

INF-0020/26

INFORME SOLICITUD DE ASISTENCIA

FIDEICOMISO RD VIAL

ENERO 28, 2026.-

Informe

Luego de un cordial saludo, sirva la presente para exponer consideraciones de la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), respecto al proceso de compra para la **adquisición e Implementación del Sistema para la Gestión de los Peajes a nivel Nacional**, el cual se nos ha presentado como dirección ejecutiva del gabinete de innovación y desarrollo digital.

Observaciones:

- Se adjunta carta de solicitud
- Se adjunta justificación de compra
- Se adjunta ficha técnica

A groso modo se solicita:

- **1 Contratación de un servicio integral de actualización, gestión, operación y recaudación del sistema de peaje nacional, que incluya la adecuación tecnológica, integración, puesta en operación y provisión de los componentes operativos necesarios para la prestación continua del servicio en las veinte (20) estaciones de peaje y sus ciento ochenta y tres (183) carriles.**
- **1 Servicio de licenciamiento e implementación de Software de Back Office Operacional (BOO), incluyendo configuración, puesta en operación y soporte inicial, con capacidad de despliegue en infraestructura de nube segura o equivalente, conforme a las especificaciones técnicas del pliego para las (20) estaciones de peaje.**
- **1 Servicios de Ciberseguridad; Servicios y soluciones que deberán ser provistos:**
 - Análisis de Vulnerabilidades y Pruebas de Penetración (2 veces al año). Incluyendo como mínimo:
 - SQL Injection (SQLi)
 - Command Injection

- XML External Entities (XXE)
- LDAP Injection
- Cross-Site Scripting (XSS) reflejado
- Cross-Site Scripting (XSS) almacenado
- Cross-Site Scripting (XSS) DOM-Based
- Cross-Site Request Forgery (CSRF)
- Escalación horizontal y vertical de privilegios
- Bypass de autenticación
- Fuerza bruta y credenciales débiles
- Token hijacking (JWT, cookies)
- Sesiones con sesiones mal cerradas
- Exposición de Información sensible como datos personales (PII) y contraseñas en texto claro
- Exposición de Información sensible como configuraciones por defecto
- Configuración de headers HTTP, SSL/TLS inseguros
- RCE (Remote Code Execution) mediante objetos deserializados
- Ejecución de archivos maliciosos.
- Firewall de Aplicaciones Web (WAF): inspección y bloqueo de ataques a nivel de aplicación, incluyendo inyección SQL, XSS, ejecución remota de comandos y amenazas identificadas en OWASP Top 10.
- Protección contra ataques DDoS: mitigación de ataques de denegación de servicio a nivel de red y aplicación, asegurando la disponibilidad de la aplicación web incluso ante incidentes de gran escala.
- Seguridad de APIs: descubrimiento automático de APIs expuestas, validación de tráfico legítimo, protección contra abuso, inyección y explotación de vulnerabilidades específicas de APIs.
- Gestión de Bots: detección y bloqueo de tráfico automatizado malicioso, diferenciando entre bots maliciosos y aquellos autorizados (ej. motores de búsqueda, integraciones de terceros).

- Protección avanzada y adaptable: mecanismos de aprendizaje automático (machine learning) para identificar comportamiento anómalo y ajustar políticas de seguridad automáticamente.
- Gestión de incidentes: monitoreo y soporte sobre la aplicación WEB (24x7), especializado para la detección, contención y respuesta ante incidentes de seguridad.
- Mesa de Ayuda: Disponer de un servicio de asistencia técnica para la resolución de incidentes, esto podrá ser vía llamadas telefónicas, apertura de casos mediante una herramienta WEB y correo electrónico.

Conclusión:

Luego de revisar la documentación aportada, verificar la solicitud y sus soportes, evaluamos las especificaciones técnicas y consideramos que cumplen con todos los aspectos necesarios requeridos y no solapan ningún proyecto que haya de ejecutarse desde la Agenda Digital 2030, esta aprobación tiene vigencia hasta el 28 de abril 2026.

Mario Adames

Encargado Departamento Asistencia Técnica Especializada
Oficina Gubernamental de Tecnologías de la Información y Comunicación
(OGTIC)