



SECRETARÍA DE GOBERNACIÓN

DIRECCIÓN GENERAL DEL REGISTRO NACIONAL DE POBLACIÓN E IDENTIFICACIÓN PERSONAL

INFORME SOBRE EL USO DE LOS DATOS CONTENIDOS EN EL REGISTRO NACIONAL DE USUARIOS DE TELEFONÍA MÓVIL, Y LAS MEDIDAS DESTINADAS A GARANTIZAR SU DEBIDO RESGUARDO Y EVENTUAL CANCELACIÓN

MAYO DE 2012

Contenido

I. ANTECEDENTES	4
II. MARCO NORMATIVO DEL RENAUT	7
1. Ley Federal de Telecomunicaciones	7
2. Reglas de operación del RENAUT	10
3. Derogación del RENAUT	12
III. PARTICIPACIÓN DE LA SECRETARÍA DE GOBERNACIÓN	14
IV. INFORME TÉCNICO	17
1. Datos Generales	17
2. Información Estadística	18
3. Aplicaciones	19
4. Protección de Datos Personales y Seguridad de la Información	20
5. Almacenamiento lógico	24
6. Almacenamiento físico	25
7. Respaldos	25
8. Bloqueo y conservación de datos	26
9. Cancelación de la información	26
V. ANEXOS	29



Anexo 1

29

Anexo 2

30

I. ANTECEDENTES

El 25 de agosto de 2008 se publicó en el Diario Oficial de la Federación (DOF) el “Acuerdo Nacional por la Seguridad, la Justicia y la Legalidad”. Este Acuerdo fue suscrito el 21 de agosto de 2008 por los Poderes Ejecutivos Federal y Estatales, el Congreso de la Unión, el Poder Judicial Federal, representantes de las asociaciones de Presidentes Municipales, medios de comunicación y las organizaciones de la sociedad civil, empresariales, sindicales y religiosas, en el marco de la Vigésima Tercera Sesión Ordinaria del Consejo Nacional de Seguridad Pública.

El motivo que impulsó la celebración de dicho Acuerdo multisectorial fue el reconocimiento por parte de muy diversos sectores de la sociedad mexicana del importante reto que representa el combate a la impunidad, la corrupción, la falta de coordinación entre las autoridades, así como la inseguridad y la violencia.

Uno de los aspectos más delicados fue sin duda, la penetración de la delincuencia en los órganos de seguridad y la complicidad de algunas autoridades con los criminales. En razón de ello, y a efecto de poner un alto al crimen y a la inseguridad que minan el desarrollo de las personas y el progreso de nuestro país, la sociedad exigió de sus autoridades un compromiso para contar con instituciones de seguridad sólidas, eficaces y honestas, así como para replantear los mecanismos de coordinación interinstitucional.

En este sentido, se buscaron compromisos que garantizaran la coordinación, cooperación e intercambio de información entre los tres Poderes de la Unión y los tres órdenes de gobierno. Asimismo, el Acuerdo sumó a los ciudadanos, a la sociedad civil y a sus organizaciones más representativas, en donde se incluyeron las empresariales.

En este contexto, se reconoció el esfuerzo institucional para frenar la acción del crimen organizado, a través de acciones como dotar a las fuerzas del orden con tecnología de punta y sistemas de información e inteligencia policial adecuados, eficaces y eficientes, con el objetivo de garantizar de manera más efectiva la seguridad pública. También se establecieron compromisos interinstitucionales para dotar al Estado mexicano de mayores herramientas para hacer frente, de manera conjunta, a los retos planteados, a fin de desarrollar y complementar el marco normativo en materia de seguridad pública y fortalecer los mecanismos de información e inteligencia.

En este contexto, el Poder Ejecutivo Federal asumió, entre otros, el siguiente compromiso:

“Artículo Segundo:

...

VII. Regular el registro, establecimiento y acceso a bases de datos de los equipos de telefonía móvil y fija, así como el acceso a la información sobre la ubicación física de los móviles en tiempo real, en los casos en que sean aparatos y números telefónicos relacionados con actividades delictivas.

Las secretarías de Comunicaciones y Transportes, Economía, Seguridad Pública, así como la Procuraduría General de la República y la Comisión Federal de Telecomunicaciones, se comprometen a emitir o, en su caso, a promover un instrumento de regulación, realización de inspecciones y aplicación de las normas en caso de incumplimiento.

- Tiempo de ejecución: seis meses.

...”

De esta forma, el H. Congreso de la Unión aprobó el “Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones” (en adelante el DECRETO RENAUT), el cual se publicó el 9

de febrero de 2009 el DOF, instrumento por el que creó el Registro Nacional de Usuarios de Telefonía Móvil (RENAUT).

El RENAUT fue concebido como una gran base de datos cuyo fin fue concentrar la información de los usuarios de telefonía móvil con el objeto de coadyuvar en la prevención, investigación y persecución de delitos como el secuestro y la extorsión.

Sin embargo, y con el fin de contar con mejores instrumentos para la prevención, investigación y persecución de delitos, el H. Congreso de la Unión aprobó el "Decreto por el que se reforman, adicionan y derogan diversas disposiciones del Código Federal de Procedimientos Penales, del Código Penal Federal, de la Ley Federal de Telecomunicaciones, de la Ley que Establece las Normas Mínimas sobre Readaptación Social de Sentenciados y de la Ley General del Sistema Nacional de Seguridad Pública" (en adelante el DECRETO), publicado en el DOF el 17 de abril del año que transcurre, mismo que dio por terminado el funcionamiento de dicho registro.

