarán ataques de denegación de servicio a nivel de aplicación, protegiendo contra exploits web y abusos lógicos. Además, el WAF y las reglas de rate limiting complementan la mitigación L7.
Mitigación automática en segundos - Capacidad de **detección y neutralización automática** de ataques DDoS, sin intervención manual, con respuesta en **segundos**.	**Sí**	La solución de Flumotion opera de forma altamente automática: su mitigación DDoS detecta y contrarresta ataques sin intervención humana, en cuestión de 1-3 segundos típicamente. Esto está respaldado por la métrica de TTM ~3s mencionada.

Características avanzadas		
CDN global con Anycast - Integración con una red CDN de gran capacidad, con tecnología **Anycast** y presencia a nivel global.	**Sí**	Cloudflare es pionera en Anycast: su red global anuncia las mismas direcciones IP en todos sus data centers, dirigiendo automáticamente a cada usuario al centro más cercano. La oferta resalta la "huella en más de 320 ciudades" y ser la red más interconectada, con <50ms de latencia para la mayoría de los usuarios.
Servicios completos en cada PoP - Los puntos de presencia deben proporcionar **todos los servicios** ofertados (no solo CDN, sino también WAF, DDoS, etc.).	**Sí**	En Cloudflare, todos los puntos de presencia ofrecen la gama completa de servicios: cada datacenter ejecuta el WAF, el motor de bots, DDoS, cache, etc. La oferta de Flumotion no distingue roles de PoPs; al contrario, la configuración Full Setup implica que cualquier nodo atiende cualquier funcionalidad necesaria para los dominios de APB. Cloudflare no segmenta capacidades por PoP, así que este requisito se cumple de manera natural.
Reglas gestionadas auto-actualizadas - Uso de reglas gestionadas que se **actualizan automáticamente** basadas en inteligencia global de amenazas.	**Sí**	Las reglas gestionadas de Cloudflare se actualizan continuamente mediante la inteligencia global que recopila su equipo de seguridad. La oferta indica que Cloudflare cubre nuevos tipos de ataques rápidamente con sus reglas gestionadas. También menciona que evalúa ataques 0-day en tiempo real. Cloudflare mantiene una base de datos de amenazas global, actualizando automáticamente las contramedidas.
Funciones serverless personalizadas - Soporte para ejecutar **lógica personalizada en el edge** mediante tecnologías *serverless* (p. ej. funciones para gestión de tráfico, bots, rate limiting).	**Sí**	La plataforma Cloudflare dispone de funciones *serverless* (llamadas Cloudflare Workers), que permiten ejecutar código personalizado en su edge (para lógicas de negocio, manipulación de tráfico, etc.).
Control avanzado de bots (sin fricción) - Soluciones avanzadas de gestión de bots con mecanismos de **detección, desafío y verificación** sin fricción para usuarios legítimos.	**Sí**	*Super Bot Fight Mode* proporciona control avanzado de bots con detección y acciones de desafío/verificación automáticas. La oferta detalla que Cloudflare asigna un score a cada cliente (bot vs humano) y permite desplegar protecciones automáticas para bloquear bots. Adicionalmente, Cloudflare puede requerir CAPTCHA o JavaScript challenge a tráfico sospechoso de ser bot, todo ello de manera transparente para usuarios legítimos.

Que la empresa **NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.** aporta documento con la descripción propuesta; **sin embargo, en la documentación presentada no se acreditan ni se describen de forma expresa determinadas características técnicas mínimas exigidas en el PPT**, las cuales se detallan a continuación de manera exhaustiva.

Características mínimas	**Cumplimiento**	**Comentarios y justificación**
Infraestructura		
Capacidad mínima CDN y cobertura - Soportar **≥6 TB/mes** de tráfico CDN y **≥50 millones peticiones/mes**, con **WAF** y mitigación **DDoS sin límite** de tráfico, *rate limiting* hasta **10 millones/mes**, servicio de soporte estándar, cubriendo **hasta 4 dominios** principales.	**Sí**	NTT DATA dimensiona su solución justamente con esos valores mínimos: la CDN propuesta soporta *6 TB/mes*, *50 millones* de peticiones mensuales, protección DDoS sin límite de tráfico, WAF sin límite, *rate limiting* hasta *10 millones* de solicitudes al mes, y cubre 4 dominios. Cumple por tanto la capacidad requerida.
Infraestructura de la plataforma CDN - El proveedor debe tener presencia de red en **>2 ciudades de España** (al menos 3 PoPs en España) y nodos en Europa, garantizando **baja latencia** y alineación con marcos/certificaciones exigibles.	**Sí**	La solución de NTT (Transparent Edge) dispone de más de 70 PoPs globales, 3 de ellos en España, distribuidos en Europa, América, Asia, etc., lo que cumple con la exigencia de presencia en múltiples ciudades españolas y Europa. Esto asegura baja latencia (contenido servido desde el nodo más cercano).
Plataforma unificada - La solución debe incluir **en una única plataforma integrada** los servicios de **DNS, CDN, WAF, mitigación DDoS y Rate Limiting**, con gestión centralizada.	**Sí**	NTT DATA propone una plataforma unificada (Transparent Edge) que integra todos esos servicios en un solo panel. Indica explícitamente "una única plataforma para todos los servicios", centralizando la entrega de contenidos y la seguridad (CDN, WAF, DDoS, rate limiting, DNS). Cumple con la necesidad de solución todo en uno.
Despliegue rápido de cambios - Cualquier cambio de configuración debe poder propagarse en la red en **<5 segundos**.	**No se menciona en la propuesta presentada**	Se requerirá evidencia de que la plataforma Transparent Edge cumpla con la característica técnica mínima.
Sin limitaciones de tráfico - La plataforma **no debe imponer limitaciones** de ancho de banda ni peticiones por segundo (tráfico ilimitado).	**Sí**	NTT DATA cumple este requisito. Su oferta indica explícitamente que la protección DDoS es "sin límite de tráfico" y que el WAF no impone límites de tráfico. Es decir, no se imponen topes de ancho de banda ni de peticiones por segundo a la solución propuesta, tal como exige el pliego.

