

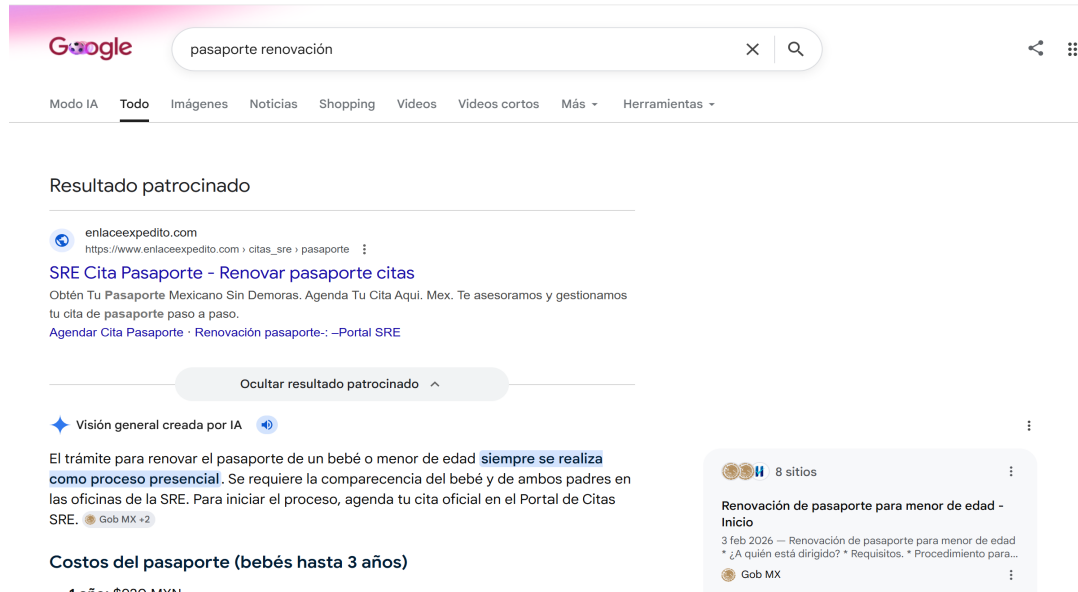
PROPOSICIÓN CON PUNTO DE ACUERDO POR EL QUE LA COMISIÓN PERMANENTE DEL H. CONGRESO DE LA UNIÓN EXHORTA A LA SECRETARÍA DE RELACIONES EXTERIORES, A LA AGENCIA DE TRANSFORMACIÓN DIGITAL Y TELECOMUNICACIONES, A LA FISCALÍA GENERAL DE LA REPÚBLICA Y A LA GUARDIA NACIONAL A FORTALECER LAS ACCIONES DE PREVENCIÓN, ALERTA, DETECCIÓN Y DESACTIVACIÓN DE SITIOS DE INTERNET APÓCRIFOS QUE SUPLANTAN LOS SERVICIOS OFICIALES PARA LA OBTENCIÓN DE CITAS DE PASAPORTE Y OTROS TRÁMITES GUBERNAMENTALES.

Quien suscribe, **Diputado Rubén Ignacio Moreira Valdez**, integrante del Grupo Parlamentario del Partido Revolucionario Institucional, de la LXVI Legislatura de la Cámara de Diputados del Honorable Congreso de la Unión, con fundamento en lo dispuesto por la fracción III del párrafo segundo del artículo 78 de la Constitución Política de los Estados Unidos Mexicanos; 116 y 122, numeral 1, de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos; 58 y 60 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos; y 32 del Acuerdo de la Mesa Directiva de la Comisión Permanente por el que se establecen las Reglas Básicas para el funcionamiento de la Comisión Permanente del H. Congreso de la Unión; someto a consideración de esta Honorable Asamblea, la Proposición con Punto de Acuerdo, al tenor de los siguientes:

CONSIDERANDOS

La transformación digital de los servicios públicos ha permitido que un número cada vez mayor de trámites gubernamentales pueda realizarse mediante plataformas electrónicas, lo que ha contribuido a reducir tiempos, facilitar el acceso de la población y modernizar la relación entre las instituciones públicas y la ciudadanía, sin embargo, el crecimiento de los servicios digitales también ha sido aprovechado por grupos dedicados al fraude electrónico, quienes utilizan herramientas tecnológicas para suplantar la identidad de instituciones públicas y engañar a las personas usuarias.