Asimismo, este DECRETO establece en su artículo Segundo Transitorio, del artículo Tercero, que la Secretaría de Gobernación y la Comisión Federal de Telecomunicaciones deberán remitir al Congreso de la Unión, un informe sobre el uso de los datos contenidos en el Registro Nacional de Usuarios de Telefonía Móvil y sobre las medidas destinadas a garantizar su debido resguardo y eventual cancelación, dentro de los quince días naturales siguientes a la entrada en vigor de dicho DECRETO.

II. MARCO NORMATIVO DEL RENAUT

1. Ley Federal de Telecomunicaciones

El DECRETO RENAUT estableció, entre otras, las siguientes obligaciones relacionadas con la integración y administración del RENAUT:

A. La obligación de la Secretaría de Comunicaciones y Transportes:

- Supervisar, a través de la Comisión Federal de Telecomunicaciones, la elaboración y actualización por parte de los concesionarios del Registro Nacional de Usuarios de Telefonía Móvil de (Art. 7, fracción XIII).

B. La obligación de los concesionarios de redes públicas de telecomunicaciones de:

- Llevar un registro y control separado de sus usuarios, tanto en la modalidad de líneas contratadas en plan tarifario, como en líneas de prepago, el cual contendría como mínimo los siguientes datos:
 - Número y modalidad de la línea telefónica.
 - Nombre completo, domicilio, nacionalidad, número correspondiente y demás datos contenidos en identificación oficial vigente con fotografía, así como comprobante de domicilio actualizado del usuario y toma de impresión de huella dactilar directamente en tinta y/o electrónicamente (Arts. 44, fracciones XI, XII y XIII, 64, fracción XVI, y Sexto Transitorio).

- Conservar copias fotostáticas o en medios electrónicos de los documentos necesarios para el RENAUT, así como mantener la reserva y protección de las bases de datos personales, las cuales no podrán ser usadas con fines diferentes a los señalados en las leyes.

- Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permita identificar con precisión los siguientes datos:
 - Tipo de comunicación, servicios suplementarios o servicios de mensajería o multimedia empleados.
 - Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago.
 - Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia.
 - Se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización desde la que se haya activado el servicio.
 - La ubicación digital del posicionamiento geográfico de las líneas telefónicas.
 - La obligación de conservación de datos cesa a los doce meses, contados a partir de la fecha en que se haya producido la comunicación.

- Tomar las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control.

- Entregar los datos conservados al Procurador General de la República o Procuradores Generales de Justicia de las Entidades Federativas, cuando realicen funciones de investigación de los delitos de extorsión, amenazas, secuestro, en cualquiera de sus modalidades o de algún delito grave o relacionado con la delincuencia organizada, en sus respectivas competencias.
- En los casos de contratación de telefonía móvil, solicitar la Credencial para votar emitida por el Instituto Federal Electoral y/o Cédula Única del Registro Nacional de Población (CURP) y/o Pasaporte, y acompañarlo con constancia de domicilio oficial con recibo de agua, luz y/o teléfono, además de la impresión de la huella dactilar directamente en tinta y/o electrónicamente.
- Realizar campañas y programas informativos a sus clientes o usuarios para incentivar la obligación de denunciar en forma inmediata el robo o extravío de sus equipos celulares o chips inteligentes, para prevenir cualquier uso indebido de las líneas, así como en los casos que se trate de venta o cesión de una línea telefónica.

C. La obligación de la Comisión Federal de Telecomunicaciones (Artículos Segundo y Tercero Transitorios):

- Elaborar el proyecto de reglamento que debería emitir el Ejecutivo Federal.
- Expedir las disposiciones administrativas para reglamentar el registro de usuarios de telefonía, así como la actualización de datos personales y registros fehacientes de identificación y ubicación de los usuarios que contratan telefonía en cualquiera de sus modalidades.

A este respecto, es menester señalar que el citado reglamento relativo a las reformas a la *Ley Federal de Telecomunicaciones* no se expidió.

Como puede observarse, de la lectura de la citada reforma a la *Ley Federal de Telecomunicaciones* se desprende que el legislador no asignó obligación alguna para la Secretaría de Gobernación en relación con la integración del RENAUT. De igual forma, la ley establece con claridad los sujetos obligados, tanto públicos como privados, así como sus respectivas obligaciones relativas a la integración del citado Registro.

2. Reglas de operación del RENAUT

El Pleno de la Comisión Federal de Telecomunicaciones publicó el 15 de mayo de 2009 en el DOF, las "Reglas del Registro Nacional de Usuarios de Telefonía Móvil". Su objeto fue establecer la forma en que los proveedores de servicios llevarían el registro de usuarios de telefonía móvil, incluyendo la actualización de sus datos personales, así como los registros fehacientes de identificación y ubicación de los usuarios del servicio de telefonía móvil.

Las citadas Reglas establecieron las siguientes obligaciones:

A. Para los usuarios:

- Proporcionar la información necesaria para el registro de sus líneas telefónicas en el RENAUT.

