AUTORIZACION DE ADQUISICIONES TIC

Decreto Reglamentario Nro. 3248/2025, Articulos Nro. 397 y 398.

Considerando las atribuciones y competencias del Ministerio de Tecnologías de la Información y Comunicación (MITIC), en el marco de lo dispuesto en los Artículos Nº 397 y 398 del DECRETO Nº 3248/2025, POR EL CUAL SE REGLAMENTA LA LEY Nº 7408 DEL 30 DE DICIEMBRE DE 2024 “QUE APRUEBA EL PRESUPUESTO GENERAL DE LA NACIÓN PARA EL EJERCICIO FISCAL 2025”, respecto al pedido de autorización realizado a través del Portal de Solicitud de Servicios del MITIC (servicios.mitic.gov.py):

Nro de trámite: 20090

Institución: Administración Nacional de Electricidad - ANDE

Nombre del llamado: LP1923-25 ADQUISICIÓN DE LICENCIAMIENTO Y SOPORTE DE SOLUCIÓN DE CIBERSEGURIDAD WAAP PARA PROTECCIÓN CONTRA ATAQUES EN CAPA DE APLICACIÓN WEBEN NUBE, TAMBIÉN CONOCIDO COMO CLOUD WAAP (WEB APPLICATION FIREWALL + API PROTECTION + BOT MANAGEMENT)

ID del llamado: 466843

Se ha realizado el análisis correspondiente a las ESPECIFICACIONES TÉCNICAS presentadas por la institución requirente, y se concluye:

Autorizado con Observación:

* Se ha realizado el análisis en base a la documentación e información enviada sobre los Lotes/Items correspondientes a ciberseguridad, y se sugiere incorporar: Pruebas de Aceptación y Validación del WAAP El oferente adjudicado deberá realizar, junto con el equipo técnico de la institución, una serie de pruebas para validar la correcta configuración y rendimiento de la solución

Fecha de Emisión: 18-09-2025 14:52:48

Código Verificación:

MInisterio de Tecnologias de la Información y Comunicación (MITIC)

Código de Verificación:
mh1y x8fj szwb
Verifique la validez de este documento en:
https://servicios.mitic.gov.py/validador

AUTORIZACION DE ADQUISICIONES TIC

Decreto Reglamentario Nro. 3248/2025, Articulos Nro. 397 y 398.

de seguridad. Pruebas de Falsos Positivos: Objetivo: Asegurar que el sistema no bloquea el tráfico legítimo y crítico para el negocio. Metodología: Se definirá un conjunto de transacciones de negocio críticas (ej. login, registro, transacciones comerciales) que serán ejecutadas de forma controlada. Criterio de Éxito: La tasa máxima de bloqueo de estas transacciones legítimas (falsos positivos) deberá ser ? 0.1%. Pruebas de Falsos Negativos: Objetivo: Confirmar la capacidad del WAAP para detectar y bloquear ataques conocidos y técnicas de evasión. Metodología: Se ejecutarán inyecciones controladas y verificables utilizando una variedad de payloads (cargas útiles) para simular los siguientes ataques: Inyección SQLi, XSS, SSRF, y Command Injection. Técnicas de evasión de WAF, como el uso de codificaciones alternativas y la ofuscación de payloads. Criterio de Éxito: El WAAP deberá bloquear el 100% de los intentos de ataque detectables en las categorías del OWASP Top 10 para Web y API. Pruebas de Gestión de Bots: Objetivo: Verificar la capacidad del WAAP para diferenciar entre tráfico humano, bots legítimos y bots maliciosos sin afectar la experiencia de usuario. Metodología: Validar el uso de challenges adaptativos invisibles. Verificar la detección de herramientas de automatización (frameworks como Selenium o Puppeteer). Confirmar la aplicación de acciones graduadas contra el tráfico sospechoso (ej. rate limiting dinámico, tarpitting, CAPTCHA). Criterio de Éxito: El sistema debe clasificar el tráfico correctamente y aplicar las acciones de mitigación de forma apropiada y sin generar fricción indebida para usuarios legítimos. El incumplimiento de estos criterios será causal de corrección obligatoria por parte del proveedor antes de que la solución pueda ser puesta en producción.

Fecha de Emisión: 18-09-2025 14:52:48

Código Verificación:

MInisterio de Tecnologias de la Información y Comunicación (MITIC)

Código de Verificación:
mh1y x8fj szwb
Verifique la validez de este documento en:
https://servicios.mitic.gov.py/validador