Uno de los casos que con mayor frecuencia se presenta corresponde al trámite de expedición de pasaportes de la Secretaría de Relaciones Exteriores. El esquema de fraude opera mediante la contratación de anuncios patrocinados en motores de búsqueda de internet, lo que permite que páginas electrónicas apócrifas aparezcan entre los primeros resultados cuando las personas realizan búsquedas con términos como "*citas para pasaporte*", "*cita SRE*" o "*pasaporte mexicano*". Esta estrategia genera que un número importante de personas ingrese, creyendo de buena fe que se trata del portal oficial del Gobierno de México.



Google

pasaporte renovación

Modo IA Todo Imágenes Noticias Shopping Videos Videos cortos Más Herramientas

Resultado patrocinado

enlaceexpedito.com
https://www.enlaceexpedito.com/citas_sre/pasaporte

SRE Cita Pasaporte - Renovar pasaporte citas

Obtén Tu Pasaporte Mexicano Sin Demoras. Agenda Tu Cita Aquí. Mex. Te asesoramos y gestionamos tu cita de pasaporte paso a paso.

Agendar Cita Pasaporte · Renovación pasaporte: -Portal SRE

Ocultar resultado patrocinado

Visión general creada por IA

El trámite para renovar el pasaporte de un bebé o menor de edad **siempre se realiza como proceso presencial**. Se requiere la comparecencia del bebé y de ambos padres en las oficinas de la SRE. Para iniciar el proceso, agenda tu cita oficial en el Portal de Citas SRE. Gob MX +2

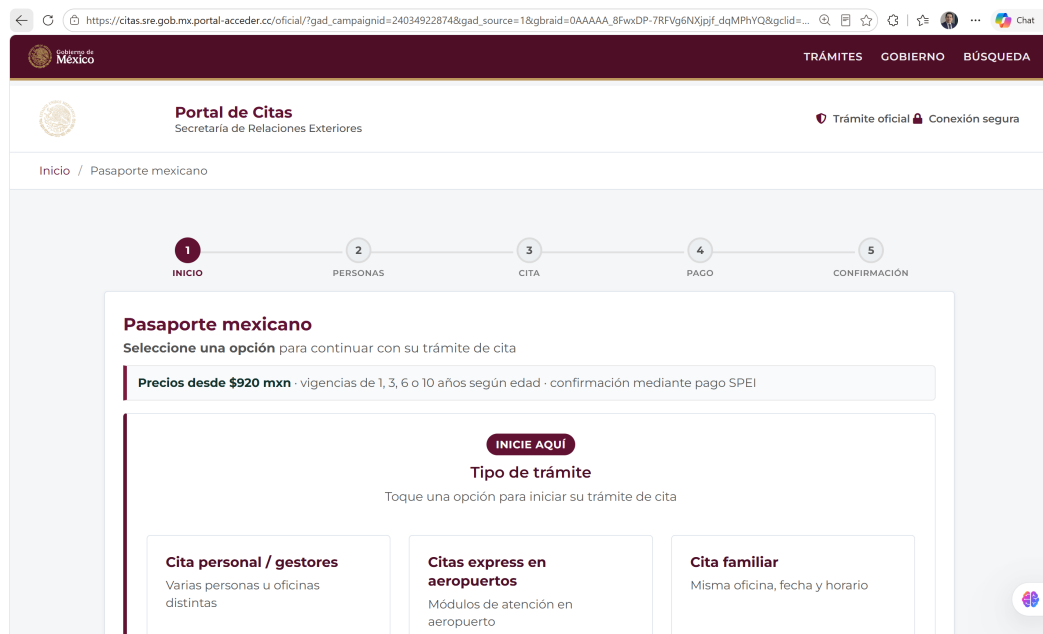
Costos del pasaporte (bebés hasta 3 años)

Renovación de pasaporte para menor de edad - Inicio

3 feb 2026 — Renovación de pasaporte para menor de edad
* ¿A quién está dirigido? * Requisitos. * Procedimiento para...