B. Para el Proveedor de Servicios:

- No activar los servicios de la línea telefónica del usuario en caso de falta de registro.

- Poner a disposición de sus usuarios un número para la atención de reportes de robo o extravío, el cual debería estar disponible las 24 horas del día los 365 días del año.
- Mantener la información relativa a la modalidad de las líneas telefónicas, ya sean de prepago o de pospago.
- Mantener un registro de comunicaciones de voz que incluyera la fecha, la hora de inicio, la duración de la llamada y la ubicación digital de posicionamiento geográfico.
- Mantener un registro de mensajes cortos (SMS) y multimedia (MMS) que incluyera fecha de envío del mensaje, hora de envío y ubicación digital de posicionamiento geográfico.
- Mantener un registro de comunicaciones de datos que incluyera fecha de inicio de la sesión de datos, hora de inicio y hora de terminación de la sesión de datos y la ubicación digital de posicionamiento geográfico.

C. Generalidades:

- Estableció el sistema de SMS (*Short Message Service*) como el medio válido para que el usuario llevara a cabo el alta y la baja del registro de una línea telefónica en el RENAUT.
- Como medios alternos se establecieron la validación vía comandos IP (servicios WEB) y los procesos vía Batch.

A este respecto se informa que, de conformidad con *Ley Federal de Telecomunicaciones*, los sujetos obligados a integrar y administrar el RENAUT eran los concesionarios de redes públicas de telecomunicaciones, en términos de

los artículos 44, fracciones. XI, XII y XIII, 64, fracción XVI, y Sexto Transitorio del respectivo DECRETO RENAUT.

Como se detallará en el apartado III del presente informe, la Secretaría de Gobernación únicamente colaboró con la Secretaría de Comunicaciones y Transportes y la Comisión Federal de Telecomunicaciones a fin de posibilitar la verificación y acreditación fehaciente de la identidad de los usuarios inscritos en el RENAUT, por medio de la validación de la CURP que se enviaba a la Dirección General del Registro Nacional de Población e Identificación Personal, para dar de alta una línea de telefonía móvil.

Lo anterior, en razón de que la Secretaría de Gobernación, de conformidad con la *Ley Federal de Telecomunicaciones*, no era responsable de la administración del RENAUT.

3. Derogación del RENAUT

El pasado 17 de abril de 2012, se publicó en el DOF el DECRETO que derogó la figura del RENAUT.

Esta nueva reforma a la *Ley Federal de Telecomunicaciones* establece en su artículo Segundo Transitorio, del Artículo Tercero, del DECRETO que la Secretaría de Gobernación y la Comisión Federal de Telecomunicaciones deberán remitir al Congreso de la Unión, un informe sobre el uso de los datos contenidos en el Registro Nacional de Usuarios de Telefonía Móvil y sobre las medidas destinadas a garantizar su debido resguardo y eventual cancelación, dentro de los quince días naturales siguientes a la entrada en vigor de dicho DECRETO.

Finalmente, se informa que la Secretaría de Gobernación ha sostenido reuniones de trabajo con el Instituto Federal de Acceso a la Información y Protección de

Datos, con la finalidad de establecer las medidas técnicas necesarias para la cancelación de los datos del RENAUT.

III. PARTICIPACIÓN DE LA SECRETARÍA DE GOBERNACIÓN

La hoy derogada fracción XVI del artículo 64 de la *Ley Federal de Telecomunicaciones* establecía que, tratándose de contratación de telefonía móvil, los concesionarios deberían solicitar la CURP.

En este sentido, el artículo 27, fracción V, de la *Ley Orgánica de la Administración Pública Federal*, establece que corresponde a la Secretaría de Gobernación manejar el Servicio Nacional de Identificación Personal, a través de la Dirección General del Registro Nacional de Población e Identificación Personal que, en consonancia con el artículo 1º, fracción VI, inciso a), del "Acuerdo por el que se adscriben orgánicamente las unidades administrativas y los órganos desconcentrados de la Secretaría de Gobernación", publicado en el DOF el 8 de agosto de 2002, está adscrita a la Subsecretaría de Población, Migración y Asuntos Religiosos.

Asimismo, la *Ley General de Población* y su Reglamento establecen en sus numerales 85 y 92, y 41 a 43, respectivamente, que la Secretaría de Gobernación tiene a su cargo la acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero. Por ende, esta dependencia cuenta con las atribuciones para coordinar los métodos de identificación de las dependencias de la Administración Pública Federal, con el fin de constituir un sistema integrado de registro de población.

De acuerdo con lo anterior, las dependencias y entidades de la Administración Pública Federal que en virtud de sus atribuciones, integran algún registro de personas, deben adoptar el uso de la CURP como elemento de aquél.

Al respecto, corresponde a la ya citada Dirección General del Registro Nacional de Población e Identificación Personal la asignación de la CURP, con fundamento en los artículos 23, fracción III, del *Reglamento Interior de la Secretaría de Gobernación* y 3º del "Acuerdo para la Adopción y Uso por la Administración Pública Federal de la Clave Única de Registro de Población", publicado en el DOF el 23 de octubre de 1996.