Autenticación multifactor (MFA) - Debe ofrecer **MFA** para el acceso administrativo a la plataforma.	**No se menciona en la propuesta presentada**	Se requerirá evidencia de que la plataforma Transparent Edge cumpla con la característica técnica mínima.
Seguridad web (WAF)		
Visibilidad de seguridad completa - Debe proporcionar **panel de control en tiempo real** con métricas claras de tráfico, ataques y rendimiento.	**Sí**	Transparent Edge ofrece visibilidad completa mediante un panel unificado con analítica en tiempo real de tráfico y eventos de ciberseguridad. Además, almacena y muestra datos detallados de cada petición (IP, URL, país, código, etc.) para tener trazabilidad completa. Esto cumple el requisito de monitorización clara y en vivo de tráfico y posibles ataques.
Protección OWASP y reglas gestionadas - Debe cubrir ataques típicos (OWASP Top 10) y exploits emergentes, y disponer de **conjuntos de reglas de seguridad gestionadas actualizadas**.	**Sí**	Transparent Edge cumple este requisito. Su WAF incluye las reglas OWASP Top 10 configuradas por defecto y un *Core Rule Set* actualizado constantemente para detectar los últimos ataques. Ofrece protección específica contra ataques de aplicación comunes: SQLi, XSS, CSRF, etc... Las reglas gestionadas se mantienen al día, minimizando falsos positivos, tal como exige el pliego.
Evaluación de riesgo en tiempo real (0-day) - Debe evaluar en tiempo real el riesgo de los ataques para **mitigar amenazas desconocidas (0-day)**.	**Sí**	La solución de NTT emplea técnicas de Machine Learning para análisis de patrones y detección de anomalías en tiempo real, incluso frente a amenazas nuevas. Indican que el sistema perfila el tráfico por host e identifica alteraciones sospechosas de forma autónoma. Puede notificar o bloquear automáticamente peticiones anómalas, adelantándose a ataques no conocidos.
Inspección de tráfico HTTPS cifrado - Capacidad de **inspeccionar HTTPS** sin comprometer privacidad ni rendimiento.	**Sí**	La plataforma ofertada por NTT DATA (Transparent Edge) inspecciona el tráfico HTTPS en el propio nodo *edge*. El WAF está integrado en la CDN, lo que añade mínima latencia al filtrar tráfico cifrado en el edge. Soporta cifrado TLS y la oferta menciona explícitamente esa capacidad. Por tanto, es capaz de inspeccionar tráfico SSL/TLS entrante sin degradar significativamente el rendimiento ni violar la privacidad (el descifrado ocurre en nodos seguros de la red de Transparent Edge).
Reglas de seguridad personalizadas - Posibilidad de definir **reglas WAF personalizadas**	**Sí**	Transparent Edge permite reglas personalizadas en su WAF: la solución se puede configurar vía código (VCL) en el edge, al ser parte integral

por aplicación, subdominio o servicio.		de la plataforma. Esto implica flexibilidad para implementar reglas específicas por sitio o servicio. También admite excepciones a reglas, firmas personalizadas y listas blancas/negras, cubriendo la definición de políticas a medida por aplicación o dominio.
Clasificación de peticiones con IA - La solución debe usar **Machine Learning/AI** para clasificar en tiempo real las peticiones HTTP según su riesgo potencial.	**No se menciona en la propuesta presentada**	Se requerirá evidencia de que la plataforma Transparent Edge cumpla con la característica técnica mínima.
Funcionalidad de Rate Limiting - Debe incluir **limitación de tasas** de peticiones por usuario/IP en cierto periodo (para mitigar abusos).	**Sí**	Transparent Edge integra *Rate Limiting*: se menciona explícitamente tanto en el dimensionamiento (reglas de limitación para hasta 10M solicitudes/mes) como en las características del WAF (incluye *"Rate limit"* como funcionalidad configurable). Por tanto, la solución permite establecer umbrales de peticiones por IP/usuario para prevenir abusos, tal como requiere el PPT.
Protección frente tráfico automatizado (Bots) - Debe incluir protección nativa contra **bots maliciosos**, con despliegue sencillo y **sin necesidad de agentes** en clientes.	**Sí**	Transparent Edge ofrece un servicio dedicado de Bot Mitigation en el edge para tráfico automatizado. Detecta y responde en tiempo real a bots avanzados que imitan comportamiento humano. Su solución identifica IPs maliciosas globalmente sin necesidad de instalar agentes en los clientes. Además, permite listas blancas/negras y aplica un sistema de puntuación global (basado en 350 criterios) para bloquear bots evasivos.
Propagación ágil de reglas WAF - Los cambios en reglas WAF deben propagarse en **<10 segundos** en la red.	**No se menciona en la propuesta presentada**	Se requerirá evidencia de que la plataforma Transparent Edge cumpla con la característica técnica mínima.
Protección de APIs - Debe ofrecer funcionalidades específicas para proteger **APIs** (validación de esquemas, tokens, autenticación reforzada, etc.).	**Sí**	La oferta de NTT DATA incluye protección de APIs. Explica un módulo dedicado que carga especificaciones OpenAPI/Swagger y aplica un modelo de seguridad positivo: bloquea llamadas a endpoints no definidos o métodos no permitidos, valida estrictamente los parámetros según el esquema esperado, etc. Esto reduce drásticamente la superficie de ataque de las APIs, cumpliendo con la validación de esquemas exigida. También soporta autenticación reforzada: permite mutual TLS (según necesidad) y manejo de tokens/API keys