Gob MX

Una vez dentro del sitio fraudulento, las personas usuarias encuentran una interfaz que reproduce la imagen institucional de la Secretaría de Relaciones Exteriores, utilizando logotipos, colores, tipografía y elementos gráficos similares a los empleados en los portales oficiales. Durante el supuesto proceso de programación de la cita se solicita información personal, como la Clave Única de Registro de Población (CURP) y otros datos de identificación, para posteriormente requerir el pago de una cantidad de dinero con el argumento de concluir el trámite.



Portal de Citas
Secretaría de Relaciones Exteriores

Trámite oficial Conexión segura

Inicio / Pasaporte mexicano

1 INICIO 2 PERSONAS 3 CITA 4 PAGO 5 CONFIRMACIÓN

Pasaporte mexicano

Seleccione una opción para continuar con su trámite de cita

Precios desde \$920 mxn · vigencias de 1, 3, 6 o 10 años según edad · confirmación mediante pago SPEI

INICIE AQUÍ

Tipo de trámite

Toque una opción para iniciar su trámite de cita

Cita personal / gestores
Varias personas u oficinas distintas

Citas express en aeropuertos
Módulos de atención en aeropuerto

Cita familiar
Misma oficina, fecha y horario

 **Portal de Citas**
Secretaría de Relaciones Exteriores

TRÁMITES GOBIERNO BÚSQUEDA

Trámite oficial Conexión segura

Inicio / Pasaporte mexicano / Trámite en línea

Personas hasta pago · Personas → Pago
Desde selección de personas hasta la pantalla de pago: 30 min. En confirmación (CLABE) tendrá otros 30 min aparte para transferir y enviar comprobante. **29:56**

Pasaporte mexicano
Modalidad: Familiar
Registre a cada persona que realizará el trámite

1 INICIO 2 PERSONAS 3 CITA 4 PAGO 5 CONFIRMACIÓN

✎ Escriba su CURP (18 caracteres). La validación es instantánea: fecha, sexo y estado se obtienen al momento, sin consultas externas.

PERSONAS EN EL TRÁMITE 1 persona

0 DE 1 PERSONA LISTA

Persona 1 SOLICITANTE

Tengo CURP Buscar por datos

CURP *

18 CARACTERES

8/18 Validación instantánea al completar 18 caracteres

Ingrese la CURP de cada persona (consulta instantánea)

← Regresar Continuar →

Posteriormente, el sistema despliega instrucciones para efectuar una transferencia electrónica (SPEI) a una cuenta bancaria que se presenta como "datos oficiales para transferencia", indicando el nombre de un supuesto beneficiario, la institución bancaria receptora, una cuenta CLABE, un concepto de pago específico y el monto exacto que debe transferirse para concluir el trámite. Incluso, el sitio ofrece una aparente "garantía de reembolso" y asegura que la cita será confirmada en un plazo determinado, simulando mecanismos de validación propios de una dependencia pública y reforzando la apariencia de autenticidad del portal.