Por lo anteriormente expuesto, resultó conveniente que la Secretaría de Gobernación colaborara con la Secretaría de Comunicaciones y Transportes y la Comisión Federal de Telecomunicaciones, a fin de posibilitar la verificación y acreditación fehaciente de la identidad de los usuarios inscritos en el RENAUT, por medio de la validación de la CURP que se enviaba a la Dirección General del Registro Nacional de Población e Identificación Personal, para dar de alta una línea de telefonía móvil.

De esta forma, con base en la obligación de cooperación técnica prevista en el artículo 25 de la *Ley Orgánica de la Administración Pública Federal*, las Secretarías de Gobernación y de Comunicaciones y Transportes, suscribieron el 21 de octubre de 2009 las *Bases de Colaboración* para que la Secretaría de Gobernación, a través de la Dirección General del Registro Nacional de Población e Identificación Personal, verificara la identidad de los usuarios mediante el cotejo de los datos personales contenidos en el RENAUT con la CURP, a fin de corroborar la información.

Consecuentemente, la Secretaría de Gobernación únicamente coadyuvó con la Secretaría de Comunicaciones y Transportes y la Comisión Federal de Telecomunicaciones en estricto apego a sus atribuciones en materia de verificación de la identidad y asignación de la CURP.

El procedimiento se realizó mediante el envío de un mensaje del usuario, el cual solicitó el alta correspondiente al enviar la CURP”.

De manera alterna se recibían peticiones de los concesionarios a través de los servicios WEB y archivos Batch para validación de las CURP. El proveedor NEXTEL utilizaba este mecanismo como su vía principal de validación, mientras que los otros concesionarios la utilizaron sólo de manera esporádica.

De esta manera, la Secretaría de Gobernación únicamente conserva un archivo histórico o administrativo de los cotejos de identidad solicitados, que consisten en la validación de una CURP existente asociada a un número telefónico móvil. Dicho archivo comparte los recursos de almacenamiento de la Base de Datos Nacional de la CURP.

Se insiste, por tanto, que la intervención de la Secretaría de Gobernación se limitó a recibir los SMS que enviaban los usuarios de telefonía móvil, para validar su CURP y dar de alta su línea telefónica. De suerte que la única información con la que esta dependencia cuenta, es una Tabla de Verificación de la CURP relacionada a un número telefónico.

Por estas razones, es posible afirmar que en ningún momento se ponen en riesgo los datos personales de los usuarios de telefonía móvil, u otro tipo de información sensible.

Finalmente, se informa que la Secretaría de Gobernación recibió el primer registro producto de las validaciones de la CURP el 9 de abril de 2009 y, en cumplimiento del DECRETO, la Secretaría de Gobernación recibió el último registro el 17 de abril de 2012.

IV. INFORME TÉCNICO

Dentro de este informe se presentan las principales características técnicas de las aplicaciones de validación que ha soportado la operación de la CURP, así como los mecanismos de seguridad que permiten garantizar la integridad, confidencialidad y resguardo de los datos personales y se describe el procedimiento de borrado que eventualmente se realizaría.

1. Datos Generales

A continuación se detallan los datos de aplicación de la validación:

Sistema operativo: HP-UX 11g

Versión Oracle: Oracle Database 11g Enterprise Edition Release 11.2.0.2.0

Espacio utilizado: 218,652 MB (218 GB)

