MANUAL Técnico de la Solución Tecnológica para Instituciones Diversas.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Gobierno de México.

MANUAL TÉCNICO DE LA SOLUCIÓN TECNOLÓGICA PARA INSTITUCIONES DIVERSAS

PLATAFORMA ÚNICA DE IDENTIDAD (PUI)

Versión 1.0| 13/01/2026

Índice

Anexos

1. Introducción

El 27 de noviembre de 2025 se publicaron en el Diario Oficial de la Federación los Lineamientos para el Desarrollo y Operación de la Plataforma Única de Identidad (en adelante, "Lineamientos"), los cuales tienen por objeto establecer las disposiciones generales para el desarrollo de la Plataforma Única de Identidad, los mecanismos mínimos de seguridad, procedimientos, la gestión y control de accesos y trazabilidad de su operación.

La fracción XVII del artículo 5 de los "Lineamientos" establece que el Manual Técnico de la Solución Tecnológica para Instituciones Diversas constituye el documento para las instituciones diversas que con base en lo que disponen dichos "Lineamientos" determina los requisitos, procesos, intercambio de información, interconexión, gestión y trazabilidad para el desarrollo y operación de la Plataforma Única de Identidad para la consulta de información requerida para la investigación, búsqueda, localización e identificación de personas desaparecidas o no localizadas.

El presente Manual da cumplimiento a lo que disponen los artículos 3, 5, fracción XVII, 6, fracción IV, 14, párrafo segundo, 15 y 30 de los "Lineamientos", los cuales establecen los mecanismos mínimos de seguridad, procedimientos, la gestión y control de accesos y trazabilidad de la operación de la Plataforma Única de Identidad.

A través de este Manual se determinan los procedimientos de interconexión a la Plataforma Única de Identidad, a efecto de fortalecer y eficientar las labores de búsqueda mediante la habilitación de un servicio web que pone a disposición distintos endpoints funcionales, orientados a:

1. **La ingesta de nuevos casos de personas desaparecidas o no localizadas.**
2. **La notificación inmediata de coincidencias a las autoridades de búsqueda e investigación registradas.**

Las instituciones diversas que se interconecten a la Plataforma Única de Identidad brindarán información respecto de aquellas personas que tengan asignado un Folio Único de Búsqueda del Registro Nacional de Personas Desaparecidas y No Localizadas (RNPDNO) y, en su caso, el número de carpeta de investigación, para poder realizar la consulta de los datos relacionados con la persona desaparecida o no localizada.

Los Anexos contenidos en el presente Manual deberán utilizarse para facilitar la implementación tecnológica de la PUI y para formalizar la interconexión por parte de las instituciones diversas:

- **Anexo 1:** Ficha técnica de referencia para la integración tecnológica de instituciones diversas a la Plataforma Única de Identidad.
- **Anexo 2:** Guía para el acceso e inscripción de instituciones diversas (personas morales) mediante Llave MX.
- **Anexo 3:** Alcance y descripción del desarrollo tecnológico que deberán implementar las instituciones públicas y diversas.
- **Anexo 4:** Tabla de mapeo de etiqueta y descripción de huellas.
- **Anexo 5:** Tabla de mapeo de códigos de CURP a entidades federativas.

2. Objetivos

1. Establecer el procedimiento para el intercambio controlado de información, mediante servicios web de interoperabilidad con las instituciones diversas, con la finalidad exclusiva de apoyar las acciones de búsqueda y localización de personas desaparecidas o no localizadas.
2. Diseñar y desarrollar un endpoint específico que permita la consulta de reportes activos de personas desaparecidas y no localizadas.
3. Diseñar y desarrollar un endpoint específico para el reporte de hallazgos de coincidencias o de información relevante que contribuya a la búsqueda de una persona desaparecida o no localizada, cuando exista un reporte de desaparición registrado ante las autoridades competentes.
4. Diseñar y desarrollar los procesos internos de búsqueda, diferenciando entre la Búsqueda para completar datos básicos, la Búsqueda histórica y la Búsqueda continua.

3. Fundamento Legal

De manera enunciativa más no limitativa, se indican las disposiciones que sustentan el presente Manual.

1. Constitución Política de los Estados Unidos Mexicanos.
2. Ley Nacional para Eliminar Trámites Burocráticos.
3. Ley Orgánica de la Administración Pública Federal.
4. Ley General en Materia de Desaparición Forzada de Personas, Desaparición Cometida por Particulares y del Sistema Nacional de Búsqueda de Personas.
5. Ley General de Población.
6. Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
7. Reglamento de la Ley General de Población.
8. Reglamento Interior de la Secretaría de Gobernación.
9. Lineamientos para el Desarrollo y Operación de la Plataforma Única de Identidad.

4. Ámbito de Aplicación

El presente Manual define los criterios técnicos aplicables a las instituciones diversas que, en el ámbito de sus operaciones y conforme a la normativa vigente, participen en la interconexión de sus sistemas, bases de datos o registros administrativos a la Plataforma Única de Identidad, contribuyendo con sus acciones a la búsqueda, localización e identificación de personas reportadas como desaparecidas y no localizadas en México. Su alcance comprende la definición de los procedimientos técnicos y operativos que deberán observar las instituciones diversas para garantizar la interconexión de sus sistemas, la transmisión segura de información y la consulta en tiempo real de datos administrativos que faciliten la localización de personas reportadas como desaparecidas.

5. Definiciones y acrónimos

1. **Access Control List (ACL)**

Lista de control de acceso que define los permisos asociados a un recurso, especificando qué usuarios o sistemas pueden acceder a él y qué operaciones pueden realizar. En el contexto de la Plataforma Única de Identidad, las ACL pueden utilizarse para limitar el acceso a información sensible o para definir los privilegios de cada institución conectada.

2. **ATDT**

La Agencia de Transformación Digital y Telecomunicaciones.

3. **API (Application Programming Interface)**

Conjunto de reglas y protocolos que permiten la comunicación entre diferentes sistemas de software.

4. **Bearer token**

Método de autenticación de acceso temporal para solicitudes a una API o web service, el cual se incluye en el encabezado de autorización de una solicitud HTTP o HTTPS.

5. **Búsqueda continua (búsqueda fase 3)**

Consulta periódica automatizada que revisa entradas nuevas o modificadas en la base de datos para detectar coincidencias con personas desaparecidas, con la finalidad de completar sus datos básicos y proveer información de utilidad para su búsqueda. Debe generar un reporte por cada coincidencia encontrada.

6. **Búsqueda histórica (búsqueda fase 2)**

Consulta que se realiza sobre la base de datos institucional desde la fecha de desaparición hasta el momento presente (cuando se da el alta del registro), con la finalidad de completar sus datos básicos y proveer información de utilidad para su búsqueda. En caso de que la fecha de desaparición tenga más de 12 años de antigüedad, deberá acotarse el periodo de búsqueda a los últimos 12 años. Debe generar un reporte por cada coincidencia encontrada.

7. **Búsqueda para completar datos básicos (búsqueda fase 1)**

Consulta automatizada que devuelve los valores más recientes de los campos básicos de que se disponga en las bases de datos, para completar la ficha de búsqueda de la persona desaparecida o no localizada. Debe generar un único reporte en caso de que se encuentre al menos un dato para completar los campos básicos, o ninguno en caso contrario.

8. **Certificado Digital**

Archivo criptográfico que valida la identidad de un emisor y su clave pública, emitido por una autoridad certificadora.

9. **CNB**

Comisión Nacional de Búsqueda de Personas. Institución responsable de coordinar acciones de búsqueda de personas desaparecidas o no localizadas.

10. **Criticidad**

Grado de importancia de un activo, proceso o sistema según su impacto en el negocio si resulta comprometido.

11. **cURL (Client URL)**

Herramienta de línea de comandos que permite transferir datos desde o hacia un servidor utilizando protocolos como HTTP, HTTPS, FTP, entre otros. Muy utilizada para probar endpoints de API o realizar solicitudes web desde scripts.

12. **Endpoint**

Ruta específica dentro de una API que define una funcionalidad disponible para los clientes (por ejemplo, ***/buscar***).

13. **HTTPS (Hypertext Transfer Protocol Secure)**

Versión segura del protocolo HTTP. Utiliza TLS para cifrar la comunicación entre el navegador del usuario y el servidor web, garantizando la confidencialidad e integridad de los datos transmitidos.

14. **ID de búsqueda**

Identificador de la persona desaparecida o no localizada. Se denomina de esta forma al Folio Único de Búsqueda (FUB) con el que se encuentran registradas las personas desaparecidas o no localizadas en el Registro Nacional de Personas Desaparecidas y No Localizadas (RNPDNO), al cual se le agrega un UUID4 para asegurar su unicidad.

15. **Instituciones diversas**

A las encargadas de los registros, bases o sistemas de información que hace referencia el artículo 12 Bis, fracción V de la Ley General en Materia de Desaparición Forzada de Personas, Desaparición Cometida por Particulares y del Sistema Nacional de Búsqueda de Personas, cuya naturaleza jurídica es distinta a las instituciones Públicas, y que conforme a la legislación citada deberán interconectar sus sistemas de información con la Plataforma Única de Identidad.

16. **JSON (JavaScript Object Notation)**

Formato ligero de intercambio de datos, basado en texto, utilizado para estructurar datos en las API.

17. **JWT (JSON Web Token)**

Es un estándar abierto (RFC 7519) que define un método compacto y seguro para representar información entre dos partes como un objeto JSON firmado digitalmente. Se utiliza comúnmente para autenticación y autorización en API.

18. **Log**

Registro estructurado de eventos del sistema, usado para auditoría, depuración y trazabilidad.

19. **Plataforma Única de Identidad (PUI)**

Fuente primaria de consulta permanente y en tiempo real que se interconectará con bases de datos o sistemas de información que permita realizar búsquedas continuas entre registros.

20. **Raw JSON**

Se refiere a un formato JSON (JavaScript Object Notation) en su estado puro, sin ser modificado ni interpretado. Generalmente se utiliza para representar datos estructurados directamente en solicitudes o respuestas HTTP, especialmente en API REST.

21. **REST**

Arquitectura de software para servicios web basada en el uso de métodos HTTP y recursos accesibles mediante URLs.

22. **RENAPO**

A la Dirección General del Registro Nacional de Población e Identidad de la Secretaría de Gobernación.

23. **RNPDNO (Registro Nacional de Personas Desaparecidas y No Localizadas)**

Base de datos nacional que concentra la información de los registros de Personas Desaparecidas y No Localizadas, tanto de la Federación como de las Entidades Federativas, tal como lo menciona la fracción XXI, del artículo 4 de la Ley General en Materia de Desaparición Forzada de Personas, Desaparición Cometida por Particulares y del Sistema Nacional de Búsqueda de Personas, administrada y coordinada por la CNB.

