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

## 1. 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**.

**2. 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**.

**3. 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.