		(mencionado en la oferta).
Detección de credenciales comprometidas (ATO) - Debe poder identificar **credenciales comprometidas** de la APB para prevenir **tomas de control de cuentas.**	**No se menciona en la propuesta presentada**	Se requerirá evidencia de que la plataforma Transparent Edge cumpla con la característica técnica mínima.
Gestión de certificados		
Gestión de certificados (manual) - Posibilidad de **emitir y renovar manualmente ~200 certificados** por dominio, con hasta **50 SANs por certificado**.	**No se menciona en la propuesta presentada**	Se requerirá evidencia de que la plataforma Transparent Edge cumpla con la característica técnica mínima.
Gestión de certificados (automática) - Emisión y renovación automática de certificados SSL/TLS para todos los subdominios protegidos, **sin limitación**.	**No se menciona en la propuesta presentada**	Se requerirá evidencia de que la plataforma Transparent Edge cumpla con la característica técnica mínima.
Cifrado resistente cuántico - Soporte de algoritmos criptográficos **post-quantum** (resistentes a computación cuántica) en el intercambio de claves TLS.	**No se menciona en la propuesta presentada**	Se requerirá evidencia de que la plataforma Transparent Edge cumpla con la característica técnica mínima.
Visibilidad y control		
Panel de control en tiempo real - Disponibilidad de un **dashboard** en vivo, con métricas claras de tráfico, ataques y rendimiento.	**Sí**	Transparent Edge ofrece un panel centralizado con monitorización en tiempo real tanto de métricas de CDN (tráfico web) como de los servicios de seguridad (WAF, DDoS, bots). Se actualiza continuamente y proporciona visibilidad instantánea de eventos de seguridad y rendimiento. Esto cumple la necesidad de un dashboard en vivo para supervisar el estado de las webs de la APB.
Analítica avanzada con filtrado - Acceso a **paneles analíticos avanzados**, con filtros por hostname, IP, código, URL, y análisis por rangos temporales específicos.	**Sí**	La solución de NTT DATA proporciona analíticas detalladas: su herramienta de análisis almacena cada petición durante al menos una semana y permite filtrar consultas por IP, sitio web, URL, país, User-Agent, código de estado, tipo de contenido, etc. También ofrece datos históricos (1 semana) además de tiempo real.
Actualización en tiempo real - Los paneles deben **actualizarse en tiempo real** sin recarga manual.	**Sí**	Se infieren capacidades en tiempo real, aunque NTT DATA no lo enuncia textualmente en su oferta. Dado que su plataforma habla de analítica "en tiempo real", es de suponer que los

		dashboards se actualizan dinámicamente. No se menciona necesidad de refresco manual, cumpliendo implícitamente el requisito. *No obstante, la oferta no lo especifica de forma explícita.*
Integración con SIEM - La plataforma debe ser integrable con los **SIEM** existentes de la APB.	**No se menciona en la propuesta presentada**	Se requerirá evidencia de que la plataforma Transparent Edge cumpla con la característica técnica mínima.
Alertas configurables - Soporte de **alertas por email o webhook** ante eventos de seguridad o indisponibilidad.	**No se menciona en la propuesta presentada**	Se requerirá evidencia de que la plataforma Transparent Edge cumpla con la característica técnica mínima.
Reportes periódicos automáticos - Capacidad de generar y enviar **informes periódicos** con métricas clave de seguridad y cumplimiento.	**Si**	La oferta de NTT DATA no aporta información sobre generación de informes automáticos periódicos. No se describe ningún mecanismo de reporte programado hacia APB. El requisito del PPT indica que debería haber envíos regulares de informes de seguridad. Al no mencionarlo, NTT no garantiza esta prestación. *La plataforma de Transparent Edge si se puede obtener informes regulares.*
Mitigación DDoS		
Mitigación DDoS L3/L4 - Protección a nivel de red (capas **L3 y L4**) contra ataques volumétricos y de protocolo.	**Sí**	Transparent Edge ofrece mitigación DDoS integral: su solución AntiDDoS protege tanto nivel red (L3/L4) para ataques volumétricos (ej. floods) y de protocolo, como nivel aplicación. Indica que su CDN/WAF de edge detecta y bloquea ataques volumétricos lejos de la infraestructura de APB.
Mitigación DDoS L7 - Protección a nivel **aplicación (L7)** contra ataques dirigidos a vulnerabilidades web o recursos lógicos.	**Sí**	El WAF en los nodos edge analiza el tráfico L7 y bloquea ataques dirigidos a las aplicaciones web (inyecciones, exploits, etc.). De hecho, la oferta destaca protección contra intentos de intrusión y explotación de vulnerabilidades en las apps de APB. Las reglas gestionadas y personalizadas del WAF incluyen mitigaciones para ataques L7 (SQLi, XSS, etc.), cumpliendo la defensa en capa de aplicación.
Mitigación automática en segundos - Capacidad de **detección y neutralización automática** de ataques DDoS, sin intervención manual, con respuesta en **segundos**.	**Sí**	La solución Transparent Edge opera de forma automática. Ante ataques DDoS, la red de Transparent Edge los detecta y mitiga en el *edge* de manera inmediata, sin requerir acciones manuales. Aunque NTT DATA, en su oferta, no cuantifica explícitamente el *Tiempo de Mitigación* en segundos, sí afirma que su