Registros al día 17 de abril de 2012: 98,455,247

Inicio de operación: 09 de abril de 2009

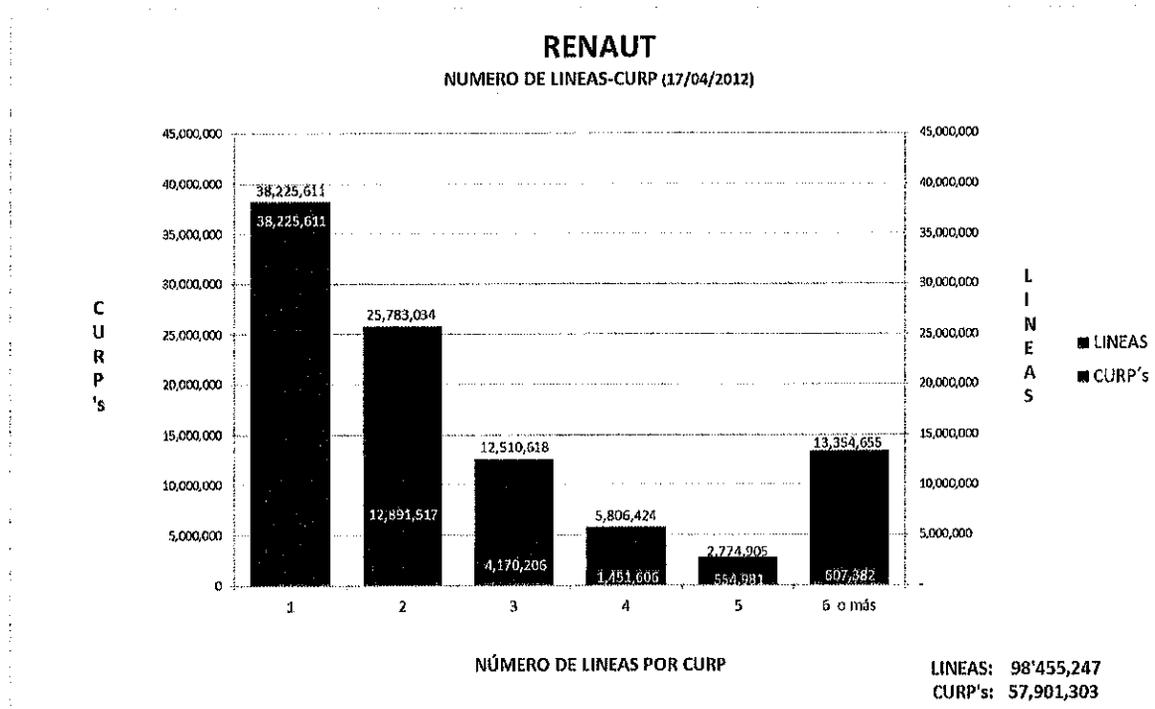
Fin de operaciones: 17 de abril de 2012

Es importante aclarar que la información de las validaciones de la CURP comparten los recursos de sistema operativo, servidor, almacenamiento y motor de base de datos utilizados en la operación del Programa de Uso y Adopción de la CURP.

2. Información Estadística

Registros al día 17 de abril de 2012: 98,455,247

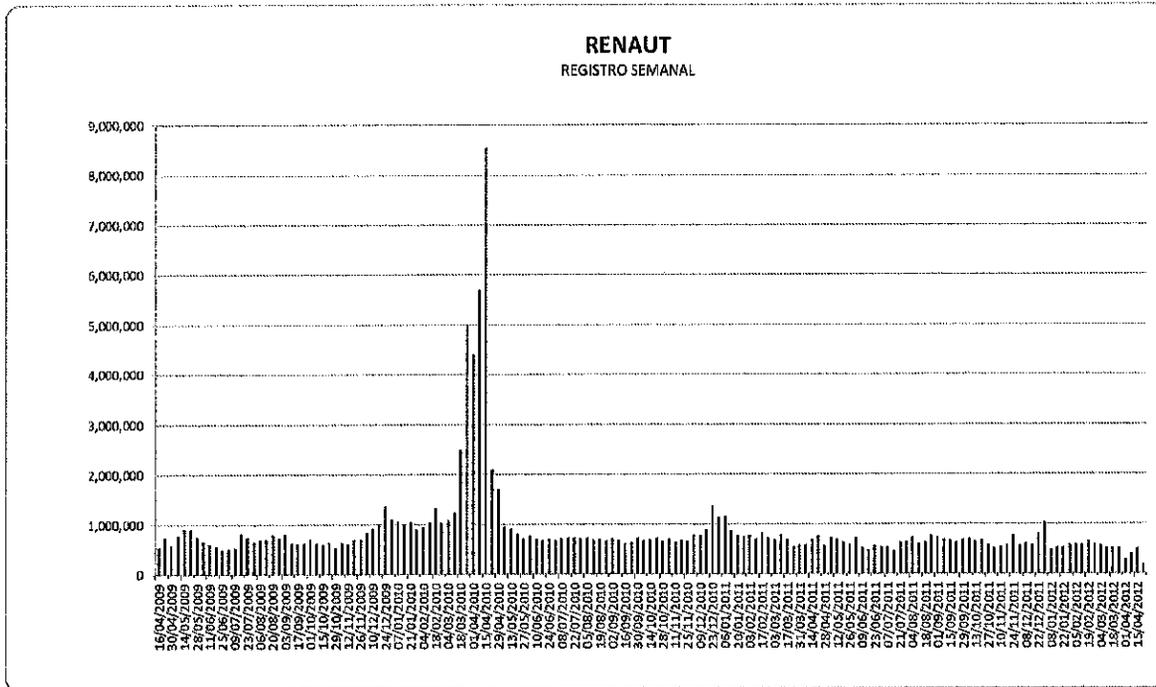
En la siguiente gráfica se puede observar la cantidad de líneas asociadas a una CURP:



Como puede verse, el 66.01% de las CURP registradas tienen asociado un número celular; 22% de las CURP tiene asociado dos líneas; 7.2% están asociadas a tres líneas; 2.5% de las CURP tienen asociadas cuatro líneas telefónicas; 0.95% están asociadas a cinco celulares y, finalmente, 1.04% de las CURP registradas están asociadas a seis o más líneas telefónicas.

La siguiente gráfica muestra la cantidad de celulares que se registraron semanalmente durante la vigencia del Registro. Sobre el particular, se observa un incremento importante en el mes de abril de 2010, situación que se dio por el

plazo que se tenía para realizar el registro de aquellos celulares que operaban antes de la creación del registro.



3. Aplicaciones

La operación está conformada por tres esquemas que permiten acceder a los servicios de validación de la CURP a las compañías telefónicas:

- **SMS.-** Mecanismo mediante el cual el usuario envía un mensaje desde su teléfono celular el cual contiene su CURP.
- **Web Services.-** Mecanismo que permite a las telefónicas realizar la validación mediante aplicaciones Web.
- **Batch.-** Mecanismo que permite a las telefónicas realizar la validación de CURP de manera masiva.

4. Protección de Datos Personales y Seguridad de la Información

La debida protección de los datos personales y su adecuado tratamiento y resguardo es un tema que ha ocupado un lugar preponderante en la agenda nacional. Es clara la importancia de velar por el adecuado manejo de la información y, por supuesto, por la existencia de medidas físicas y lógicas de protección de la información.