24. **Sandbox**

Entorno de pruebas controlado que simula el comportamiento de un sistema real sin afectar datos en producción.

25. **Seguridad de la Información.**

La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.

26. **TLS (Transport Layer Security)**

Protocolo criptográfico que proporciona comunicaciones seguras por una red, como Internet. TLS es la evolución del SSL y se utiliza para cifrar conexiones HTTPS, asegurando confidencialidad e integridad de los datos.

27. **VPN (Virtual Private Network)**

Tecnología que crea una conexión segura y cifrada sobre una red pública, como Internet. Permite a los usuarios acceder a redes privadas de forma remota, protegiendo la información transmitida y ocultando la dirección IP del usuario.

28. **Vulnerabilidad**

Factor de riesgo de un componente o sistema que está susceptible a sufrir un daño.

29. **UUID4 (Universally Unique Identifier 4)**

Identificador Único Universal versión 4. Es un número de 128 bits representado con 32 dígitos hexadecimales, generado aleatoriamente con el fin de ser usado como identificador. Se concatena con el Folio Único de Búsqueda (FUB) para ser usado en conjunto como identificador (id) de la persona desaparecida o no localizada dentro de la plataforma, previniendo colisiones.

6. Datos Generales del Sistema

El sistema de consulta permanente de coincidencias de registros administrativos de personas desaparecidas o no localizadas se realizará por medio de la Plataforma Única de Identidad, con la información que proporcionen las diversas instituciones participantes. La comunicación se realiza a través de una API con seguridad basada en autenticación[1] mediante *Bearer token* y firmado/validado de la información en formato JSON de respuesta, además del uso de TLS. Toda la información intercambiada debe estar codificada en formato UTF-8, a fin de garantizar la compatibilidad y correcta interpretación de los datos. El objetivo es facilitar el cruce de datos administrativos para identificar coincidencias o posibles indicios de vida, posteriores a la fecha de desaparición.

Flujo del Proceso

1. La CNB o las Comisiones Locales de Búsqueda reciben un reporte de una persona desaparecida o no localizada registrándolo en el RNPDNO. Dichos reportes deberán acompañarse del número de carpeta de investigación correspondiente, la cual será integrada por la Fiscalía Especializada competente, que iniciará de manera inmediata la investigación y dará seguimiento puntual al caso, en términos del marco jurídico aplicable.

2. Una vez registrado, se crea una entrada en el RNPDNO, de donde el reporte de persona desaparecida o no localizada es reenviado automáticamente a la Plataforma Única de Identidad.

[1] **Nota aclaratoria sobre el acceso al sistema:**
Para el uso del sistema basado en API, la seguridad estará garantizada mediante el uso de conexiones seguras a través del protocolo HTTPS, un esquema de autenticación basado en *Bearer Token* y el uso de *Access Control List*. Por lo anterior, no será necesario implementar ni utilizar conexiones VPN, ya que la comunicación segura entre cliente y servidor está asegurada mediante cifrado TLS y control de acceso por token. Este enfoque cumple con las mejores prácticas de seguridad en el consumo de servicios web y permite una integración ágil y segura desde diversas ubicaciones y plataformas.

3. Se envía una notificación a todas las instituciones diversas integradas en la Plataforma Única de Identidad a sus *endpoint* ***/activar-reporte*** con los campos y estructura definidos en la sección Activar reporte de búsqueda de este documento (los campos "*id*" y "*curp*" estarán siempre presentes). Todos los *endpoints* deberán enviar y recibir datos codificados en UTF-8, garantizando la interoperabilidad y correcta interpretación de la información intercambiada.

4. Las instituciones diversas realizan los siguientes pasos:

a. Búsqueda para completar datos básicos (búsqueda fase 1)

Se realiza una búsqueda para remitir los datos más recientes disponibles para la persona reportada como desaparecida o no localizada, con el objetivo de complementar, en caso de que sea necesario, los datos básicos del reporte. Estos datos incluyen: CURP, nombre, primer apellido, segundo apellido, fecha y lugar de nacimiento, sexo asignado, teléfono, correo electrónico, calle, número, colonia, código postal, municipio o alcaldía, entidad federativa, así como fotos y huellas. El reporte debe notificarse a la Plataforma Única de Identidad mediante el *endpoint* ***/notificar-coincidencia*** (omitiendo los campos *tipo_evento*, *fecha_evento*, *descripcion_lugar_evento* y *direccion_evento*, únicamente para esta fase), con el campo *fase_busqueda* con valor "1". En caso de que no se encuentren registros de la persona en las bases, o de que no se cuente con ningún dato para completar, la notificación debe omitirse.

b. Búsqueda histórica (búsqueda fase 2)

Se realiza una búsqueda histórica en sus bases, considerando los registros existentes desde la fecha de desaparición de la persona hasta la fecha actual, considerando que el periodo de búsqueda deberá acotarse a un máximo de 12 años, con fundamento en el artículo 22, fracción II, de los "Lineamientos".

Si el tiempo entre la fecha de desaparición y la creación del reporte supera este periodo, se tomarán sólo los últimos 12 años de datos históricos. Si la fecha de desaparición no está presente (vacía o nula), deberá considerarse como fecha de desaparición la fecha actual (fecha de solicitud de alta del reporte), por lo que se omitirá esta fase de búsqueda en tal caso. Cada coincidencia encontrada, debe notificarse a la plataforma mediante el *endpoint* ***/notificar-coincidencia*** (incluyendo los campos *tipo_evento*, *fecha_evento*, *descripcion_lugar_evento* y *direccion_evento*, además de los campos básicos), con el campo *fase_busqueda* con valor "2".

Una vez concluidos estos dos primeros pasos, la institución diversa deberá reportar la finalización de la búsqueda histórica a través del *endpoint* ***/busqueda-finalizada***. Esto debe realizarse independientemente de que se hayan o no encontrado coincidencias en la fase 2.

c. Búsqueda continua (búsqueda fase 3)

Posteriormente (independientemente de que se hayan o no encontrado coincidencias en la fase 2), se deberá integrar el registro de la persona desaparecida o no localizada, a su sistema de búsqueda continua, el cual deberá revisar periódicamente si hay registros nuevos o modificados que coincidan y reportarlos mediante el *endpoint* ***/notificar-coincidencia*** (incluyendo los campos *tipo_evento*, *fecha_evento*, *descripcion_lugar_evento* y direccion_evento, además de los campos básicos), con el campo *fase_busqueda* con valor "3". La metodología a implementar para la búsqueda continua, así como la periodicidad, dependen de cada institución diversa, pero se considera conveniente que se realice con la mayor frecuencia posible, siempre que no afecte el desempeño de la institución. Las frecuencias típicas de búsqueda son cada hora, cada cuatro horas o una vez al día, pero puede ser menor o mayor que esto. La búsqueda continua de un reporte debe finalizar únicamente cuando se solicite la baja del reporte.

5. La Plataforma Única de Identidad valida los datos recibidos del punto anterior y los envía a CNB de manera automática.

6. Cuando una persona es localizada, CNB cambia el estatus del reporte en el RNPDNO y:

6.1. Se da de baja el caso.

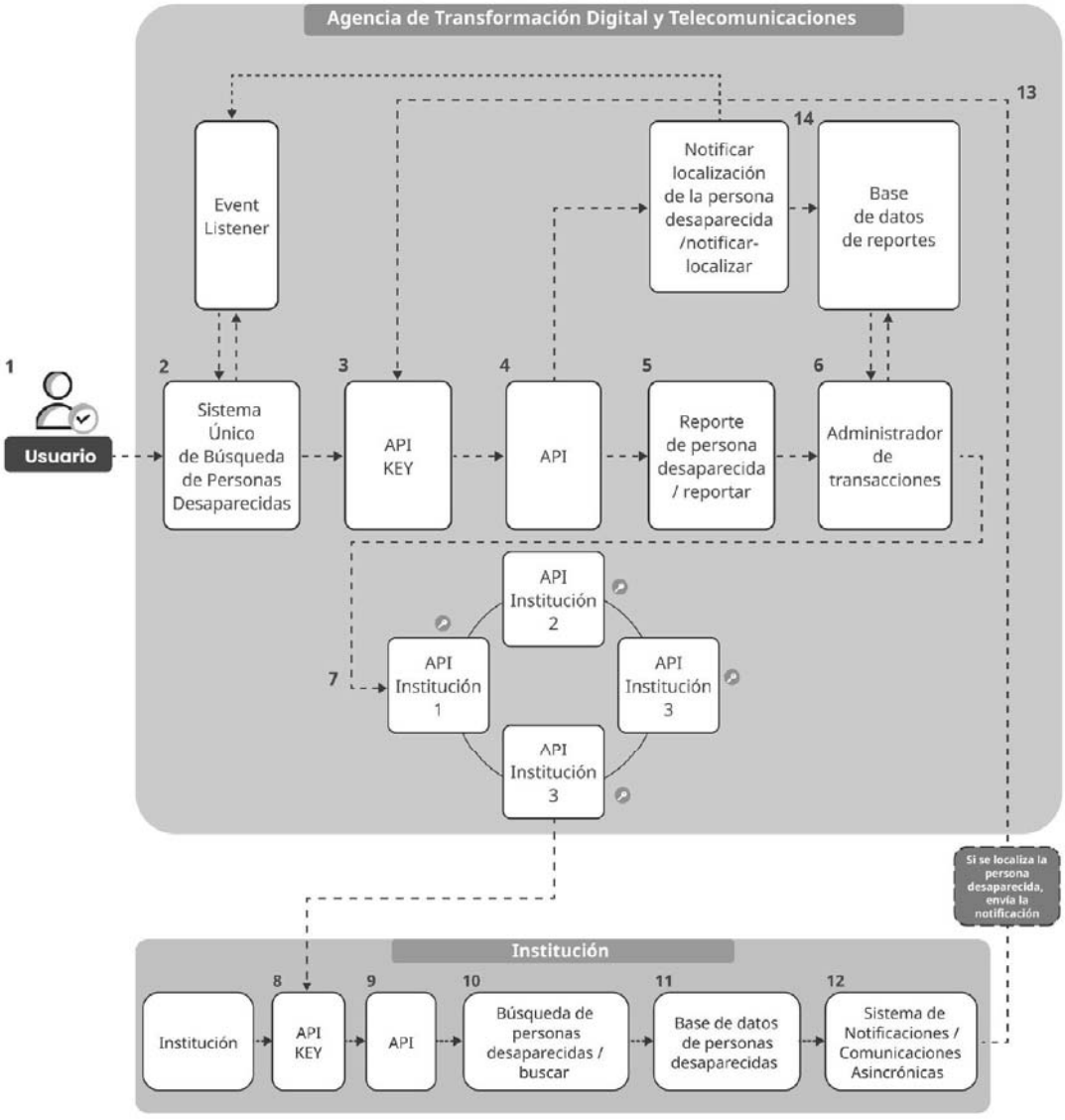
6.2. Se notifica a todas las instituciones diversas a través de su API para que también lo den de baja por medio del *endpoint* ***/desactivar-reporte***.