Confirmación y método de pago

Modalidad: Familiar

Revise su cita y elija cómo realizará el pago

1

2

3

4

5

INICIO

PERSONAS

CITA

PAGO

CONFIRMACIÓN

FOLIO DE SEGUIMIENTO

IMPORTE TOTAL

MXPAS-20260718-1140am-MTg2Ljk2LjEzOS4yMzE=

\$2,795.00 MXN

📅 Registrado: 18/07/2026 11:46 am · 1 pasaporte(s)

Cita 1: GUGM880612HDFTNN01 · 25-07-2026 9:30 AM
Oficina de Enlace Zitacuaro, Mich.j — CALLE OCAMPO PTE. No 13 ESQ. 5 DE MAYO (Palacio Municipal), COL. CENTRO C.P.615001 [Ver mapa](#)

👤 Datos del solicitante y desglose

ⓘ Es obligatorio seleccionar su método de pago en un máximo de **30 minutos** desde que registró las **personas (CURP)** hasta esta pantalla (personas → cita → pago). Al pasar a confirmación tendrá un **tiempo independiente de 30 minutos** para enviar su comprobante. De lo contrario, su cita será cancelada y podrá quedar sujeto a **penalización por citas sin pago**, con bloqueo de CURP por al menos **6 meses** en la plataforma oficial y oficinas.

🏠 SELECCIONE SU MÉTODO DE PAGO

🛡️ No cierre ni suspenda esta ventana. Si abandona sin completar el pago y comprobante, la CURP GUGM880612HDFTNN01 quedará sujeta a **bloqueo preventivo por al menos 6 meses** en la plataforma SRE y módulos presenciales.

Transferencia electrónica SPEI **RECOMENDADO**

SPEI
Continuar con SPEI

Tarjeta de crédito o débito **INHABILITADO**

VISA MasterCard
Pasarela no disponible

4

PASO 1 — REALICE SU TRANSFERENCIA SPEI
Use los datos oficiales desde su aplicación bancaria o banca en línea

Datos oficiales para transferencia SPEI
Secretaría de Relaciones Exteriores

INSTRUCCIONES DE PAGO SPEI · SRE

BENEFICIARIO
Relaciones Ext

INSTITUCIÓN BANCARIA
UALA

CLABE INTERBANCARIA
138580200000498927
Clic para copiar CLABE

CONCEPTO DE PAGO
MXP1A3119

\$ IMPORTE EXACTO
\$2,795.00
MXN

1 Capture el **concepto exacto** al transferir para agilizar la validación de su pago.

GARANTÍA EXPRESS
Confirmación en 15 minutos o reembolso al 100%
Si su cita express no se confirma en el plazo, se aplica **reembolso total** conforme a las políticas de la Secretaría. Capture el concepto exacto para agilizar la validación.

¿Por qué utilizamos cuentas digitales? +

Lo más preocupante ocurre una vez que la persona descubre que ha sido víctima del fraude. Al comunicarse con la Secretaría de Relaciones Exteriores para informar que existe una página de internet que suplanta la identidad de la dependencia y continúa engañando a la ciudadanía, la respuesta que recibe es que la Secretaría no solicita depósitos para la obtención de citas y que, al tratarse de un fraude, debe presentar la denuncia correspondiente. Es decir, **la autoridad reconoce que la página es falsa, pero no ofrece una respuesta inmediata para evitar que continúe operando y siga captando nuevas víctimas.**

Posteriormente, al reportar el sitio ante la Policía Cibernética, la orientación consiste en registrar el reporte para que sea analizado y recomendar a la víctima acudir al Ministerio Público a presentar una denuncia. Sin embargo, aun cuando las autoridades ya tienen conocimiento de la existencia de la página fraudulenta y cuentan con la dirección electrónica específica desde la cual se está cometiendo el engaño, ésta permanece activa, **incluso el día de hoy al momento de registrar**

este punto el enlace fraudulento esta activo a pesar de haber sido reportado a la autoridad, es decir, es accesible para cualquier persona que realice una búsqueda en internet.

Resulta inaceptable que un sitio de internet utilizado para cometer fraudes continúe operando con total normalidad aun después de haber sido reportado formalmente a las autoridades competentes. Mientras las víctimas son enviadas de una dependencia a otra para denunciar los hechos, la página sigue funcionando, continúa apareciendo entre los primeros resultados de los motores de búsqueda y continúa obteniendo recursos económicos mediante el engaño de nuevas personas.