		arquitectura escala y reacciona en tiempo real automáticamente. Dado su diseño distribuido, la respuesta a un ataque es prácticamente instantánea en los nodos cercanos al origen del ataque.
Características avanzadas		
CDN global con Anycast - Integración con una red CDN de gran capacidad, con tecnología **Anycast** y presencia a nivel global.	**Sí**	La propuesta de NTT se basa en Transparent Edge, que tiene una red global de más de 70 nodos *edge*. Aunque NTT no menciona el término "Anycast", su funcionamiento lo implica: los usuarios son atendidos por el nodo más cercano geográficamente y la red puede escalar automáticamente añadiendo nodos en minutos. La amplia huella global y entrega desde el nodo óptimo cumplen con la filosofía Anycast (rápida convergencia hacia el nodo más cercano).
Servicios completos en cada PoP - Los puntos de presencia deben proporcionar **todos los servicios** ofertados (no solo CDN, sino también WAF, DDoS, etc.).	**Sí**	En la arquitectura de Transparent Edge, cada nodo edge ejecuta todos los servicios de seguridad y entrega. La oferta indica que en los nodos edge "se aplican los servicios de ciberseguridad" además de cachear contenido, y que es una plataforma unificada en cada PoP. No hay distinción de nodos con funciones limitadas: todos los PoPs pueden filtrar ataques (WAF/DDoS), entregar contenido y aplicar reglas, como exige el pliego.
Reglas gestionadas auto-actualizadas - Uso de reglas gestionadas que se **actualizan automáticamente** basadas en inteligencia global de amenazas.	**Sí**	Transparent Edge cumple esto a través del *Core Rule Set* de su WAF, mantenido al día con las últimas amenazas. La oferta señala que siempre cuentan con "las últimas reglas para la detección de ataques" gracias a actualizaciones constantes. Asimismo, Transparent Edge al estar certificado por CCN-CERT y usado en organismos nacionales, presumiblemente incorpora *threat intel* global. Por tanto, las reglas gestionadas se mantienen actualizadas automáticamente, alineadas con la inteligencia de amenazas exigida.
Funciones serverless personalizadas - Soporte para ejecutar **lógica personalizada en el edge** mediante tecnologías *serverless* (p. ej. funciones para gestión de tráfico, bots, rate limiting).	**Sí**	La solución propuesta por NTT DATA ofrece esta capacidad mediante la extensión de su CDN con código en el edge. En concreto, Transparent Edge está basada en Varnish Enterprise y permite trasladar lógica de la aplicación al edge mediante scripts VCL (Varnish Configuration Language). Esto

		habilita implementar funciones a medida (por ejemplo, lógica de redirecciones, inspección personalizada, filtrados avanzados) directamente en los nodos, sin infraestructura adicional. Aunque no use el término "serverless", en la práctica cumple el objetivo: posibilitar funciones personalizadas en la red perimetral.
Control avanzado de bots (sin fricción) - Soluciones avanzadas de gestión de bots con mecanismos de **detección, desafío y verificación** sin fricción para usuarios legítimos.	**Sí**	La mitigación de bots de Transparent Edge incluye métodos de bloqueo, CAPTCHA o desafío JavaScript para identificar bots sin afectar al usuario real. De hecho, en el plan de despliegue describen activar modo *producción* con bloqueo, CAPTCHA o *JS challenge* tras un periodo de aprendizaje. Su sistema detecta bots avanzados que simulan humanos y puede desafiarlos sin impacto para usuarios legítimos, ya que distingue con altas garantías el tráfico humano (ej. analizando comportamiento, IP, etc.). Esto corresponde a los mecanismos solicitados (detección más desafío antifricción).