Requisitos del API institucional

Cada institución diversa, puede utilizar las tecnologías y la metodología que mejor se adapte a sus necesidades y sistemas existentes, con el fin de poder exponer un *web service* que se adecue a las siguientes consideraciones básicas:

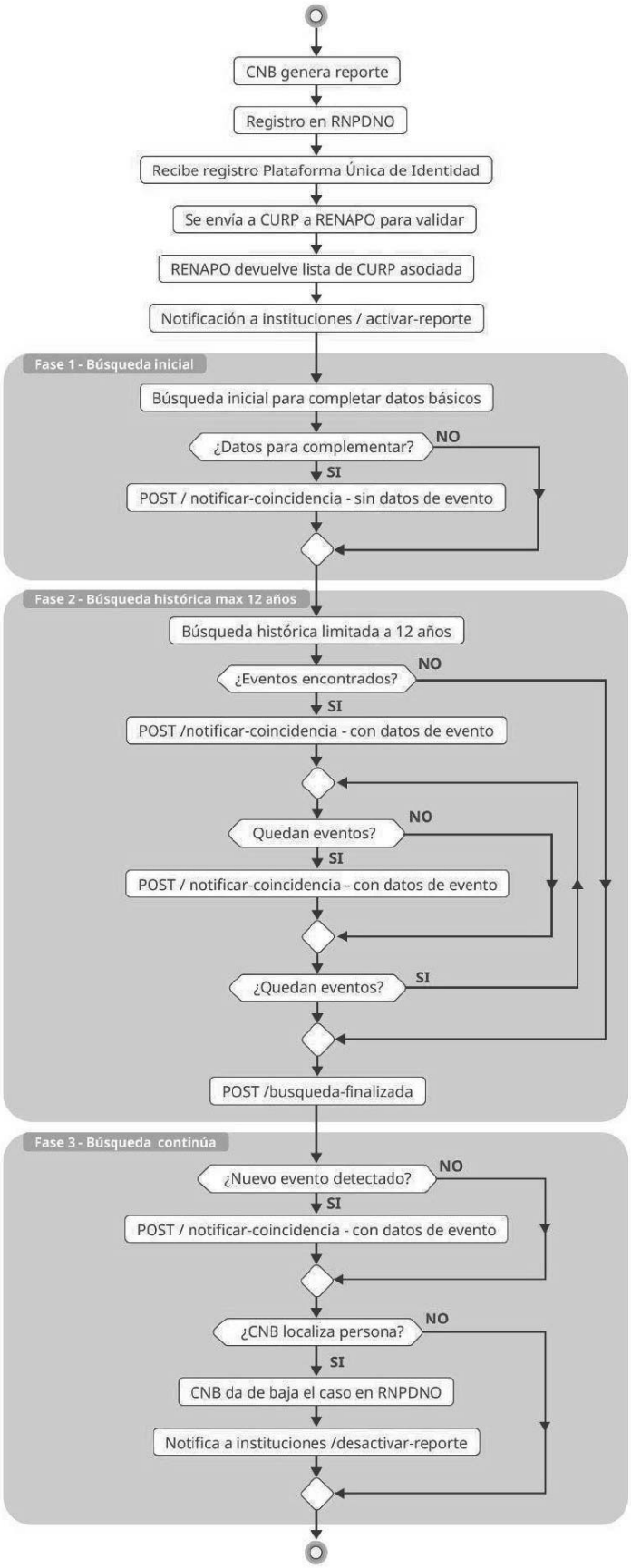
Autenticación mediante Bearer token y firmado/validado de la información en el JSON de respuesta.[2]
Mecanismo de notificación activa (POST) para respuestas de coincidencia.
Persistencia de las búsquedas y coincidencias en bases de datos locales.
Un sistema de monitoreo para la búsqueda continua.
Mecanismo de resincronización para solventar posibles tiempos de inactividad de los sistemas.

Diagrama del Sistema



[2] **Nota:** Tanto en la fase de pruebas como para el entorno de producción, se implementará un esquema de autenticación basado en *Bearer token* y firmado/validado de la información en el JSON de respuesta, con el objetivo de garantizar la integridad y confidencialidad de las comunicaciones, así como la verificación de identidad de las partes involucradas.

Flujo del reporte



7. Endpoints expuestos por la Plataforma Única de Identidad

Los siguientes endpoints son expuestos por la PUI y deberán ser consumidos por la Institución diversa para efectos de autenticación, consulta de catálogos y obtención de información relacionada con los reportes activos.

7.1. Acceso

La Institución diversa deberá enviar una petición con sus credenciales para obtener un JWT.

https://pui.example.mx/login

El contenido de la consulta deberá ser de tipo raw-JSON (application/json) con las siguientes propiedades:

Solicitud

Propiedad	Tipo	Longitud	Descripción	Obligatorio
institucion_id	String	**Min: 4** **Max: 13**	Identificador de institución, en el caso de instituciones diversas el valor será el RFC de la institución con homoclave.	Sí
clave	String	**Min: 1** **Max: 50**	Clave proporcionada por el área técnica.	Sí

Respuesta

Propiedad	Tipo	Descripción
token	String	JWT generado.

Vigencia del token

La vigencia del token es de una hora. Se recomienda que las instituciones diversas lo renueven antes de alcanzar el 80 % de su tiempo de expiración, a fin de reducir riesgos de uso indebido, mejorar la trazabilidad y mantener el control ante posibles compromisos de credenciales. En caso de que el token expire, será necesario generar uno nuevo enviando nuevamente la solicitud de autenticación con las credenciales correspondientes.

Códigos de error HTTP

Para detectar si las peticiones u operaciones que se han realizado a la API han finalizado de manera correcta o se ha producido algún tipo de error, el protocolo HTTP retorna los siguientes códigos de error:

Código	Valor	Descripción
200	JWT	JWT generado.
403	Error	Credenciales inválidas.
500	Error procesando petición	Petición recibida pero el servidor provocó un error interno no controlado.

Ejemplo de invocación

A continuación, se muestra un ejemplo del método login mediante el uso de cURL.

```
cURL -X POST https://pui.example.mx/login \
-H "Content-Type: application/json" \
-d '{ "institucion_id": "0000", "clave": "xx8NLiiFWov8KZQ"}'
```

Respuesta


```
{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpbnN0aXR1Y2lvbl9pZCI6IjAwMD
AiLCJwZXJtaXNvcyI6WyJub3RpZmljYXIiLCJjb25jbHVpciJdLCJpYXQiOjE3NDk4NDI3NTgsImV
4cCI6MTc0OTg0NjM1OH0.SjjczNrHMuJXQuUiv33lEaYbxjnx_zeexpwqmaRjCmE"}
```

Error de credenciales (403)

Ejemplo de invocación

A continuación, se muestra un ejemplo del método login mediante el uso de cURL.

```
 cURL -X POST https://pui.example.mx/login \
-H "Content-Type: application/json" \
-d '{ "institucion_id": "0000", "clave": "xx8NLiiFWovxQx"}'
```

Respuesta

```
{"error":"Credenciales inválidas"}
```

7.2. Notificar coincidencia

Se deberá acceder a la siguiente URL, el método de envío será tipo **POST**.

https://pui.example.mx/notificar-coincidencia

El contenido de la consulta deberá ser de tipo raw-JSON (application/json) y codificado en UTF-8 con las siguientes propiedades:

Solicitud

Propiedad	Tipo	Longitud	Descripción	Obligatorio
curp	String	**Min: 18** **Max: 18**	CURP de la persona desaparecida o no localizada. Sólo se aceptan letras mayúsculas y números. Expresión regular: ^[A-Z0-9]{18}$	Sí
nombre_completo	Object	**N/A**	Nombre completo de la persona, formado por los campos *nombre*, *primer_apellido* y *segundo_apellido*.	No
nombre	String	**Min: 1** **Max: 50**	Nombre de persona desaparecida o no localizada. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ '-]{1,50}$	No
primer_apellido	String	**Min: 1** **Max: 50**	Primer apellido de persona desaparecida o no localizada. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ '-]{1,50}$	No
segundo_apellido	String	**Min: 1** **Max: 50**	Segundo apellido de persona desaparecida o no localizada. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ '-]{1,50}$	No
fecha_nacimiento	String	**Min: 10** **Max: 10**	Fecha de nacimiento de la persona desaparecida o no localizada en formato ISO 8601 YYYY-MM-DD	No
lugar_nacimiento	String ((enum)	**Min: 0** **Max: 20**	Si la CURP es inválida o el código no corresponde a un estado reconocido, se debe enviar el valor DESCONOCIDO. En cualquier otro caso, el código debe mapearse al estado correspondiente siguiendo la tabla de referencia (ver Anexo 5). Si el código obtenido es "NE", se debe enviar el valor FORANEO.	Sí

Propiedad	Tipo	Longitud	Descripción	Obligatorio
sexo_asignado	String	**Min: 1** **Max: 1**	Sexo asignado de la persona desaparecida o no localizada, “H" para hombres, “M" para mujeres y “X" para el resto de los casos. Expresión regular: ^[MHX]{1}$	No
telefono	String	**Min: 0** **Max: 15**	Teléfono de la persona desaparecida o no localizada. Expresión regular: ^\+?\d{0,15}$	No
correo	String	**Min: 0** **Max: 50**	Correo electrónico de la persona desaparecida o no localizada. Expresión regular: ^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,50}$	No
domicilio	Object	**N/A**	Dirección de la persona desaparecida o no localizada, formada por los campos *direccion* (dirección completa con mayor detalle posible), *calle*, *numero*, *colonia*, *codigo_postal*, *municipio_o_alcaldia* y *entidad_federativa*.	No
direccion	String	**Min: 0** **Max: 500**	Dirección completa de la persona desaparecida o no localizada con mayor detalle posible. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,500}$	No
calle	String	**Min: 0** **Max: 50**	Calle o avenida de persona desaparecida o no localizada. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,50}$	No
numero	String	**Min: 0** **Max: 20**	Número de domicilio de la persona desaparecida o no localizada con el mayor detalle posible (exterior e interior si existe). Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,20}$	No
colonia	String	**Min: 0** **Max: 50**	Colonia de la persona desaparecida o no localizada. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,50}$	No
codigo_postal	String	**Min: 0** **Max: 5**	Código postal de persona desaparecida o no localizada. Expresión regular: ^\d{0,5}$	No
municipio_o_alcaldia	String	**Min: 0** **Max: 100**	Municipio o Alcaldía de persona desaparecida o no localizada. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,100}$	No
entidad_federativa	String	**Min: 0** **Max: 40**	Entidad Federativa de persona desaparecida o no localizada. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,40}$	No