En los hechos, la respuesta institucional se limita a advertir a la ciudadanía que no caiga en fraudes y a pedir que las víctimas presenten una denuncia una vez consumado el delito. No existen acciones visibles, oportunas y eficaces para retirar de circulación estos sitios fraudulentos, impedir que continúen operando o evitar que nuevas personas sean afectadas. Esta inacción institucional termina favoreciendo a los delincuentes, quienes saben que pueden mantener activas estas páginas durante días o incluso semanas sin enfrentar una reacción inmediata por parte de las autoridades.

Ante la magnitud de esta estafa la respuesta de la Cancillería ha sido publicar alertas de esta naturaleza

Ap
Ap

La SRE advierte sobre fraudes en trámites de pasaporte: solo paga en bancos autorizados y agenda citas oficiales

Fecha de publicación:
30 de enero de 2026



Síntesis

¿Vas a tramitar tu pasaporte mexicano? Hazlo de forma segura y evita fraudes.

El pago del trámite solo se realiza en bancos autorizados. No pagues en tiendas de conveniencia, no deposites en cuentas personales ni envíes dinero mediante enlaces en redes sociales o mensajes.

Recuerda: en las oficinas de la SRE no se acepta efectivo. La cita es personal, gratuita y sin intermediarios.

Agenda únicamente en <http://citas.sre.gob.mx>

Centro de contacto y WhatsApp: 55 89 32 48 27 (24/7)

¡Evita fraudes!

Ver Perfil

Compartir

Ante la magnitud de este esquema de fraude, resulta preocupante que la principal respuesta de la Secretaría de Relaciones Exteriores haya consistido en la publicación esporádica de comunicados o avisos en sus redes sociales, en los que simplemente se advierte a la población que no realice pagos fuera de los canales oficiales.

Sin embargo, cabe preguntarse si esa medida resulta suficiente frente a un fenómeno que afecta cotidianamente a personas que buscan realizar un trámite oficial. ¿Puede considerarse una estrategia eficaz de prevención una publicación aislada en redes sociales que difícilmente será vista por quienes, precisamente, están siendo dirigidos a páginas fraudulentas mediante motores de búsqueda?

Si la propia Secretaría tiene conocimiento de que su identidad institucional está siendo utilizada para cometer fraudes, resulta razonable esperar una respuesta mucho más contundente y permanente. La advertencia no debería limitarse a una publicación que pasa inadvertida para la mayoría de la ciudadanía; debería existir una campaña permanente de información, alertas visibles en la página oficial de citas, mensajes preventivos durante todo el proceso de obtención del pasaporte, así como una estrategia constante de difusión en redes sociales y otros medios de comunicación.

La prevención no puede descansar exclusivamente en la diligencia de la ciudadanía. Cuando una dependencia pública conoce que su imagen institucional está siendo utilizada para engañar a la población, tiene la responsabilidad de desplegar todas las acciones razonables a su alcance para advertir de manera permanente sobre el riesgo y evitar que más personas sean víctimas de este tipo de fraudes.

Una publicación aislada, por sí sola, difícilmente puede considerarse una respuesta proporcional frente a un esquema delictivo que continúa operando de manera cotidiana, aprovechándose precisamente de la confianza que la población deposita en las instituciones del Estado.

Este fenómeno representa una modalidad de fraude digital particularmente preocupante porque explota la confianza que la ciudadanía deposita en las instituciones públicas. A diferencia de otros esquemas de fraude, en estos casos las personas no buscan realizar operaciones comerciales privadas, sino acceder a un servicio público esencial mediante lo que aparenta ser el portal oficial del Gobierno de México.

Otro cuestionamiento que surge derivado de esta estado es respecto de los mecanismos de prevención implementados por las instituciones del sistema financiero. Los recursos obtenidos mediante estos fraudes no desaparecen; son depositados en cuentas bancarias plenamente identificables, abiertas en instituciones financieras legalmente autorizadas para operar en el país. Ello lleva a preguntarse si los controles de monitoreo y gestión de riesgos permiten detectar oportunamente cuentas que reciben de manera reiterada depósitos de múltiples personas bajo conceptos relacionados con trámites gubernamentales, sin que exista vínculo alguno con la dependencia pública cuya identidad se suplanta.