Que la empresa **TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A.** aporta documento con la descripción propuesta, **cumpliendo íntegramente** con las características mínimas exigidas en el PPT, a continuación se detalla el análisis efectuado:

Características mínimas	**Cumplimiento**	**Comentarios y justificación**
Infraestructura		
Capacidad mínima CDN y cobertura - Soportar **≥6 TB/mes** de tráfico CDN y **≥50 millones peticiones/mes**, con **WAF** y mitigación **DDoS sin límite** de tráfico, *rate limiting* hasta **10 millones/mes**, servicio de soporte estándar, cubriendo **hasta 4 dominios** principales.	**Sí**	La oferta de Telefónica (Cloudflare) supera estos mínimos. Declara capacidad para >6 TB mensuales y >50 M peticiones/mes. Cloudflare cuenta con infraestructura global muy sobredimensionada (más de 330 centros de datos) incluyendo España, por lo que tráfico y peticiones máximas no serán problema (prácticamente tráfico ilimitado). Cubre al menos 4 dominios y es escalable a más.
Infraestructura de la plataforma CDN - El proveedor debe tener presencia de red en **>2 ciudades de España** (al menos 3 PoPs en España) y nodos en Europa, garantizando **baja latencia** y alineación con	**Sí**	Cloudflare (propuesta de Telefónica) tiene presencia masiva: 330+ PoPs globales con varios en España (Madrid, Barcelona, etc.). La red Cloudflare está en >320 ciudades y es la red más interconectada del mundo, situándose a <50ms del 95% de la población.

marcos/certificaciones exigibles.		
Plataforma unificada - La solución debe incluir **en una única plataforma integrada** los servicios de **DNS, CDN, WAF, mitigación DDoS y Rate Limiting**, con gestión centralizada.	**Sí**	Telefónica propone usar Cloudflare en modo Autoritativo (Full Setup), haciendo que Cloudflare gestione DNS y todos los servicios en una plataforma única. En dicha configuración, el panel de Cloudflare unifica la gestión de DNS, CDN, seguridad L7, etc., desde un solo interface.
Despliegue rápido de cambios - Cualquier cambio de configuración debe poder propagarse en la red en **<5 segundos**.	**Sí**	Cloudflare destaca por la rapidez en la propagación de cambios. En particular, señala que los cambios en reglas WAF se propagan en <10s, y además la mitigación DDoS tiene TTM ~3s. Aunque no menciona explícitamente "<5s para cualquier cambio", la arquitectura global de Cloudflare es conocida por su inmediatez al aplicar configuraciones.
Sin limitaciones de tráfico - La plataforma **no debe imponer limitaciones** de ancho de banda ni peticiones por segundo (tráfico ilimitado).	**Sí**	Cloudflare posee una capacidad de red enorme (tera-bps), sin imponer límites fijos al tráfico de un cliente. La oferta no fija tope alguno a ancho de banda ni solicitudes; por el contrario, enfatiza la robustez de la infraestructura. Los valores mínimos (6TB/50M) se cumplen con margen, y no se indica restricción superior, por lo que se asume tráfico ilimitado para APB dentro de la oferta.
Autenticación multifactor (MFA) - Debe ofrecer **MFA** para el acceso administrativo a la plataforma.	**Sí**	Cloudflare ofrece autenticación multifactor para el acceso al panel de control (es una plataforma orientada a seguridad). Aunque la oferta de Telefónica no lo menciona textualmente, es sabido que Cloudflare soporta MFA/2FA y SSO para sus cuentas.
Seguridad web (WAF)		
Visibilidad de seguridad completa - Debe proporcionar **panel de control en tiempo real** con métricas claras de tráfico, ataques y rendimiento.	**Sí**	Telefónica provee a APB acceso al completo dashboard en tiempo real de Cloudflare, con visibilidad total de tráfico, rendimiento y ataques. De hecho, Cloudflare incluye incluso monitorización de usuario real (*Real User Monitoring*) y métricas Web Vitals en su panel, enriqueciendo la visibilidad.
Protección OWASP y reglas gestionadas - Debe cubrir ataques típicos (OWASP Top 10) y exploits emergentes, y disponer de **conjuntos de reglas de seguridad gestionadas actualizadas**.	**Sí**	Telefónica (Cloudflare) cubre todas las vulnerabilidades conocidas: su WAF incluye reglas gestionadas creadas por el equipo de seguridad de Cloudflare, abarcando ataques típicos (RCE, SQLi, XSS, etc.) y el estándar OWASP Top 10. También dispone de aprendizaje automático para detectar patrones