En este apartado se refieren las medidas de seguridad implementadas por la Secretaría de Gobernación a fin de garantizar la confidencialidad, integridad y disponibilidad de los datos registrados. La confidencialidad garantiza la protección contra accesos no autorizados a la información. La integridad previene contra alteraciones no autorizadas de la información. Por último, la disponibilidad hace referencia a la garantía de un acceso sin interrupciones a la información.

Con estas acciones se busca asegurar que el ente que recopila los datos personales debe de protegerlos mediante la implementación de medidas técnicas y organizativas que resulten idóneas en cada momento para garantizar su integridad, confidencialidad y disponibilidad.

Al respecto es oportuno mencionar que la Secretaría de Gobernación ha adoptado los más altos estándares en materia de seguridad de la información. Asimismo, existe un marco jurídico en materia de protección de datos y responsabilidades que evita el abuso en el manejo de esta información, lo que permite que la Secretaría de Gobernación desarrolle sus funciones de verificación de la CURP con absoluta seguridad.

Por lo anterior, es una obligación de la Dirección General del Registro Nacional de Población e Identificación Personal adoptar y mantener las medidas de seguridad

administrativas, físicas y técnicas necesarias para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, mediante acciones que eviten su daño, alteración, pérdida, destrucción, o el uso, transmisión y acceso no autorizado.

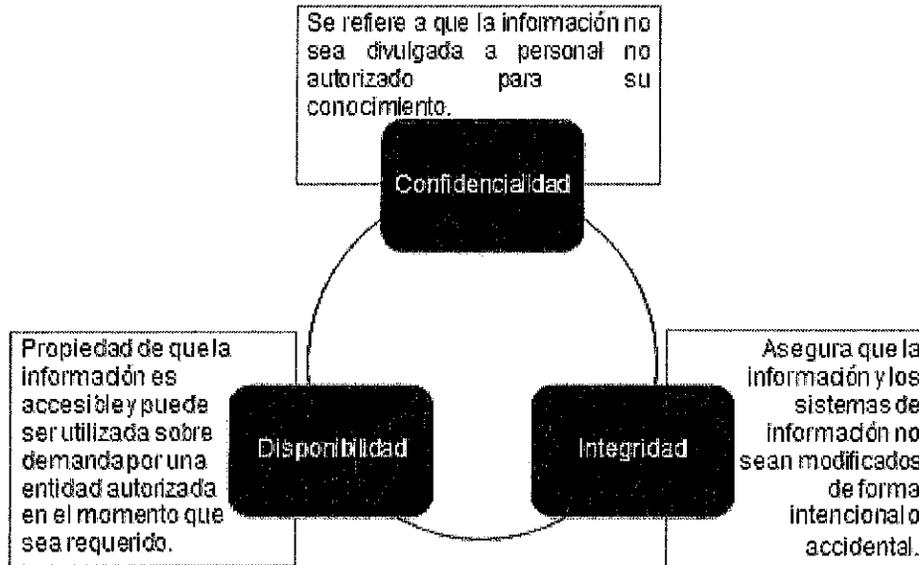
En este sentido, la Secretaría de Gobernación cumplió con las medidas establecidas por la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental* (LFTAIPG), su Reglamento y los Lineamientos para la protección de datos personales (Lineamientos) expedidos por el Instituto Federal de Acceso a la Información y Protección de Datos, en materia de protección de datos personales, tales como:

- La Secretaría de Gobernación ha capacitado debidamente a los servidores públicos involucrados en el manejo de las Tablas de Verificación de la CURP;
- Se ha dado a conocer información sobre las políticas en relación con la protección de datos personales;
- Se han adoptado medidas que garantizan la seguridad de los datos personales y evitan su alteración, pérdida, transmisión y acceso no autorizado;
- No se han difundido o distribuido los datos personales contenidos en las Tablas de Verificación de la CURP;
- Se cuenta con un sitio seguro para el sistema de datos personales y se tiene controlado el acceso a las instalaciones donde se encuentra el equipo;
- Se tienen procedimientos de control de acceso con perfiles de usuarios y mecanismos de auditoría o rastreabilidad de operaciones, y
- Se tienen operaciones de acceso, actualización, respaldo y recuperación.

Adicionalmente, se cuenta con medidas de seguridad implementadas para lograr mayor protección de los servidores, frente a diferentes riesgos detonados por amenazas como pudieran ser el sabotaje, la divulgación no autorizada, el fraude, la interrupción del servicio, el mal uso de la información y los desastres naturales, tales como:

- Centro de Operaciones de Seguridad (Security Operations Center: SOC).- El SOC brinda un servicio de protección integral contra riesgos y amenazas latentes en la red con el fin de proveer de confidencialidad, integridad y disponibilidad de la información. La disponibilidad de este servicio es 7x24x365.
- Pruebas de Intrusión (Hackeo Ético).- Se realizan pruebas continuas al sistema con el fin de evaluar la seguridad lógica con la que cuenta para así estar en posibilidades de mitigar aquellas vulnerabilidades con las que se cuente la posibilidad de remediar.
- Proceso de administración de cambios.
- Proceso de administración de incidencias.
- Protección contra amenazas externas y ambientales.
- Control biométrico al Centro de Datos para eliminar los accesos no autorizados.
- Seguridad en la red. Se cuenta con dispositivos de seguridad perimetral (firewalls e IPS de red y de host).
- Monitoreo continuo del sistema.
- Administración de registros de usuarios, gestión de privilegios, gestión de contraseñas de usuario.
- Resguardo de sistemas de datos personales con soportes físicos.
- Bitácoras para accesos y operación cotidiana, registro de actividades de la operación cotidiana con un sistema de video vigilancia en las zonas de acceso restringido.
- Perfiles de usuario y contraseñas.- Se tienen políticas para la definición de perfiles de usuario y manejo de contraseñas.

