**Documento: Políticas y Lineamientos de Ciberseguridad para la Publicación de Trámites Digitales en Internet**

**1. Introducción / Contexto**

La digitalización de trámites en la Administración Pública Federal (APF) constituye un avance estratégico en la modernización del Estado. La publicación de aplicaciones en internet facilita el acceso de la ciudadanía, pero también implica riesgos que deben gestionarse mediante políticas claras, proporcionales y adaptadas al nivel de criticidad de cada trámite.

Este documento establece las **políticas y lineamientos de ciberseguridad** que deberán observarse para autorizar y mantener trámites digitales en internet, con criterios de aplicación diferenciados en tres niveles: **Básico, Medio y Avanzado**.

**2. Objetivo del Documento**

Definir las políticas de ciberseguridad que regulan la publicación de trámites digitales en internet, asegurando que:

* Se proteja la información de acuerdo con su clasificación.
* Los controles de seguridad sean proporcionales al número de transacciones y usuarios.
* Exista un marco común mínimo para todos los trámites y un esquema escalonado para los de mayor criticidad.

**3. Alcances Generales**

* **Cobertura**: aplica a todos los trámites digitales, portales y aplicaciones expuestas en internet bajo responsabilidad de dependencias de la APF.
* **Exclusiones**: sistemas internos sin exposición pública y proyectos piloto sin interacción ciudadana.
* **Ámbito de aplicación**: inicialmente en la ADTDT, con visión de extensión a toda la APF.

**4. Criterios de Aplicabilidad**

La clasificación de cada trámite en **Básico, Medio o Avanzado** se realizará con base en los siguientes criterios:

1. **Clasificación de la información**
   * Básico: Información pública o de bajo riesgo.
   * Medio: Información personal o de operación interna.
   * Avanzado: Información sensible, financiera o crítica.
2. **Cantidad de datos y transacciones**
   * Básico: Menos de 10,000 registros anuales.
   * Medio: Entre 10,000 y 1 millón.
   * Avanzado: Más de 1 millón.
3. **Cantidad de usuarios**
   * Básico: Menos de 1,000 usuarios.
   * Medio: Entre 1,000 y 100,000.
   * Avanzado: Más de 100,000.

Un trámite será clasificado en el nivel más alto según cualquiera de los tres criterios.

**5. Políticas de Ciberseguridad**

**5.1 Gobernanza y Gestión de Riesgos**

| **Política** | **Básico** | **Medio** | **Avanzado** |
| --- | --- | --- | --- |
| Todo trámite digital deberá contar con un análisis de riesgos antes de su publicación. | ✅ | ✅ | ✅ |
| Los riesgos deberán revisarse al menos una vez al año. |  | ✅ | ✅ |
| Los trámites de alto impacto deberán integrarse a un programa de gestión continua de riesgos con métricas reportables. |  |  | ✅ |

**5.2 Desarrollo Seguro (DevSecOps)**

| **Política** | **Básico** | **Medio** | **Avanzado** |
| --- | --- | --- | --- |
| Todo desarrollo deberá someterse a análisis estático de código antes de su liberación. | ✅ | ✅ | ✅ |
| Los componentes de terceros deberán verificarse contra vulnerabilidades conocidas. | ✅ | ✅ | ✅ |
| Deberán realizarse pruebas dinámicas de seguridad antes de pasar a producción. |  | ✅ | ✅ |
| Los trámites críticos deberán contar con pruebas interactivas (IAST) y revisiones manuales de seguridad. |  |  | ✅ |
| La seguridad deberá integrarse de forma automatizada en el pipeline CI/CD. |  | ✅ | ✅ |

**5.3 Protección de Datos y Criptografía**

| **Política** | **Básico** | **Medio** | **Avanzado** |
| --- | --- | --- | --- |
| Todo dato en tránsito deberá cifrarse con TLS 1.3 o superior. | ✅ | ✅ | ✅ |
| Los datos sensibles en reposo deberán cifrarse con algoritmos robustos (AES-256 o superior). |  | ✅ | ✅ |
| La gestión de llaves y certificados deberá realizarse de forma centralizada. |  | ✅ | ✅ |
| Queda prohibido el uso de protocolos y algoritmos obsoletos (ej. SSL, SHA-1). | ✅ | ✅ | ✅ |

**5.4 Autenticación y Control de Acceso**

| **Política** | **Básico** | **Medio** | **Avanzado** |
| --- | --- | --- | --- |
| Todo trámite deberá contar con políticas de contraseñas robustas y control de sesiones. | ✅ | ✅ | ✅ |
| La autenticación multifactor será obligatoria para administradores y usuarios internos. |  | ✅ | ✅ |
| En trámites críticos, la autenticación multifactor deberá aplicarse a todos los usuarios. |  |  | ✅ |
| Los privilegios deberán revisarse periódicamente bajo el principio de mínimo privilegio. | ✅ | ✅ | ✅ |

**5.5 Monitoreo y Respuesta a Incidentes**

| **Política** | **Básico** | **Medio** | **Avanzado** |
| --- | --- | --- | --- |
| Todo trámite deberá generar registros de seguridad revisables. | ✅ | ✅ | ✅ |
| Los registros deberán enviarse a un SIEM para su correlación. |  | ✅ | ✅ |
| Los trámites críticos deberán integrarse al CSOC nacional con monitoreo en tiempo real. |  |  | ✅ |
| Se deberán realizar simulacros de respuesta a incidentes de forma periódica. |  | ✅ | ✅ |

**5.6 Continuidad Operativa y Resiliencia**

| **Política** | **Básico** | **Medio** | **Avanzado** |
| --- | --- | --- | --- |
| Todo trámite deberá contar con respaldos periódicos y documentar un procedimiento de recuperación. | ✅ | ✅ | ✅ |
| Deberá existir un plan de continuidad operativa probado al menos una vez al año. |  | ✅ | ✅ |
| Los trámites críticos deberán contar con redundancia activa y pruebas de recuperación semestrales. |  |  | ✅ |

**6. Conclusión**

Este documento establece un marco claro y escalonado de políticas de ciberseguridad, aplicables a la publicación de trámites digitales en internet. La clasificación en **niveles de aplicación (Básico, Medio, Avanzado)** permite asegurar un piso común de protección para todos los trámites, al mismo tiempo que exige controles más robustos en aquellos de mayor riesgo, volumen o criticidad.

Con este enfoque, la ADTDT garantiza que la seguridad digital sea gestionada de forma **proporcional, clara y auditable**, facilitando la homologación en toda la APF y fortaleciendo la confianza de la ciudadanía en los servicios digitales del Estado.