		de ataque nuevos.
Evaluación de riesgo en tiempo real (0-day) - Debe evaluar en tiempo real el riesgo de los ataques para **mitigar amenazas desconocidas (0-day)**.	**Sí**	Cloudflare WAF tiene capacidades de evaluación en tiempo real de ataques nuevos (0-day). Además, Telefónica incluye en su propuesta la funcionalidad *Super Bot Fight Mode*, que emplea machine learning e IA para distinguir tráfico malicioso desconocido.
Inspección de tráfico HTTPS cifrado - Capacidad de **inspeccionar HTTPS** sin comprometer privacidad ni rendimiento.	**Sí**	Cloudflare intercepta y analiza tráfico HTTPS en sus data centers sin afectar rendimiento ni privacidad. La oferta afirma que inspecciona tráfico cifrado sin comprometer rendimiento. Cloudflare utiliza certificados propios y optimizaciones (por ej., TLS 1.3, HTTP/3) para asegurar mínima latencia. APB se beneficiará de inspección SSL a nivel global sin impacto perceptible.
Reglas de seguridad personalizadas - Posibilidad de definir **reglas WAF personalizadas** por aplicación, subdominio o servicio.	**Sí**	Cloudfare permite definir reglas WAF personalizadas fácilmente. En la oferta se menciona que los operadores de APB pueden crear reglas propias para bloquear tráfico no deseado (por IP, país, patrones específicos) utilizando el potente motor de reglas de Cloudflare. Además, se incluye la posibilidad de reglas personalizadas por área/subdominio (hasta 2 por cada, ampliables) durante la implantación.
Clasificación de peticiones con IA - La solución debe usar **Machine Learning/AI** para clasificar en tiempo real las peticiones HTTP según su riesgo potencial.	**Sí**	Cloudfare utiliza el Super Bot Fight Mode, que clasifica el tráfico automatizado con una puntuación de 1 (bot) a 100 (humano) en tiempo real. Esta clasificación basada en ML/IA evalúa cada petición o sesión por su probabilidad de ser maliciosa, permitiendo aplicar umbrales de seguridad dinámicos. Es exactamente el enfoque de clasificación inteligente de tráfico que el pliego pretendía (Cloudflare aplica IA tanto para bots como para tráfico anómalo general).
Funcionalidad de Rate Limiting - Debe incluir **limitación de tasas** de peticiones por usuario/IP en cierto periodo (para mitigar abusos).	**Sí**	La propuesta de Telefónica incluye explícitamente el servicio Rate Limiting avanzado de Cloudflare. La oferta detalla que el *Rate Limiter* se puede aplicar a tráfico definido muy granularmente, contando peticiones y definiendo acciones (bloquear, captchas, etc.) al exceder el límite.
Protección frente tráfico automatizado (Bots) - Debe incluir protección nativa contra **bots**	**Sí**	Cloudflare cuenta con Bot Management nativo que no requiere agentes. *Super Bot Fight Mode* detecta bots avanzados y evasivos en el tráfico

maliciosos, con despliegue sencillo y **sin necesidad de agentes** en clientes.		de APB sin necesidad de nada en el cliente. Emplea huellas de reputación global y ML para distinguir bots humanos. La oferta explica que se pueden bloquear bots automáticamente con esa funcionalidad. También admite listas blancas para no interferir con tráfico legítimo.
Propagación ágil de reglas WAF - Los cambios en reglas WAF deben propagarse en **<10 segundos** en la red.	**Sí**	La propuesta de Telefónica señala que los cambios en reglas WAF se propagan en menos de 10 segundos globalmente. Se remarca que es "de las tecnologías más rápidas" en aplicar cambios, manteniendo la seguridad lo más actualizada posible.
Protección de APIs - Debe ofrecer funcionalidades específicas para proteger **APIs** (validación de esquemas, tokens, autenticación reforzada, etc.).	**Sí**	Incluye Cloudflare API Shield en su propuesta, lo que proporciona descubrimiento y protección de APIs expuestas. Cloudflare API Shield permite definir políticas basadas en esquemas (validación de schema), así como autenticación mutua mTLS para clientes API. Estas funciones brindan visibilidad de las APIs en uso y control granular, exactamente conforme a lo exigido.
Detección de credenciales comprometidas (ATO) - Debe poder identificar **credenciales comprometidas** de la APB para prevenir **tomas de control de cuentas.**	**Sí**	Cloudflare dispone de un sistema específico de identificación de credenciales comprometidas de usuarios. La oferta menciona que, mediante ese sistema, se ayuda a prevenir tomas de control de cuentas.
Gestión de certificados		
Gestión de certificados (manual) - Posibilidad de **emitir y renovar manualmente ~200 certificados** por dominio, con hasta **50 SANs por certificado**.	**Sí**	La oferta de Telefónica especifica claramente que puede generar y gestionar al menos 200 certificados SSL para APB, con hasta 50 subdominios adicionales (SAN) por certificado. En la oferta se detalla que Cloudflare emite certificados (firmados por CAs reconocidas como Google Trust/Let's Encrypt) con validez configurable y que cubren hasta 50 SANs. Esto confirma expresamente el cumplimiento de las cifras requeridas (200 certs/50 SAN).
Gestión de certificados (automática) - **Emisión y renovación automática** de certificados SSL/TLS para todos los subdominios protegidos, **sin limitación**.	**Sí**	La propuesta de Telefónica señala que la solución presenta generación y gestión automática de certificados SSL para las propiedades web de APB. Cloudflare emite y renueva automáticamente certificados (dual RSA/ECDSA) para todos los subdominios proxificados, sin límite práctico.
Cifrado resistente cuántico - Soporte de algoritmos criptográficos	**Sí**	Telefónica destaca que Cloudflare ya soporta cifrado post-cuántico: siempre que el cliente lo