Lo anterior pone de manifiesto la necesidad de fortalecer una estrategia integral que combine acciones preventivas, campañas permanentes de información, monitoreo del entorno digital y una actuación más eficaz de las autoridades competentes para identificar, investigar y solicitar la desactivación de estos sitios de internet.

Asimismo, resulta indispensable que la ciudadanía pueda identificar con claridad cuáles son los únicos canales oficiales para la obtención de citas, la realización de pagos y el seguimiento de sus trámites. La difusión permanente de esta información constituye una medida preventiva de bajo costo y de alto impacto para reducir el número de personas afectadas.

Por otra parte, la investigación de estos hechos requiere la coordinación de las autoridades encargadas de la persecución de delitos informáticos y de aquellas responsables de la seguridad en el ciberespacio, a fin de identificar a las personas responsables, desarticular las redes que operan este tipo de esquemas fraudulentos y gestionar la baja o bloqueo oportuno de los dominios utilizados para cometer estos delitos.

La protección de la ciudadanía frente a los fraudes digitales constituye una responsabilidad compartida del Estado mexicano. La confianza en los servicios digitales gubernamentales depende no sólo de la calidad de las plataformas oficiales, sino también de la capacidad institucional para prevenir la suplantación de identidad de las dependencias públicas y proteger a las personas frente a quienes buscan aprovecharse de la buena fe de la población.

Por estas razones se somete a la consideración de esta Honorable Asamblea, la siguiente proposición con el siguiente:

PUNTO DE ACUERDO

PRIMERO: La Comisión Permanente del H. Congreso de la Unión exhorta respetuosamente a la Secretaría de Relaciones Exteriores para que fortalezca las campañas permanentes de información y prevención dirigidas a la población sobre la existencia de sitios de internet apócrifos que suplantan los servicios oficiales para la obtención de citas de pasaporte y otros trámites consulares, difundiendo de manera clara y permanente cuáles son los únicos canales oficiales para la programación de citas y la realización de pagos.

SEGUNDO: La Comisión Permanente del H. Congreso de la Unión exhorta respetuosamente a la Agencia de Transformación Digital y Telecomunicaciones para que, en el ámbito de sus atribuciones y en coordinación con las dependencias de la Administración Pública Federal, fortalezca las estrategias de autenticación, verificación e identificación de los portales oficiales del Gobierno de México, así como las acciones de difusión que permitan a la ciudadanía distinguir los sitios oficiales de aquellos utilizados para cometer fraudes electrónicos.

TERCERO: La Comisión Permanente del H. Congreso de la Unión exhorta respetuosamente a la Fiscalía General de la República para que, a través de las unidades competentes en materia de investigación de delitos cibernéticos, fortalezca las acciones de investigación y persecución de las personas físicas o morales que operan sitios de internet utilizados para suplantar la identidad de dependencias del Gobierno Federal con fines de fraude, particularmente aquellos relacionados con la expedición de pasaportes y otros trámites oficiales.

CUARTO. La Comisión Permanente del H. Congreso de la Unión exhorta respetuosamente a la Secretaría de Seguridad y Protección Ciudadana y a la Guardia Nacional, por conducto de las áreas competentes en materia de seguridad cibernética, para que fortalezcan las acciones de monitoreo del ciberespacio, identifique oportunamente sitios de internet utilizados para suplantar la identidad de dependencias del Gobierno Federal y, en coordinación con las autoridades competentes y los proveedores de servicios digitales, impulse las acciones necesarias para su desactivación o baja, así como la emisión de alertas preventivas dirigidas a la ciudadanía.

Dado en el Salón de Sesiones de la Comisión Permanente el 22 de julio del 2026.



DIP. RUBÉN IGNACIO MOREIRA VALDEZ