Propiedad	Tipo	Longitud	Descripción	Obligatorio
fotos	Object	**N/A**	Arreglo de Strings de fotos de la persona desaparecida o no localizada. Cada foto de la que se disponga debe tener una resolución mínima de 300 ppi y un peso máximo de 240KB. Posteriormente deben pasarse a base64 y cifrarse usando AES-256-GCM con la contraseña para biométricos proporcionada a la institución. Si no se cuenta con fotos debe omitirse el arreglo.[3]	No
formato_fotos	String	**Min: 0** **Max: 20**	Formato del archivo de la foto, por ejemplo “png", “jpg", “bmp", etc.	No
huellas	Object	**N/A**	Las huellas deben incluirse en un objeto formado con los campos correspondientes de la siguiente tabla de referencia (ver Anexo 4). Cada huella de la que se disponga debe tener una resolución mínima de 500 ppi y en escala de grises de 8 bits. Posteriormente, debe pasarse a base64 y cifrarse usando AES-256-GCM con la contraseña para biométricos proporcionada a la institución, y debe colocarse en su etiqueta correspondiente. Las huellas con las que no se cuente pueden omitirse (en caso de no contar con ninguna se omite el objeto completo). Formato de ejemplo huellas:{"rone":"...", "rtwo":"...", ..., "lpalm":"..."}[4]	No
formato_huellas	String	**Min: 0** **Max: 50**	Formato del archivo de la huella, por ejemplo “wsq".	No
id	String	**Min: 36** **Max: 75**	El identificador único se generará automáticamente para cada solicitud. Se construye concatenando el FUB con un UUID versión 4, separados por un guión. Formato: <FUB>-<UUID4> Ejemplo: e7b5a4c2-9f4e-4a99-91a2-6d4a8a1eaf3d-550e8400-e29b-41d4-a716-446655440000	Sí
institucion_id	String	**Min: 4** **Max: 13**	Identificador de institución, en el caso de instituciones diversas el valor será el RFC de la institución con homoclave. Expresión regular: ^[A-Z0-9]{4,13}$	Sí
tipo_evento	String	**Min: 0** **Max: 500**	Tipo de operación administrativa en que se encontró la coincidencia. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,500}$	No

[3] La Plataforma Única de Identidad (PUI) constituye un mecanismo de interoperabilidad tecnológica y consulta controlada, y no un repositorio biométrico. En este sentido, la PUI y el Registro Nacional de Población (RENAPO) no captan ni almacenan de manera permanente huellas dactilares ni imágenes faciales como bases de datos propias.
Los datos biométricos permanecen bajo la custodia y responsabilidad de las instituciones diversas legalmente facultadas para su tratamiento, conforme a sus atribuciones y a la normativa aplicable. La participación de la PUI se limita a facilitar procesos de interconexión, verificación y notificación de coincidencias, sin concentración, reutilización ni conservación autónoma de información biométrica.

[4] La Plataforma Única de Identidad (PUI) constituye un mecanismo de interoperabilidad tecnológica y consulta controlada, y no un repositorio biométrico. En este sentido, la PUI y el Registro Nacional de Población (RENAPO) no captan ni almacenan de manera permanente huellas dactilares ni imágenes faciales como bases de datos propias.
Los datos biométricos permanecen bajo la custodia y responsabilidad de las instituciones diversas legalmente facultadas para su tratamiento, conforme a sus atribuciones y a la normativa aplicable. La participación de la PUI se limita a facilitar procesos de interconexión, verificación y notificación de coincidencias, sin concentración, reutilización ni conservación autónoma de información biométrica.

Propiedad	Tipo	Longitud	Descripción	Obligatorio
fecha_evento	String	**Min: 10** **Max: 10**	Fecha en que se dio la operación administrativa en que se encontró la coincidencia en formato ISO 8601 (por ejemplo, si el hallazgo fue de una unión civil, sería la fecha en que se dió la unión) YYYY-MM-DD	No
descripcion_lugar_evento	String	**Min: 0** **Max: 500**	Texto libre que describe el sitio donde ocurrió el evento (por ejemplo, “Escuela Secundaria Tecnica No. 22", “Sucursal Lomas Estrella", etc.). Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,500}$	No
direccion_evento	Object	**N/A**	Dirección del evento reportado, formada por los campos *direccion* (dirección completa con mayor detalle posible), *calle*, *numero*, *colonia*, *codigo_postal,* *municipio_o_alcaldia* y *entidad_federativa*.	No
direccion	String	**Min: 0** **Max: 500**	Dirección completa del evento reportado con mayor detalle posible. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,500}$	No
calle	String	**Min: 0** **Max: 50**	Calle o avenida del evento reportado. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,50}$	No
numero	String	**Min: 0** **Max: 20**	Número de domicilio del evento reportado con el mayor detalle posible (exterior e interior si existe). Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,20}$	No
colonia	String	**Min: 0** **Max: 50**	Colonia del evento reportado. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,50}$	No
codigo_postal	String	**Min: 0** **Max: 5**	Código postal del evento reportado. Expresión regular: ^\d{0,5}$	No
municipio_o_alcaldia	String	**Min: 0** **Max: 100**	Municipio o Alcaldía del evento reportado. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,100}$	No
entidad_federativa	String	**Min: 0** **Max: 40**	Entidad federativa del evento reportado. Expresión regular: ^[A-Za-zÁÉÍÓÚÜÑáéíóúüñ0-9 .,#'/:()\-]{0,40}$	No
fase_busqueda	String	**Min: 1** **Max: 1**	Fase de la búsqueda: “1" para la fase 1 (búsqueda para completar datos básicos), “2" para la fase 2 (búsqueda histórica), y “3" para la fase 3 (búsqueda continua). Expresión regular: ^[1-3]$	Sí

Respuesta

Propiedad	Tipo	Descripción
message	String	Coincidencia recibida correctamente

Códigos de error HTTP

Para detectar si las peticiones u operaciones que se han realizado a la API han finalizado de manera correcta o se ha producido algún tipo de error, el protocolo HTTP retorna los siguientes códigos de error:

Código	Valor	Descripción
200	Ok	Coincidencia recibida correctamente
300	Coincidencias múltiples	Se identifica a más de una persona distinta a partir de los elementos utilizados para la búsqueda
400	Solicitud Incorrecta	Error en los siguientes campos
500	Error procesando coincidencia	Petición recibida pero el servidor provocó un error interno no controlado.
401	Token inválido o expirado	Antes de que se procesen los datos de la solicitud si hay un problema con tu autenticación. Falta de autenticación o Token expirado.

Ejemplo de invocación

A continuación, se muestra un ejemplo del método notificar-coincidencia mediante el uso de cURL.

```
 cURL -X POST https://pui.example.mx/notificar-coincidencia \
-H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpbnN0aXR1Y2lvbl9pZCI6IjAwMDAiLCJwZXJt
aXNvcyI6WyJub3RpZmljYXIiLCJjb25jbHVpciJdLCJpYXQiOjE3NDk4NTM3MTgsImV4cCI6MTc0O
Tg1NzMxOH0.E0VNedmQALILhbVqyezFwDhI3Il_6fCQ-gqBFnWHnYA" \
-H "Content-Type: application/json" \
-
d'{"curp":"XEXX010101HNEXXXA0","nombre_completo":{"nombre":"Juan","primer_ape
llido":"Pérez","segundo_apellido":"López"},"fecha_nacimiento":"1990-05-
15","lugar_nacimiento":"CDMX","sexo_asignado":"H","telefono":"5512345678","co
rreo":"juan.perez@example.com","domicilio":{"direccion":"Calle Reforma
123,Centro","calle":"Reforma","numero":"123","colonia":"Centro","codigo_posta
l":"06000","municipio_o_alcaldia":"Cuauhtémoc","entidad_federativa":"CDMX"},"
fotos":["aGVsbG8gd29ybGQ=","aW1hZ2VuMiBiYXNlNjQ="],"formato_fotos":"jpg","hue
llas":{"rtwo":"ZHVtbXlmaW5nZXIx","ltwo":"ZHVtbXlmaW5nZXIy"},"formato_huellas"
:"wsq","id":"e7b5a4c2-9f4e-4a99-91a2-6d4a8a1eaf3d-550e8400-e29b-41d4-a716-
446655440000","institucion_id":"0000","tipo_evento":"Apertura de cuenta
bancaria","fecha_evento":"2025-05-21","descripcion_lugar_evento":"Sucursal 22
Lomas Estrella","direccion_evento":{"direccion":"Cerrada Zacarías Topete 1562
Int. B, De los Ángeles, San Luis Potosí","calle":"Cerrada Zacarías
Topete","numero":"1562 Int. B","colonia":"De los
Ángeles","codigo_postal":"01245","municipio_o_alcaldia":"San Luis
Potosí","entidad_federativa":"SAN LUIS POTOSÍ"},"fase_busqueda":"1"}'
```

Respuesta

```
{"message":"Coincidencia recibida correctamente"}
```

Ejemplo de invocación

A continuación, se muestra un ejemplo del error de petición inválida por longitud de campos mediante el uso de cURL.

```
cURL -X POST https://pui.example.mx/notificar-coincidencia \

-H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpbnN0aXR1Y2lvbl9pZCI6IjAwMDEiLCJwZXJt
aXNvcyI6WyJub3RpZmljYXIiLCJjb25jbHVpciJdLCJpYXQiOjE3NTM3MjE3NDIsImV4cCI6MTc1M
zcyNTM0Mn0.kvP5YyizhxfwHpgVJxFL0FJlmCae-IDl6nwUmNvORTg" \

-H "Content-Type: application/json" \

-
d'{"curp":"CURP_INVALIDA_DEMASIADO_LARGA_XEXX010101HNEXXXA0XYZ","nombre_compl
eto":{"nombre":"NombreDemasiadoLargoParaPruebaDeErrorDeValidacionDeLongitudMa
ximalDelCampoNombreEnLaAPI","primer_apellido":"Pérez","segundo_apellido":"Lóp
ez"},"fecha_nacimiento":"15-05-
1990","id":"ID_CORTO","lugar_nacimiento":"CDMX","fase_busqueda":"1"}'
```

Respuesta

```
{"errores":["'curp' debe tener entre 0 y 18 caracteres","'nombre' debe tener
entre 0 y 50 caracteres","'id' debe tener entre 36 y 75
caracteres","'institucion_id' es obligatorio","'fecha_nacimiento' debe estar
en formato YYYY-MM-DD"]}
```