post-quantum (resistentes a computación cuántica) en el intercambio de claves TLS.		permita, Cloudflare negociará TLS usando algoritmos post-cuánticos (ej. Kyber híbrido con X25519). Esto asegura resiliencia criptográfica futura. La propuesta de Telefónica ofrece explícitamente esta capacidad de vanguardia.
Visibilidad y control		
Panel de control en tiempo real - Disponibilidad de un **dashboard** en vivo, con métricas claras de tráfico, ataques y rendimiento.	**Sí**	Como indicado, APB dispondrá del panel Cloudflare con datos en tiempo real. La oferta describe que Cloudflare proporciona paneles analíticos avanzados en tiempo real para monitorizar sus servicios. Además, incluye monitores activos (health checks) que actualizan el estado al instante en el panel.
Analítica avanzada con filtrado - Acceso a **paneles analíticos avanzados**, con filtros por hostname, IP, código, URL, y análisis por rangos temporales específicos.	**Sí**	El panel de Cloudflare permite filtrar y segmentar datos por multitud de parámetros. Si bien la oferta no enumera cada filtro, sí menciona visibilidad de APIs, tráfico por servicios, etc. y la disponibilidad de analíticas web detalladas. Dado que Cloudflare expone incluso consultas via GraphQL API para datos históricos, es evidente que APB podrá filtrar por rango temporal, por dominio, tipo de tráfico, etc. (Cloudflare ofrece dashboards filtrables por host, ruta, código, país, etc., alineado al requerimiento).
Actualización en tiempo real - Los paneles deben **actualizarse en tiempo real** sin recarga manual.	**Sí**	Los paneles de Cloudflare son interactivos y se actualizan en tiempo real sin intervención manual. La oferta describe "tiempo real mediante paneles analíticos avanzados", implicando actualización continua. Adicionalmente, Cloudflare envía notificaciones push (correo/webhook) que reflejan eventos en el panel automáticamente.
Integración con SIEM - La plataforma debe ser integrable con los **SIEM** existentes de la APB.	**Sí**	La propuesta de Telefónica satisface plenamente este requisito. La oferta indica que Cloudflare permite exportar logs por múltiples medios (API, Syslog, conectores SIEM) hacia plataformas externas como Splunk. Es decir, APB podrá integrar fácilmente los eventos en su SIEM existente, ya sea consumiendo vía Syslog directo o mediante los conectores nativos que ofrece Cloudflare.
Alertas configurables - Soporte de **alertas por email o webhook** ante eventos de seguridad o	**Sí**	La solución propuesta de Telefónica resalta que Cloudflare genera notificaciones configurables por email o webhook ante diversos eventos de

indisponibilidad.		seguridad. Se menciona la capacidad de enviar alertas a los operadores de APB cuando ocurre un evento de seguridad (ej. ataque DDoS). También en la sección de monitorización se especifica que fallos en *health checks* pueden disparar alertas por correo o webhook según preferencia del cliente.
Reportes periódicos automáticos - Capacidad de generar y enviar **informes periódicos** con métricas clave de seguridad y cumplimiento.	**Si**	La oferta de Telefónica no detalla explícitamente el envío de informes periódicos programados, pero dado el ecosistema Cloudflare, es posible con Analytics. Cloudflare permite extraer datos vía API/GraphQL para generar informes personalizados, y con las notificaciones y panel histórico APB podría obtener reportes regulares.
Mitigación DDoS		
Mitigación DDoS L3/L4 - Protección a nivel de red (capas **L3 y L4**) contra ataques volumétricos y de protocolo.	**Sí**	Cloudfare ofrece protección DDoS integral en todas las capas. Cloudflare tiene uno de los sistemas DDoS más robustos del mercado, con mitigación distribuida a nivel de red (L3/L4) automática. La oferta indica explícitamente que el sistema DDoS de Cloudflare cubre ataques de red volumétricos y de protocolo, con un Tiempo de Mitigación ~3 segundos.
Mitigación DDoS L7 - Protección a nivel **aplicación (L7)** contra ataques dirigidos a vulnerabilidades web o recursos lógicos.	**Sí**	Una vez el tráfico llega a Cloudflare, se analiza y filtra también a nivel **L7 (aplicación)**. La oferta señala que tras el cambio DNS, todo tráfico web de APB pasará por Cloudflare donde se mitigarán ataques de denegación de servicio a nivel de aplicación, protegiendo contra exploits web y abusos lógicos. Además, el WAF y las reglas de rate limiting complementan la mitigación L7.
Mitigación automática en segundos - Capacidad de **detección y neutralización automática** de ataques DDoS, sin intervención manual, con respuesta en **segundos**.	**Sí**	La solución de Telefónica (Cloudfare) opera de forma altamente automática: su mitigación DDoS detecta y contrarresta ataques sin intervención humana, en cuestión de 1-3 segundos típicamente. Esto está respaldado por la métrica de TTM ~3s mencionada.
Características avanzadas		
CDN global con Anycast - Integración con una red CDN de gran capacidad, con tecnología **Anycast** y presencia a nivel global.	**Sí**	Cloudflare es pionera en Anycast: su red global anuncia las mismas direcciones IP en todos sus data centers, dirigiendo automáticamente a cada usuario al centro más cercano. La oferta resalta la “huella en más de 320 ciudades” y ser la red

