# Matriz de Riesgos de Ciberseguridad para la Publicación de Trámites Digitales en Internet

## Introducción / Contexto

La digitalización de trámites gubernamentales representa un paso estratégico para la modernización de la Administración Pública Federal (APF), ya que permite a la ciudadanía un acceso más ágil y eficiente a los servicios del Estado. Sin embargo, la exposición de aplicaciones y sistemas en internet incrementa significativamente la superficie de ataque y, por ende, los riesgos de ciberseguridad que pueden comprometer la **confidencialidad, integridad y disponibilidad** de la información.

El presente documento forma parte de la propuesta de directriz alternativa de ciberseguridad de la **ADTDT** y tiene como finalidad identificar y clasificar los principales riesgos asociados a la publicación de trámites digitales en internet.

La fundamentación normativa y técnica de esta matriz se soporta en:

* El **Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información**.
* Disposiciones emitidas por la **CNBV**, aplicables a la gestión de riesgos tecnológicos y de seguridad.
* Normativa del **Banco de México (BANXICO)** en materia de continuidad operativa y seguridad (SPEI).
* Estándar internacional **PCI DSS** para servicios de pago electrónico.
* Marcos de referencia globales como **OWASP Top 10 (2021)**, **ISO/IEC 27001** y **NIST Cybersecurity Framework**.

1. **Objetivo del Documento**

Establecer una **matriz de riesgos de ciberseguridad** específica para trámites digitales gubernamentales expuestos en internet, con el fin de:

* Identificar escenarios de riesgo y amenazas relevantes.
* Evaluar el impacto y la probabilidad de ocurrencia.
* Clasificar los riesgos según niveles de criticidad (**básico, medio, avanzado**).
* Recomendar controles conceptuales que orienten el diseño de políticas y controles técnicos.
* Alinear los riesgos estratégicos con vulnerabilidades técnicas reconocidas en el **OWASP Top 10**.

1. **Alcances Generales**

* **Cobertura**: aplica a todas las aplicaciones web, portales de trámites digitales y sistemas de autenticación expuestos en internet, así como a los componentes tecnológicos que soportan su operación.
* **Exclusiones**: sistemas internos sin exposición a internet, trámites no digitalizados y tecnologías ajenas al ámbito de la dependencia.
* **Responsables**: áreas de TI, responsables de seguridad de la información, custodios de datos y unidades administrativas propietarias de trámites.
* **Aplicabilidad**: inicialmente de carácter interno para la ADTDT, con visión de homologación y aplicación futura a todas las dependencias de la APF.

1. **Matriz de Riesgos**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Riesgo Identificado** | **Escenario** | **Impacto Potencial** | **Probabilidad** | **Nivel de Criticidad** | **Controles Conceptuales Recomendados** | **Referencia OWASP** |
| **Exposición de datos sensibles** | Fuga de información personal o financiera a través de vulnerabilidades en aplicaciones. | Alto: sanciones legales, pérdida de confianza pública, daño reputacional. | Media-Alta | Avanzado | - Cifrado en tránsito y reposo (TLS 1.3, AES-256).- Pruebas de seguridad en aplicaciones.- Clasificación y protección de datos sensibles.- Cumplimiento con la Ley General de Protección de Datos Personales. | **A02 – Cryptographic Failures** |
| **Interrupción de servicio (DDoS o fallas críticas)** | Ataques de denegación de servicio o indisponibilidad en infraestructura. | Alto: interrupción de trámites ciudadanos, afectación a servicios críticos. | Media | Medio/Avanzado | - Soluciones Anti-DDoS.- Balanceo de carga y redundancia.- Plan de Continuidad Operativa (BANXICO/SPEI).- Monitoreo 24/7 en CSOC. | N/A (No cubierto explícitamente en OWASP) |
| **Suplantación de identidad / acceso no autorizado** | Atacantes obtienen credenciales o se hacen pasar por usuarios legítimos. | Alto: fraude, manipulación de trámites, pérdida de confianza. | Media | Avanzado | - MFA.- Políticas de contraseñas seguras.- Monitoreo de accesos sospechosos.- Controles de sesión. | **A01 – Broken Access Control**, **A07 – Identification & Authentication Failures** |
| **Alteración de información o fraude transaccional** | Modificación no autorizada de registros o transacciones de pago. | Alto: invalidez de trámites, fraude económico. | Media | Avanzado | - Controles de integridad en bases de datos.- Segregación de funciones.- PCI DSS para cobros.- Auditorías periódicas de registros. | **A08 – Software & Data Integrity Failures** |
| **Vulnerabilidades técnicas sin remediar** | Falta de actualización de parches y configuraciones seguras. | Medio-Alto: puerta de entrada a ataques. | Alta | Básico/Medio | - Gestión de vulnerabilidades.- Hardening de servidores y aplicaciones.- Monitoreo de configuraciones.- Cumplimiento con CIS Benchmarks. | **A05 – Security Misconfiguration**, **A06 – Vulnerable & Outdated Components** |
| **Ingeniería social y phishing** | Usuarios engañados para entregar credenciales o instalar malware. | Medio-Alto: compromiso de cuentas y servicios. | Alta | Básico/Medio | - Programas de concientización.- Simulaciones de phishing.- Controles antimalware y sandboxing.- Campañas educativas permanentes. | Indirecto (relacionado con A07) |