Ejemplo de invocación

A continuación, se muestra un ejemplo del error por campos obligatorios faltantes mediante el uso de cURL.

```
cURL -X POST https://pui.example.mx/notificar-coincidencia \

-H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpbnN0aXR1Y2lvbl9pZCI6IjAwMDEiLCJwZXJt
aXNvcyI6WyJub3RpZmljYXIiLCJjb25jbHVpciJdLCJpYXQiOjE3NTM3MjE3NDIsImV4cCI6MTc1M
zcyNTM0Mn0.kvP5YyizhxfwHpgVJxFL0FJlmCae-IDl6nwUmNvORTg" \

-H "Content-Type: application/json" \
 -d'{"id":"e7b5a4c2-9f4e-4a99-91a2-6d4a8a1eaf3d-550e8400-e29b-41d4-a716-
446655440000","institucion_id":"0001","lugar_nacimiento":"CDMX","fase_busqued
a":"1"}'
```

Respuesta

```
{"errores":["'curp' es obligatorio"]}
```

7.3. Búsqueda finalizada

Se deberá acceder a la siguiente URL, el método de envío será tipo **POST**.

https://pui.example.mx/busqueda-finalizada

El contenido de la consulta deberá ser de tipo raw-JSON (application/json) y codificado en UTF-8 con las siguientes propiedades:

Solicitud

Propiedad	Tipo	Longitud	Descripción	Obligatorio
id	String	**Min: 36** **Max: 75**	El identificador único se generará automáticamente para cada solicitud. Se construye concatenando el FUB con un UUID versión 4, separados por un guión. Formato: <FUB>-<UUID4> Ejemplo: e7b5a4c2-9f4e-4a99-91a2-6d4a8a1eaf3d-550e8400-e29b-41d4-a716-446655440000	Sí
institucion_id	String	**Min: 4** **Max: 13**	Identificador de institución, en el caso de instituciones diversas el valor será el RFC de la institución con homoclave.	Sí

Respuesta

Propiedad	Tipo	Descripción
message	String	Registro de finalización de búsqueda histórica guardado correctamente.

Códigos de error HTTP

Para detectar si las peticiones u operaciones que se han realizado a la API han finalizado de manera correcta o se ha producido algún tipo de error, el protocolo HTTP retorna los siguientes códigos de error:

Código	Valor	Descripción
200	Ok	Registro de conclusión guardado correctamente
500	Error procesando coincidencia	Petición recibida pero el servidor provocó un error interno no controlado.
401	Token inválido o expirado	Antes de que se procesen los datos de la solicitud, si hay un problema con tu autenticación. Falta de autenticación o Token expirado.

Ejemplo de invocación

A continuación, se muestra un ejemplo del método /*busqueda-finalizada* mediante el uso de cURL.

```
cURL -X POST https://pui.example.mx/busqueda-finalizada \
-H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpbnN0aXR1Y2lvbl9pZCI6IjAwMDAiLCJwZXJt
aXNvcyI6WyJub3RpZmljYXIiLCJjb25jbHVpciJdLCJpYXQiOjE3NDk4NTM3MTgsImV4cCI6MTc0O
Tg1NzMxOH0.E0VNedmQALILhbVqyezFwDhI3Il_6fCQ-gqBFnWHnYA" \
-H "Content-Type: application/json"
-d '{"id":"string","institucion_id":"string"}'
```

Respuesta

```
{"message": "Registro de finalización de búsqueda histórica guardado
correctamente."}
```

Ejemplo de invocación

A continuación, se muestra un ejemplo de petición inválida por campos faltantes o inválidos mediante el uso de cURL.

```
cURL -X POST https://pui.example.mx/busqueda-finalizada \
-H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpbnN0aXR1Y2lvbl9pZCI6IjAwMDEiLCJwZXJt
aXNvcyI6WyJub3RpZmljYXIiLCJjb25jbHVpciJdLCJpYXQiOjE3NTM3MjE3NDIsImV4cCI6MTc1M
zcyNTM0Mn0.kvP5YyizhxfwHpgVJxFL0FJlmCae-IDl6nwUmNvORTg" \
-H "Content-Type: application/json" \
-d'{"institucion_id":"0001"}'
```

Respuesta

```
{"error":"Error al guardar el registro."}
```

Ejemplo de invocación

A continuación, se muestra un ejemplo de campos vacíos mediante el uso de cURL.

```
cURL -X POST https://pui.example.mx/busqueda-finalizada \
-H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpbnN0aXR1Y2lvbl9pZCI6IjAwMDEiLCJwZXJt
aXNvcyI6WyJub3RpZmljYXIiLCJjb25jbHVpciJdLCJpYXQiOjE3NTM3MjU3MzgsImV4cCI6MTc1M
zcyOTMzOH0.IgcklYNuwxJFv3u0vDPYiL6rf6dRCEAsAX2aduoJ91Q" \
-H "Content-Type: application/json" \
-d'{}'
```

Respuesta

```
{"error":"Error al guardar el registro."}
```

7.4. Listar los reportes enviados a instituciones

Se deberá acceder a la siguiente URL, el método de envío será de tipo **GET**:

https://pui.example.mx/reportes

El contenido de la consulta deberá ser de tipo raw-JSON (application/json) y codificado en UTF-8 con las siguientes propiedades:

Respuesta

Propiedad	Tipo	Descripción
List	JSON	Reportes

Códigos de error HTTP

Para detectar si las peticiones u operaciones que se han realizado a la API han finalizado de manera correcta o se ha producido algún tipo de error, el protocolo HTTP retorna los siguientes códigos de error:

Código	Valor	Descripción
200	Lista de reportes con sus estados	Petición recibida y procesada de manera correcta.
500	Error al obtener los reportes	Petición recibida pero el servidor provocó un error interno no controlado.
401	Token inválido o expirado	Antes de que se procesen los datos de la solicitud, si hay un problema con tu autenticación. Falta de autenticación o Token expirado.

Ejemplo de invocación

A continuación, se muestra un ejemplo del método reportes mediante el uso de cURL.

```
cURL -X GET https://pui.example.mx/reportes \
 -H "Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpbnN0aXR1Y2lvbl9pZCI6IjAwMDAiLCJwZXJtaXNvcyI6WyJub3RpZmljYXIiLCJjb25jbHVpciJdLCJpYXQiOjE3NDk4NTM3MTgsImV4cCI6MTc0OTg1NzMxOH0.E0VNedmQALILhbVqyezFwDhI3Il_6fCQ-gqBFnWHnYA"
```

Respuesta

```
[{"id":"e7b5a4c2-9f4e-4a99-91a2-6d4a8a1eaf3d-550e8400-e29b-41d4-a716-
446655440000","curp":"SA06EIMBDR5OVM72NY","nombre":"Dayana","primer_apellido"
:"Franecki","segundo_apellido":"Wolf","fecha_nacimiento":"1970-08-
29","fecha_desaparicion":"1995-11-22","fecha_registro":"2003-04-
20","lugar_nacimiento":"COLIMA","sexo_asignado":"M"},{"id":"g7b5a4c2-9f4e-
4a99-91a2-6d4a8a1eaf3d-550e8400-e29b-41d4-a716-
446655440011","curp":"B6PQYBJHZS91YIPXPI","nombre":"Julian","primer_apellido"
:"Neri","segundo_apellido":"Baños","fecha_nacimiento":"1995-03-
12","fecha_desaparicion":"2010-05-13","fecha_registro":"2015-01-
27","lugar_nacimiento":"CDMX","sexo_asignado":"H"},{"id":"a3b2a4c2-9f4e-4a99-
91a2-6d4a8a1eaf3d-550e8400-e29b-41d4-a716-
446655440003","curp":"AEN0ZEUQUDPMXUHVMP","nombre":"Socorro","primer_apellido
":"Cortazar","segundo_apellido":"Borges","fecha_nacimiento":"2002-08-
01","fecha_desaparicion":"2022-12-10","fecha_registro":"2023-11-
15","lugar_nacimiento":"CAMPECHE","sexo_asignado":"X"}]
```

Ejemplo de invocación:

A continuación se muestra un ejemplo de una solicitud realizada sin proporcionar el token de autenticación, utilizando cURL:

```
 cURL -X GET https://pui.example.mx/api/v2_3_0/reportes
```

Respuesta:

```
{"error":"Token no proporcionado"}
```

8. Endpoints que debe implementar la Institución diversa

Los endpoints que se especifican en esta sección, deben ser desarrollados, mantenidos y asegurados por cada Institución diversa. La PUI realizará solicitudes hacia ellos, como parte de los flujos de activación de reportes, búsqueda continua, notificación de coincidencias y finalización de casos.

Con el fin de estandarizar la invocación, facilitar la configuración y permitir que la Plataforma Única de Identidad consuma correctamente los servicios expuestos por cada institución, **todas las instituciones diversas deberán definir y mantener una URL base única** a partir de la cual se construirán los endpoints requeridos. La estructura final de los servicios quedará de la siguiente manera:

```
<URL_BASE>/<endpoint>
```

Donde:

- **<URL_BASE>** es la ruta definida por la institución (por ejemplo: https://api.institucion.gob.mx/pui, https://institucion.dominio.mx/api/v1, https://<webhook>).

5. Los endpoints se concatenan directamente sin modificar su nombre estándar.

```
Autenticación:
<URL_BASE>/login
Activación de reporte:
<URL_BASE>/activar-reporte

Activación de reporte de prueba:
<URL_BASE>/activar-reporte-prueba

Desactivación de reporte:
<URL_BASE>/desactivar-reporte
```

8.1. Autenticación de Endpoints mediante JWT

Cada institución deberá proteger sus endpoints mediante autenticación basada en JSON Web Tokens (JWT). El flujo de autenticación será el siguiente:

1. **Obtención de Token:**

   El usuario solicitará un token JWT enviando sus credenciales (usuario y contraseña) al *endpoint* ***/login***.

2. **Recepción del Token:**

   Si las credenciales son válidas, el sistema devolverá un JWT firmado, que el usuario deberá utilizar en sus siguientes solicitudes.

3. **Uso del Token:**

   Para acceder a los *endpoints* protegidos, el usuario deberá incluir el token en el encabezado HTTPS Authorization usando el esquema Bearer:

   Authorization: Bearer <token>

4. **Validación:**

   El sistema receptor validará la firma y vigencia del JWT en cada solicitud. Sólo se permitirá el acceso si el token es válido y no ha expirado.