		más interconectada, con <50ms de latencia para la mayoría de los usuarios.
Servicios completos en cada PoP - Los puntos de presencia deben proporcionar **todos los servicios** ofertados (no solo CDN, sino también WAF, DDoS, etc.).	**Sí**	En Cloudflare, todos los puntos de presencia ofrecen la gama completa de servicios: cada datacenter ejecuta el WAF, el motor de bots, DDoS, cache, etc. La oferta de Telefónica no distingue roles de PoPs; al contrario, la configuración Full Setup implica que cualquier nodo atiende cualquier funcionalidad necesaria para los dominios de APB. Cloudflare no segmenta capacidades por PoP, así que este requisito se cumple de manera natural.
Reglas gestionadas auto-actualizadas - Uso de reglas gestionadas que se **actualizan automáticamente** basadas en inteligencia global de amenazas.	**Sí**	Las reglas gestionadas de Cloudflare se actualizan continuamente mediante la inteligencia global que recopila su equipo de seguridad. La oferta indica que Cloudflare cubre nuevos tipos de ataques rápidamente con sus reglas gestionadas. También menciona que evalúa ataques 0-day en tiempo real. Cloudflare mantiene una base de datos de amenazas global (incl. a través de sus 25+ millones de sitios que protege en Internet), actualizando automáticamente las contramedidas.
Funciones serverless personalizadas - Soporte para ejecutar **lógica personalizada en el edge** mediante tecnologías *serverless* (p. ej. funciones para gestión de tráfico, bots, rate limiting).	**Sí**	La plataforma Cloudflare dispone de funciones *serverless* (llamadas Cloudflare Workers), que permiten ejecutar código personalizado en su edge (para lógicas de negocio, manipulación de tráfico, etc.).
Control avanzado de bots (sin fricción) - Soluciones avanzadas de gestión de bots con mecanismos de **detección, desafío y verificación** sin fricción para usuarios legítimos.	**Sí**	*Super Bot Fight Mode* proporciona control avanzado de bots con detección y acciones de desafío/verificación automáticas. La oferta detalla que Cloudflare asigna un score a cada cliente (bot vs humano) y permite desplegar protecciones automáticas para bloquear bots. Adicionalmente, Cloudflare puede requerir CAPTCHA o JavaScript challenge a tráfico sospechoso de ser bot, todo ello de manera transparente para usuarios legítimos.

En resumen, tras los anteriores comentarios, **SE CONCLUYE** lo siguiente:

- Que la oferta presentada por **FLUMOTION SERVICES, S.A.**, **cumple íntegramente** con las características mínimas exigidas en el apartado 22 del Cuadro de Características del Pliego de condiciones.

- Que la oferta de **NTT SPAIN INTELLIGENT TECHNOLOGIES AND SERVICES, S.L.** presenta **falta de acreditación y descripción** de determinadas características técnicas mínimas exigidas en el apartado 22 del Cuadro de Características del Pliego de condiciones, que son las que se indican a continuación:

  - Despliegue rápido de cambios - Cualquier cambio de configuración debe poder propagarse en la red en <5 segundos.
  - Autenticación multifactor (MFA) - Debe ofrecer MFA para el acceso administrativo a la plataforma.
  - Clasificación de peticiones con IA - La solución debe usar Machine Learning/AI para clasificar en tiempo real las peticiones HTTP según su riesgo potencial.
  - Propagación ágil de reglas WAF - Los cambios en reglas WAF deben propagarse en <10 segundos en la red.
  - Detección de credenciales comprometidas (ATO) - Debe poder identificar credenciales comprometidas de la APB para prevenir tomas de control de cuentas.
  - Gestión de certificados (manual) - Posibilidad de emitir y renovar manualmente ~200 certificados por dominio, con hasta 50 SANs por certificado.
  - Gestión de certificados (automática) - Emisión y renovación automática de certificados SSL/TLS para todos los subdominios protegidos, sin limitación.
  - Cifrado resistente cuántico - Soporte de algoritmos criptográficos post-quantum (resistentes a computación cuántica) en el intercambio de claves TLS.
  - Integración con SIEM - La plataforma debe ser integrable con los SIEM existentes de la APB.
  - Alertas configurables - Soporte de alertas por email o webhook ante eventos de seguridad o indisponibilidad.

- Que la oferta de **TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES DE ESPAÑA, S.A. cumple íntegramente** con las características mínimas exigidas en el apartado 22 del Cuadro de Características del Pliego de condiciones.

2. EN RELACIÓN A LA JUSTIFICACIÓN DE LA OFERTA ECONÓMICA DE LA EMPRESA FLUMOTION SERVICE, EN PRESUNCIÓN DE ANORMALIDAD:

La empresa FLUMOTION SERVICES, S.A. indica en su justificación lo siguiente:

"*Tras revisar la documentación presentada, hemos detectado que, por un error material en la interpretación del pliego, nuestro presupuesto fue calculado para dos (2) años de servicio, cuando las condiciones del contrato establecen una duración total de tres (3) años*."

Con esto no queda acreditado el nuevo importe ofertado, no se aporta ningún análisis económico ni presupuesto adicional, por lo que no queda justificado el importe total ofertado.

Todo lo anterior, sin prejuicio del cumplimiento de los requisitos mínimos exigidos a las empresas:

- Certificado Conformidad con el ENS en categoría MEDIA (como mínimo), en los sistemas de información en los que se sustenten los servicios de consultoría, instalación y soporte de software de ciberseguridad.

- Sistema de Gestión Ambiental basado en la norma ISO 14001 o EMAS o certificación/documento que avale que aplica criterios similares de gestión ambiental

Lo que se informa a los efectos oportunos,

En Palma, a fecha de la firma del documento

La Comisión técnica:

Firmado digitalmente por
Javier Segovia Mascaró
Jefe de Departamento de Desarrollo Tecnológico e Innovación

Firmado digitalmente por
José Miguel Esteve Lledó
Responsable de Sistemas de Información e Infraestructuras TIC