De igual forma, para proteger la información se deben tomar en cuenta los tres principios de la seguridad de la información aplicados a datos personales:



De esta forma, la información se encuentra protegida con los siguientes elementos de seguridad informática:

Solución de seguridad	Propósito
Clúster de Firewalls de Red (esquema de alta disponibilidad)	Realizar un control de las conexiones entrantes y salientes; que permitan sólo aquellos accesos autorizados para la operación.
Clúster de IPS (sistemas detectores/preventores de intrusos)	Sistema de detección y prevención de amenazas de red.
Analizador de vulnerabilidades	Realizar análisis de vulnerabilidades de caja negra y blanca a nivel sistema operativo.
Firewall de aplicaciones web	Protección para las aplicaciones y del contenido de las bases de datos mediante el bloqueo de amenazas conocidas a nivel aplicativo. Incluye un módulo de escaneo de aplicaciones.
Firewall de bases de datos	Escaneo de vulnerabilidades de bases de datos, módulo de monitoreo de actividad en la base de datos, alertas y bitácoras para prácticas forenses. Control de los cambios hechos a las bases de datos; control de cambios.
Correlacionador de eventos	Solución enfocada a la concentración de logs, análisis de los mismos, correlación de eventos

	y monitoreo de eventos en tiempo real. Centraliza eventos de los demás componentes de seguridad para su correlación y alertas de la actividad.
Procedimiento de Control de Cambios	Procedimiento formalizado para la correcta gestión del cambio.

5. Almacenamiento lógico

El núcleo de la información consiste en una tabla denominada "REGISTRO", la cual almacena la información vigente de Verificación de la CURP relacionada a un número telefónico.

Esta tabla contiene únicamente la CURP del titular de la línea telefónica, el número de teléfono celular, un folio de transacción, la fecha de alta y, en su caso, la fecha de baja.

En el cuadro siguiente se detalla la descripción técnica de los campos de la tabla:

CAMPO	TIPO	DESCRIPCIÓN
CURPRAIZPRIMERLETRA	VARCHAR2(4)	4 posiciones iniciales de la CURP
CURPANIONACIM	NUMBER(2)	2 posiciones año de nacimiento CURP
CURPMESNACIM	NUMBER(2)	2 posiciones mes de nacimiento CURP
CURPDIANACIM	NUMBER(2)	2 posiciones día de nacimiento CURP
CURPSEXO	VARCHAR2(1)	1 posición sexo CURP
ENTCLAVE	CHAR2(2)	2 posiciones entidad de nacimiento CURP
CURPRAIZCONSONINTER	VARCHAR2(3)	3 posiciones consonantes internas CURP
CURPCOMPLEM	VARCHAR2(2)	2 posiciones diferenciador homonimia y dígito verificador CURP
REG_NUMERO_MOVIL	VARCHAR2(10)	Teléfono Celular
TRA_ID	NUMBER(10)	Folio de transacción
REG_FOLIO_ALTA	NUMBER(10)	Fecha de alta
REG_FOLIO_BAJA	NUMBER(10)	Fecha de baja

Para el manejo de la información se utilizó ORACLE. Para su correcta administración se utilizaron diversos elementos informáticos como lo son tablas, índices y vistas. La estructura detallada de estos elementos se describe en el Anexo 1.

6. Almacenamiento físico

La información físicamente se encuentra en los servidores que manejan los sistemas relacionados con la administración de la CURP y se localizan en la ciudad de Querétaro. (Anexo 2).

7. Respaldos

El procedimiento de respaldos estipula un formato donde se especifican las rutas que son resguardadas en un robot con tecnología LTO4, con respaldos diarios, semanales, mensuales y anuales, así como la retención que tiene cada una de las políticas configuradas en la herramienta de respaldos SYMPANA.

Políticas de Respaldo

Tipo de Respaldo	Retención
Diario	Mensual
Semanal	Mensual
Mensual	Anual
Anual	5 años

A continuación se muestra un resumen total de respaldos, número de cintas y la vigencia que tiene cada uno de ellos.

Período	Total de Respaldos	Total de Cintas
Diarios	793	753
Semanales	20	20
Mensuales	47	87
Anuales	5	10
TOTAL	861	862

Para los respaldos diarios y semanales que tienen vigencia de un mes, la información que contiene para cada una de las cintas es remplazada cada 60 días, por otros respaldos diarios.

8. Bloqueo y conservación de datos

Cabe señalar que, en tanto no se cancelen los datos personales de las Tablas de Verificación de la CURP, la Secretaría de Gobernación ha implementado una serie de medidas que impiden el tratamiento de los datos.