Solicitud

El contenido de la petición es de tipo raw-JSON (application/json) con las siguientes propiedades:

Propiedad	Tipo	Longitud	Descripción	Obligatorio
usuario	String	**Min: 3** **Max: 3**	El valor de *usuario* es “PUI", es fijo, sin variaciones y se utiliza de manera constante para la autenticación de la PUI ante las instituciones diversas.	Sí
clave	String	**Min: 16** **Max: 20**	El campo *clave* corresponde a la contraseña y deberá tener entre 16 y 20 caracteres, incluir al menos una letra mayúscula, un número (0–9) y al menos uno de los caracteres especiales permitidos: ! @ # $ % ^ & * ( ) - _ . +.	Sí

8.2. Activar reporte de búsqueda

Cada una de las instituciones diversas implementarán un endpoint de tipo POST para recibir en el contenido de la petición de tipo raw-JSON (application/json) con las siguientes propiedades:[5]

Solicitud

Propiedad	Tipo	Longitud	Descripción	Obligatorio
id	String	**Min: 36** **Max: 75**	El identificador único se generará automáticamente para cada solicitud. Se construye concatenando el FUB con un UUID versión 4, separados por un guión. Formato: <FUB>-<UUID4> Ejemplo: e7b5a4c2-9f4e-4a99-91a2-6d4a8a1eaf3d-550e8400-e29b-41d4-a716-446655440000	Sí
curp	String	**Min: 18** **Max: 18**	CURP de persona desaparecida.	Sí
nombre	String	**Min: 0** **Max: 50**	Nombre de persona desaparecida.	No
primer_apellido	String	**Min: 0** **Max: 50**	Primer apellido de persona desaparecida o no localizada.	No
segundo_apellido	String	**Min: 0** **Max: 50**	Segundo apellido de persona desaparecida o no localizada.	No
fecha_nacimiento	String	**Min: 10** **Max: 10**	Fecha de nacimiento de persona desaparecida o no localizada en formato ISO 8601 YYYY-MM-DD	No
fecha_desaparicion	String	**Min: 10** **Max: 10**	Fecha en que ocurrió la desaparición de la persona, en formato ISO 8601 YYYY-MM-DD	No
lugar_nacimiento	String (enum)	**Min: 0** **Max: 20**	Si la CURP es inválida o el código no corresponde a un estado reconocido, se enviará el valor DESCONOCIDO. En cualquier otro caso, el código se mapeará al estado correspondiente siguiendo la tabla de referencia (ver Anexo 5). Si el código obtenido es "NE", se enviará el valor FORÁNEO.	Sí

[5] **Nota:** La inclusión de campos en la solicitud POST dependerá de la información disponible en el padrón. En caso de que algún dato no esté registrado, el campo correspondiente podrá omitirse o enviarse con un valor nulo. Por lo tanto, no se garantiza que todos los campos estén presentes en cada solicitud.

Propiedad	Tipo	Longitud	Descripción	Obligatorio
sexo_asignado	String	**Min: 1** **Max: 1**	Sexo asignado de persona desaparecida o no localizada, “H" para hombres, “M" para mujeres y “X" para el resto de los casos.	No
telefono	String	**Min: 0** **Max: 15**	Teléfono de persona desaparecida o no localizada.	No
correo	String	**Min: 0** **Max: 50**	Correo electrónico de persona desaparecida o no localizada.	No
direccion	String	**Min: 0** **Max: 500**	Dirección donde residía la persona, con el mayor detalle posible.	No
calle	String	**Min: 0** **Max: 50**	Calle o avenida de persona desaparecida o no localizada.	No
numero	String	**Min: 0** **Max: 20**	Número de domicilio de la persona desaparecida o no localizada con el mayor detalle posible (exterior e interior si existe).	No
colonia	String	**Min: 0** **Max: 50**	Colonia de la persona desaparecida o no localizada.	No
codigo_postal	String	**Min: 0** **Max: 5**	Código postal de persona desaparecida o no localizada.	No
municipio_o_alcaldia	String	**Min: 0** **Max: 100**	Municipio o Alcaldía de persona desaparecida o no localizada.	No
entidad_federativa	String	**Min: 0** **Max: 40**	Entidad federativa de persona desaparecida o no localizada.	No

Códigos de respuesta HTTP

Para identificar si la activación del reporte de búsqueda se procesó correctamente o si ocurrió algún error, el servicio deberá devolver los siguientes códigos de respuesta del protocolo HTTP, según corresponda:

Código	Valor	Descripción
200	Éxito	La solicitud fue recibida de manera correcta.
400	Error en la solicitud	La solicitud contiene datos inválidos o con formato incorrecto
401	Falta o falla de autenticación	Credenciales no válidas, falta de autenticación o token expirado.
403	Sin permisos	Acceso no autorizado; verifica que el usuario PUI tenga permisos.
500	Error interno del servidor	Ocurrió un error interno al procesar la solicitud.
504	El servidor tardó demasiado en responder	No fue posible completar la conexión.

Respuesta

En caso de que la solicitud de activación del reporte de búsqueda sea recibida y procesada de manera correcta por la Institución diversa, ésta deberá devolver el código **200** junto con el siguiente mensaje:

Propiedad	Tipo	Descripción
message	String	La solicitud de activación del reporte de búsqueda se recibió correctamente.

8.3. Activar reporte de prueba

Con el propósito de validar la correcta integración técnica antes de procesar reportes reales, cada Institución diversa deberá implementar el endpoint /activar-reporte-prueba, el cual permitirá confirmar:

1. La conectividad con el Webhook registrado.
2. La estructura del payload enviado por la Plataforma Única de Identidad.
3. El manejo adecuado del esquema de autenticación mediante Bearer Token.
4. La recepción y validación de los campos obligatorios.

Códigos de respuesta HTTP

Para detectar si las peticiones u operaciones que se han realizado a la API han finalizado de manera correcta o se ha producido algún tipo de error, el protocolo HTTP retorna los siguientes códigos de error:

Código	Valor	Descripción
200	Éxito	Petición recibida y procesada de manera correcta.
400	Error en la solicitud	La solicitud contiene datos inválidos o con formato incorrecto
401	Falta o falla de autenticación	Credenciales no válidas, verifica la contraseña registrada, falta de autenticación o Token expirado.
403	Sin permisos	Acceso no autorizado, verifica que el usuario PUI tenga acceso al Webhook.
500	Error interno del servidor	Ocurrió un error interno al procesar la prueba del Webhook
504	El servidor tardó demasiado en responder	No fue posible completar la conexión.

Ejemplo de invocación

Una vez obtenido el token mediante el endpoint /login, se enviará la petición de activación del reporte de prueba que a continuación, se muestra un ejemplo de la invocación mediante el uso de cURL.

```
curl -X POST '{webhook}/activar-reporte-prueba' \
--header 'accept: application/json' \
--header 'Authorization: Bearer <TOKEN_OBTENIDO_DEL_LOGIN>' \
--data '{
  "id": "A1B2C3D4E5F6-550e8400-e29b-41d4-a716-446655440000",
  "curp": "TEST010101HDFABC01",
  "nombre": "JUAN",
  "primer_apellido": "PEREZ",
  "segundo_apellido": "LOPEZ",
  "fecha_nacimiento": "1990-01-01",
  "fecha_desaparicion": "2024-12-15",
  "lugar_nacimiento": "CDMX",
  "sexo_asignado": "H",
  "telefono": "5512345678",
  "correo": "juan.perez@example.com",
  "direccion": "CALLE FICTICIA 123, CENTRO",
  "calle": "CALLE FICTICIA",
  "numero": "123",
  "colonia": "CENTRO",
  "codigo_postal": "06000",
  "municipio_o_alcaldia": "CUAUHTÉMOC",
  "entidad_federativa": "CDMX"
}'
```

Nota: El `<TOKEN_OBTENIDO_DEL_LOGIN>` es el valor exacto generado en el paso previo.

Este proceso permite corroborar que la infraestructura de la Institución cumple con los lineamientos técnicos establecidos para la recepción de reportes y garantiza que el funcionamiento del Webhook es adecuado antes de iniciar las operaciones formales.

8.4. Desactivar reporte

Se usará un *endpoint /desactivar-reporte* implementado por cada institución, de tipo POST, que desactiva la búsqueda de una persona previamente reportada, utilizando únicamente su identificador único (*id*).

Solicitud

Propiedad	Tipo	Longitud	Descripción	Obligatorio
id	String	**Min: 36** **Max: 75**	El identificador único se generó automáticamente. Se construye concatenando el FUB con un UUID versión 4, separados por un guión. Formato: <FUB>-<UUID4> Ejemplo: e7b5a4c2-9f4e-4a99-91a2-6d4a8a1eaf3d-550e8400-e29b-41d4-a716-446655440000	Sí

Respuesta

Propiedad	Tipo	Descripción
message	String	Registro de finalización de búsqueda histórica guardado correctamente

Observaciones

Este endpoint simplifica el proceso de desactivación, requiriendo únicamente el **id** como método de identificación y permitiendo su integración directa con sistemas que ya cuenten con el identificador único asignado previamente.

Asimismo, **al recibir la desactivación del reporte, la institución deberá**:

- **Dar de baja el caso en sus sistemas internos**, eliminando cualquier estado activo asociado al identificador.
- **Detener toda tarea periódica, proceso automatizado o consulta recurrente** vinculada al **id**, a fin de evitar operaciones innecesarias o notificaciones fuera de vigencia.

9. Consideraciones sobre el cifrado de huellas y fotos de las personas desaparecidas o no localizadas.

Con el fin de garantizar la seguridad e interoperabilidad en el intercambio de información biométrica, se establecen las siguientes consideraciones:

Las instituciones diversas deberán enviar la información biométrica (fotos y huellas) de la persona desaparecida o no localizada de acuerdo con las siguientes reglas:

1. **Codificación y Cifrado**: Todos los archivos biométricos deberán convertirse a **base64** y, posteriormente, cifrarse con **AES-256-GCM**, utilizando la clave de biométricos asignada a cada institución diversa.
2. **Estructura**:
   a. **Fotos**: arreglo de cadenas ("fotos": ["<foto1>", "<foto2>"]) con su campo *formato_fotos*.
   b. **Huellas**: objeto JSON con etiquetas definidas en el Anexo 1 ("huellas": {"rone":"...", "lpalm":"..."}) con su campo *formato_huellas*.
3. **Omisión**: Si no se dispone de fotos o huellas en absoluto, se omitirá el arreglo/objeto completo. En el caso de las huellas, si no se dispone de todas las descritas en el Anexo 4, pueden incluirse sólo con las que se cuente, empleando siempre las etiquetas indicadas.

10. Requisitos de ciberseguridad para el uso de la Plataforma Única de Identidad por parte de instituciones diversas

Los requisitos de ciberseguridad para el uso de la Plataforma Única de Identidad por parte de instituciones diversas, son de carácter general y deberán ser cumplidos por cualquier institución diversa que se interconecte a la Plataforma Única de Identidad.

Responsabilidades de las instituciones públicas y diversas

Cada Institución diversa es responsable de garantizar la seguridad, disponibilidad, integridad, confidencialidad y resiliencia de la infraestructura, redes y sistemas utilizados para realizar la conexión y utilizar el servicio de la Plataforma Única de Identidad.

Cada Institución diversa deberá realizar un análisis de seguridad que identifiquen vulnerabilidades que representan riesgos operativos, legales y de exposición de datos en todos los recursos (servicios, aplicaciones e infraestructura) que interactúen con la Plataforma Única de Identidad, utilizando las mejores prácticas internacionales, incluyendo OWASP API Security Top 10, OWASP ASVS, NIST SP 800-53 y NIST SP 800-115.

Derivado de los análisis de seguridad ejecutados, las instituciones diversas deberán establecer las medidas de mitigación para cerrar todas las vulnerabilidades en los recursos que interactúen con la Plataforma Única de Identidad, incluyendo configuraciones, lógica de aplicación, código, autenticación y controles de acceso.

Requisitos técnicos

Para conectarse a la Plataforma Única de Identidad, las instituciones diversas deberán observar y cumplir los siguientes requisitos técnicos:

Verificación de Autenticación y Control de Acceso

- La API debe implementar autenticación JWT para permitir la ejecución de los endpoints desarrollados.
- Los tokens deben tener expiración obligatoria y no ser reutilizables.
- Se debe validar control de acceso a nivel de:
    - Endpoint
    - Método HTTP
    - Recurso específico
- Los intentos de acceso indebido deben responder con 401 o 403, sin revelar detalles internos.
- No se deben permitir accesos no autenticados a recursos que lo requieran.
- Implementación de MFA en accesos administrativos.

Validación y Sanitización de Entradas

- Todos los parámetros deben validarse estrictamente por tipo, longitud, formato y contenido, no permitir caracteres especiales como (%,<,>,’,”,/ etc).
- No deben generarse errores 500 por entradas malformadas.
- Se debe rechazar cualquier ‘payload’ inesperado con códigos de errores como 400 o 422.
- Deben utilizarse consultas parametrizadas para prevenir inyección (SQL, NoSQL, LDAP, XPath).

Métodos HTTP y Exposición de Funcionalidades

- Únicamente deben estar habilitados los métodos para los que funciona el endpoint, si funciona con un POST, otros métodos deben estar deshabilitados.
- Métodos no usados deben responder con 405 Method Not Allowed.
- Verb tampering y métodos inventados deben ser rechazados.

Configuración Segura de CORS (si aplica)

- No debe existir Access-Control-Allow-Origin: * en APIs autenticadas o con datos sensibles.
- Sólo dominios autorizados deben tener acceso.
- Deben controlarse headers, métodos y credenciales expuestas.

Manejo Seguro de Errores y Respuestas

- No deben exponerse:
    - Stacktraces
    - Mensajes internos
    - Información del framework o rutas del servidor
- Las respuestas deben ser consistentes y no revelar información sensible.

Validación de Rate Limiting y Controles Anti-abuso

- Deberán validarse límites por:
    - PI
    - Usuario
    - Token
- Sensores para detectar:
    - Ataques de fuerza bruta
    - DDoS de bajo volumen
    - Enumeración masiva de cuentas
- Respuestas adecuadas como 429 Too Many Requests.

Protección de Datos Sensibles

- Cifrado obligatorio en tránsito mediante TLS 1.2 o superior.
- Eliminación de datos sensibles en respuestas que no sean estrictamente necesarios.
- No se deben exponer:
    - Tokens completos
    - Contraseñas
    - Información personal innecesaria
- Los registros (logs) deben evitar almacenar información sensible.

Seguridad de Infraestructura y Encabezados

- Debe configurarse correctamente:
    - Strict-Transport-Security
    - X-Content-Type-Options: nosniff

- Anti-clickjacking X-Frame-Options
- Content-Security-Policy evitando unsafe-inline y unsafe-eval.
- Referrer-Policy
- Las Cookies deben configurarse con atributos Secure, HttpOnly, Samesite y Max-Age/Expires

- Deben deshabilitarse:
  - Protocolos de comunicación inseguros como SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 deben estar deshabilitados.
  - Cifrados débiles.
  - Versiones de servidor e infraestructura expuestas en headers
  - Configurar el servidor para que los campos X-Powered-By y Server no expongan información.
  - Verificar que los puertos abiertos sean estrictamente los necesarios para el funcionamiento.

Comprobación de Versionamiento y Endpoints Deprecados

- Los endpoints obsoletos deben estar deshabilitados o protegidos.
- No se deben exponer versiones internas del API o del framework.

Mitigación de vulnerabilidades comunes

- XSS: escape adecuado, Content Security Policy (CSP).
- SQL Injection: uso de consultas preparadas.
- LFI/RFI: validación de rutas.
- Fuga de información: remoción de headers y banners sensibles.
- LLMNR/NTLM: endurecimiento del servidor según corresponda si hay hallazgos.

Reportes de seguridad

Para que una institución diversa pueda conectarse a la Plataforma Única de Identidad deberá enviar los reportes de las pruebas de seguridad SAST (Static Application Security), DAST (Dynamic Application Security) y SCA Software (Software Composition Analysis) realizadas sobre la URL Base y los endpoints desarrollados.

Los reportes deberán cumplir como mínimo con los siguientes requisitos:

● Los reportes deben ser generados directamente por las herramientas de pruebas que maneje cada Institución pública y diversa.

● Evidenciar que la ruta base y los endpoints evaluados se encuentren libres de vulnerabilidades Críticas, Altas, Medias y Bajas de acuerdo a los criterios de severidad reconocidos internacionalmente (por ejemplo CVSS).

● Incluir el alcance de las pruebas, metodología aplicada y herramientas utilizadas.

● En el reporte se debe mostrar fecha de ejecución, ambiente de ejecución (Productivo), URLs validadas y detalle de las pruebas.

La entrega y validación de esta documentación constituye un requisito obligatorio para autorizar la conectividad, integración o intercambio de información entre los endpoints y la Plataforma Única de Identidad, conforme a las mejores prácticas internacionales.

Anexos

Anexo 1. Ficha técnica de referencia para la integración tecnológica de instituciones públicas y diversas a la Plataforma Única de Identidad

Objetivo del anexo

Este anexo tiene como objetivo describir las tecnologías, componentes e infraestructura comúnmente utilizados para implementar la integración de instituciones públicas y diversas con la Plataforma Única de Identidad. Los elementos descritos son de carácter referencial y deseable, y no constituyen una imposición tecnológica, siempre que se cumpla con el Manual Técnico y los Requisitos de Ciberseguridad.

Infraestructura de red y conectividad

Se recomienda que la institución pública y diversa cuente con una infraestructura de red que permita una comunicación segura y controlada con la PUI, considerando lo siguiente:

- Dirección IP pública fija, para facilitar controles de acceso, listas blancas y monitoreo de seguridad.
- Conectividad a Internet permanente para garantizar la disponibilidad del servicio de integración.
- Certificado de seguridad TLS válido, con soporte para TLS versión 1.2 o superior, emitido por una autoridad certificadora reconocida.

Plataforma de ejecución

El servicio de integración puede implementarse sobre plataformas de uso común en entornos institucionales, tales como sistemas operativos tipo Linux, incluyendo Ubuntu, Red Hat, Amazon Linux u otros equivalentes.

La infraestructura podrá ser on premise, en nube pública, en nube privada o en esquemas híbridos. La elección de la plataforma queda a cargo de la institución pública y diversa.

Lenguajes de programación y frameworks referenciales

El desarrollo del servicio de integración puede realizarse utilizando lenguajes y frameworks ampliamente utilizados, entre otros:

- **Java**, utilizando frameworks como Spring Boot o Jakarta EE.
- **.NET**, mediante NET Core o ASP NET Core.
- **Node.js**, utilizando frameworks como Express o NestJS.
- **Python**, mediante frameworks como FastAPI, Flask o Django.

Servicio de integración institucional

La institución pública y diversa deberá desarrollar un servicio backend dedicado que funcione como punto de integración con la PUI. Dicho servicio deberá permitir recibir solicitudes oficiales de búsqueda, procesar mensajes estructurados basados en la CURP, ejecutar la lógica interna de consulta y generar respuestas conforme a los esquemas definidos en el Manual Técnico.

Seguridad de la comunicación

Se recomienda implementar mecanismos de seguridad que incluyan autenticación basada en tokens, como JWT, control de accesos por credenciales e IP, cifrado de la información en tránsito mediante HTTPS y validaciones de entrada y salida de datos. Estas medidas facilitan el cumplimiento de los Requisitos de Ciberseguridad y la validación del servicio.

Integración con sistemas internos

Para la consulta interna basada en CURP, la institución puede utilizar bases de datos relacionales o no relacionales, servicios internos, microservicios o sistemas legados, siempre que permitan la consulta por CURP. La lógica de consulta y la determinación de coincidencias reside exclusivamente en la institución pública y diversa.

Registro, monitoreo y ambientes

Es deseable que la institución cuente con bitácoras de solicitudes y respuestas, registro de eventos de seguridad y herramientas de monitoreo y alertamiento. Asimismo, se recomienda la separación de ambientes de pruebas y productivo, cada uno con su configuración, certificados e IP correspondientes.

Nota técnica de salvaguarda

Las tecnologías, infraestructuras y herramientas descritas en este anexo son referenciales y no constituyen requisitos obligatorios, siempre que se cumpla con lo establecido en el presente Manual y en los Requisitos de Ciberseguridad de la Plataforma Única de Identidad.

Anexo 2. Guía para el acceso e inscripción de instituciones diversas (personas morales) mediante Llave MX

Objetivo del anexo

Establecer el procedimiento normativo y operativo para el alta de instituciones diversas en la Plataforma Única de Identidad (PUI), garantizando que la identidad digital de la **Persona Moral** sea vinculada y validada correctamente a través del sistema **Llave MX**, conforme a los estándares de la Agencia de Transformación Digital y Telecomunicaciones (ATDT).

Alcance

Este anexo es de observancia obligatoria para los representantes legales de instituciones diversas. El proceso descrito es de carácter administrativo y de autenticación con el inicio de sesión único Llave MX; su cumplimiento es un requisito previo indispensable que no sustituye la interconexión técnica de las APIs detallada en el cuerpo de este Manual.

Requisitos previos de acceso

Para asegurar un flujo de registro exitoso, la institución debe contar con los siguientes elementos vigentes:

- **Cuenta Llave MX nivel ciudadano:** Perteneciente al representante legal que realizará el trámite.
- **e.Firma de la Persona Moral:** Es obligatorio poseer los archivos del Certificado (.cer), la Llave privada (.key) y la Contraseña de la e.Firma institucional, asociados a la persona Representante Legal.
- **RFC de la Institución:** Identificador que se utilizará en la Plataforma Única de Identidad.

Proceso operativo de alta (Paso a paso)

- **Autenticación Inicial:** El representante legal deberá ingresar al portal llave.gob.mx con sus credenciales de ciudadano.
- **Creación del Perfil Persona Moral:** Dentro de la plataforma, se deberá seleccionar la opción para agregar un perfil de **Persona Moral**.
- **Pasarela de Firmado Digital:** El usuario deberá cargar los archivos de la e.Firma de la institución. El sistema realizará una validación automática de integridad y vigencia. Si la e.Firma no es válida o está vencida, el sistema bloqueará el registro.
- **Gestión de Información Complementaria:** Tras la validación de la firma, el representante deberá completar obligatoriamente la "Información Complementaria" requerida en el perfil para habilitar el buzón de notificaciones administrativas.

Definición del Identificador Institucional

Una vez creado el perfil en Llave MX, el **RFC con homoclave** de la institución queda vinculado oficialmente como el identificador. Este valor es inalterable y deberá ser utilizado estrictamente en todas las estructuras de datos enviadas a la PUI.

Pruebas de Acceso y Acreditación

La institución podrá validar su acreditación ingresando al detalle del perfil en Llave MX. La visualización correcta de los datos institucionales confirma que la Persona Moral ha sido reconocida por el Gobierno de México y está facultada para proceder con la fase de integración técnica.

Alcance y Limitaciones Técnicas

El acceso mediante Llave MX se limita a la gestión de identidad y trámites administrativos. Este acceso no habilita por sí mismo el intercambio de información operativa ni la ejecución de servicios. Para iniciar operaciones productivas con la PUI, la institución deberá:

- Desarrollar los endpoints requeridos conforme a la Sección 8 del Manual Técnico.
- Superar las validaciones de seguridad (SAST, DAST, SCA) conforme a los Requisitos de Ciberseguridad, evidenciando que la URL Base y endpoints están libres de vulnerabilidades.
- Implementar bitácoras de auditoría que registren todas las interacciones con la PUI, conforme al Anexo 5.
- Aprobar las pruebas de conectividad y funcionales en el ambiente de Sandbox antes de pasar a producción.

Mantenimiento y Responsabilidades

Es responsabilidad exclusiva de la institución diversa mantener actualizada su e.Firma ante el Servicio de Administración Tributaria y reflejar cualquier cambio en Llave MX. La falta de vigencia en la firma digital institucional en el portal administrativo podrá derivar en la revocación automática de los tokens de acceso a la API de producción por motivos de seguridad.

Anexo 3. Alcance y descripción del desarrollo tecnológico que deberán implementar las instituciones públicas y diversas.

Objetivo del anexo

Este anexo describe de manera puntual y concreta el desarrollo que deberán realizar las instituciones públicas y diversas para integrarse a la Plataforma Única de Identidad. El objetivo es clarificar qué componentes deben construirse, cuál es su función y cómo se relacionan con los flujos definidos en el Manual Técnico, sin entrar en código ni imponer tecnologías específicas.

Alcance del desarrollo

El desarrollo descrito en este anexo aplica exclusivamente a las instituciones públicas y diversas que participen en la PUI.

Incluye únicamente los componentes necesarios para recibir solicitudes oficiales, consultar sistemas internos con base en la CURP y responder conforme a los formatos establecidos.

No incluye desarrollos de tipo administrativo, de autenticación institucional mediante Llave MX ni funcionalidades no relacionadas con la PUI.

Servicio de integración institucional

La institución deberá desarrollar un servicio backend propio que funcione como el punto de integración con la PUI. Este servicio deberá estar disponible de forma continua y ser accesible desde Internet de manera segura.

Recepción de solicitudes oficiales

El servicio de integración deberá estar preparado para recibir solicitudes oficiales de búsqueda emitidas por la PUI.

Cada solicitud contendrá información estructurada y la CURP como identificador obligatorio.

El servicio deberá validar que la solicitud cumple con los formatos y reglas definidos en el Manual Técnico antes de ser procesada.

Procesamiento de la solicitud

Una vez validada la solicitud recibida, el servicio deberá iniciar su procesamiento interno, lo cual incluye:

- Identificar la CURP recibida.
- Asociar la solicitud con el identificador de búsqueda correspondiente.
- Determinar el tipo de búsqueda aplicable conforme a las fases definidas.

Consulta a sistemas internos basada en CURP

El servicio de integración deberá ejecutar una consulta controlada a los sistemas de información internos de la institución utilizando la CURP como clave de búsqueda.

La consulta podrá realizarse sobre bases de datos, servicios internos o sistemas legados, siempre que permitan la búsqueda por CURP.

La lógica de consulta, correlación y decisión reside completamente en la institución pública y diversa.

Determinación de coincidencias

Con base en el resultado de la consulta interna, la institución deberá determinar si existe información relevante asociada a la CURP consultada.

Esta determinación podrá corresponder a información básica, histórica o a coincidencias posteriores, según la fase de búsqueda aplicable.

Construcción de la respuesta

Cuando aplique, el servicio de integración deberá construir una respuesta conforme a los formatos definidos en el Manual Técnico.

La respuesta deberá incluir la CURP y el identificador de búsqueda correspondiente, así como la información requerida para el tipo de notificación que se esté realizando.

Envío de la respuesta a la PUI

La respuesta construida deberá enviarse a la PUI utilizando el mecanismo definido en el presente manual.

El envío deberá realizarse de forma segura, controlada y únicamente en los supuestos permitidos.

No deberán enviarse respuestas fuera de los escenarios definidos.

Seguridad del desarrollo

Es obligatorio que el desarrollo sea sometido a pruebas de seguridad conforme a los lineamientos de la PUI.

Como requisito previo a la conexión, la institución debe enviar los reportes generados por herramientas de:

- **SAST** (Static Application Security Testing).
- **DAST** (Dynamic Application Security Testing).
- **SCA** (Software Composition Analysis).

Criterio de cumplimiento: Los reportes deben evidenciar que la URL Base y los endpoints están **100% libres de vulnerabilidades** (Críticas, Altas, Medias y Bajas).

Trazabilidad y bitácoras

El desarrollo debe contemplar obligatoriamente el registro estructurado de todas las interacciones (Logs).

Qué registrar:

- Todas las solicitudes recibidas (ej. /activar-reporte).
- Consultas internas ejecutadas en las bases de datos de la institución.
- Respuestas enviadas a la PUI (ej. /notificar-coincidencia).

Objetivo: Estas bitácoras deben permitir la auditoría completa del proceso para garantizar que el tratamiento de datos personales sea conforme a la ley.

Validación del desarrollo

Una vez desarrollados los endpoints y asegurada la trazabilidad, la institución debe superar:

- Pruebas de conectividad.
- Pruebas funcionales.
- Validaciones de seguridad (revisión de los reportes SAST/DAST).

Importante: La operación productiva **sólo puede iniciarse** tras superar estas validaciones.

Consideraciones finales

El desarrollo descrito en este anexo representa el conjunto mínimo de componentes necesarios para una integración correcta con la Plataforma Única de Identidad.

Cualquier desarrollo adicional queda a criterio de la institución, siempre que no contravenga el presente Manual ni los Requisitos de Ciberseguridad.

Anexo 4. Tabla de mapeo de etiqueta y descripción de huellas

La siguiente tabla establece la correspondencia a la etiqueta la cual se toma como referencia para llenar el Object (Json) de las huellas según la etiqueta que le corresponde.

Etiqueta	Descripción
rone	Pulgar derecho
rtwo	Índice derecho
rthree	Medio derecho
rfour	Anular derecho
rfive	Meñique derecho
lone	Pulgar izquierdo

Etiqueta	Descripción
ltwo	Índice izquierdo
lthree	Medio izquierdo
lfour	Anular izquierdo
lfive	Meñique izquierdo
rpalm	Palma derecha
lpalm	Palma izquierda

Anexo 5. Tabla de mapeo de códigos de CURP a entidades federativas

La siguiente tabla establece la correspondencia entre el código de dos letras (posiciones 12–13 de la CURP) y el valor que debe enviarse en el campo *lugar_de_nacimiento*.

Código	Estado / Valor a enviar
AS	AGUASCALIENTES
BC	BAJA CALIFORNIA
BS	BAJA CALIFORNIA SUR
CC	CAMPECHE
CS	CHIAPAS
CH	CHIHUAHUA
DF	CDMX
CL	COAHUILA
CM	COLIMA
DG	DURANGO
GT	GUANAJUATO
GR	GUERRERO
HG	HIDALGO
JC	JALISCO
MC	MÉXICO
MN	MICHOACÁN
MS	MORELOS

Código	Estado / Valor a enviar
NT	NAYARIT
NL	NUEVO LEÓN
OC	OAXACA
PL	PUEBLA
QO	QUERÉTARO
QR	QUINTANA ROO
SP	SAN LUIS POTOSÍ
SL	SINALOA
SR	SONORA
TC	TABASCO
TS	TAMAULIPAS
TL	TLAXCALA
VZ	VERACRUZ
YN	YUCATÁN
ZS	ZACATECAS
NE	FORÁNEO
XX	DESCONOCIDO

Notas:

El código **NE** debe mapearse siempre a **FORÁNEO**, es decir, nacido en el extranjero, ya sea una persona mexicana o extranjera.

El código **XX** no forma parte de la CURP oficial y se utiliza para indicar que el lugar de nacimiento es **DESCONOCIDO**.

Dado en la Ciudad de México a los 13 días del mes de enero de 2026, autoriza **FÉLIX ARTURO ARCE VARGAS**, **Director General del Registro Nacional de Población e Identidad de la Subsecretaría de Derechos Humanos, Población y Migración de la Secretaría de Gobernación**, con fundamento en los artículos 1o., párrafo tercero, 4o, párrafo décimo, 6o, apartado A, fracción II, 16, párrafo segundo, y 36, fracción I de la Constitución Política de los Estados Unidos Mexicanos; 27, fracción VI de la Ley Orgánica de la Administración Pública Federal; 86, 91, 91 Bis, 92 y 94 de la Ley General de Población; 3, apartado A, fracción II, inciso b, numeral 3 y 60, fracciones I III y V del Reglamento Interior de la Secretaría de Gobernación, así como 5, fracción XVIII, 6, fracciones III y IV y 8 de los Lineamientos para el Desarrollo y Operación de la Plataforma Única de Identidad.- Rúbrica.