1. El 18 de abril se bloqueó la información de Verificación de CURP a partir de las 00:00 hrs.
2. El 18 de abril se dieron de baja los servicios de Verificación de CURP relacionada a un número telefónico.
3. El 19 de abril se cancelaron las VPN (Virtual Private Network) que utilizaban los operadores de telefonía.
4. El 25 de abril se eliminaron los usuarios que utilizaban las aplicaciones.
5. El 25 de abril se cancelaron los accesos a las bases de datos.
6. Continúan activos los mecanismos de seguridad y protección de la información.

9. Cancelación de la información

Como ya se ha referido, el pasado 17 de abril de 2012, se publicó en el Diario Oficial de la Federación las reformas a la Ley Federal de Telecomunicaciones por la que se derogó la figura del RENAUT. En razón de lo anterior, es necesario

efectuar la cancelación de los datos de las Tablas de Verificación CURP en poder de la Secretaría de Gobernación.

En consonancia con ello, el 17 de abril de 2012 a las 20:20 horas, la Dirección General del Registro Nacional de Población e Identificación Personal, suspendió el envío y recepción de datos que integraban el RENAUT. Simultáneamente, se notificó a los enlaces de las distintas concesionarias de telefonía móvil, a efecto de que suspendieran el envío de datos.

A partir de las 00:00 del 18 de abril del año que transcurre, se cerró el sistema de recepción de mensajes SMS que enviaban los usuarios para dar de alta su línea telefónica móvil y se dieron de baja las aplicaciones que daban el servicio de validación de la CURP a las compañías telefónicas. Por lo que ya no se recibe ninguna información relacionada con el RENAUT y los sistemas relacionados han sido suspendidos.

Ahora bien, para la cancelación de los datos se han realizado las siguientes acciones:

1. Bloqueo de la información de Verificación de la CURP a partir de las 00:00 hrs. del 18 de abril de 2012.
2. Baja de los servicios de Verificación de la CURP relacionada a un número telefónico.
3. Cancelación de las VPN que utilizaban los operadores de telefonía.
4. Eliminación de los usuarios que utilizaban las aplicaciones.

Acciones por realizar:

1. Eliminación de la información contenida en la Tabla de Verificación de la CURP.
2. Eliminación de las estructuras lógicas.
3. La eliminación del usuario administrador.

4. La eliminación física de los archivos.
5. Destrucción de los respaldos.

Las actividades 1 a 4 se realizarán mediante la ejecución de un script.

Además, se ejecutarán una serie de pruebas a efecto de verificar la cancelación correcta de la información, con lo que se darán por cancelados los datos contenidos en el registro administrativo respecto de la validación de las CURP asociadas a un número telefónico móvil en posesión de la Secretaría de Gobernación.

La destrucción de los respaldos amerita mayor tiempo dadas las implicaciones que tienen que ver con que los cintas no solo contienen información de las verificaciones, sino que también tienen información de la Base de Datos Nacional de la CURP, por lo que se elaborará un plan para la realización de dicha actividad misma que se considera concluir en el lapso de un año. Durante ese periodo, las cintas permanecerán resguardadas en la bóveda contratada por la Dirección General del Registro Nacional de Población e Identificación Personal.

Finalmente, no se omite informar que se constituyó un grupo de trabajo entre el Instituto Federal de Acceso a la Información y Protección de Datos, la Secretaría de Comunicaciones y Transportes y la Secretaría de Gobernación, a efecto de desarrollar el procedimiento de cancelación de los datos personales contenidos en el RENAUT, mismo que al día de hoy continúa con sus trabajos.

V. Anexos

Anexo 1

Almacenamiento lógico

NOMBRE OBJETO	TIPO	DESCRIPCIÓN
ALTAVIACURP	TABLE	Bitácora de las validaciones a través de la CURP
ALTAVIAGENERALES	TABLE	Bitácora de las validaciones a través de nombre y fecha de nacimiento
BAJAVIACURP	TABLE	Bitácora de la información dada de baja a través de la CURP
CAMBIOOPERADOR	TABLE	Bitácora de la información con cambio de operador
CAMBIOVIACURP	TABLE	Bitácora de la información con cambio a través de la CURP
CAMBIOVIAGENERALES	TABLE	Bitácora de la información con cambio a través de nombre y fecha de nacimiento
CONSESIONARIO	TABLE	Catálogo de los concesionarios
CURP_INVALIDAS	TABLE	CURP's no válidas para registro
EXEPTIONS	TABLE	Tabla utilizada para revisar errores de integridad
NOTIFICACIONALTA	TABLE	Tablas de notificaciones Alta y Bajas
NOTIFICACIONBAJA	TABLE	
REGISTRO	TABLE	Tabla de las validaciones con CURP vigentes
REGISTRO_BAJAS	TABLE	Tabla de las validaciones con CURP dados de baja
REGISTRO_CAMBIOS	TABLE	Tabla de las validaciones con CURP con cambios
SERVICIO	TABLE	Catálogo de Tipo de Servicio
SOLICITUDCURP	TABLE	Catálogo de Tipo de Solicitud
TIPOBAJA	TABLE	Catálogo de Tipo Baja del registro
TIPOCAMBIO	TABLE	Catálogo de Tipo cambio del registro
TIPORESPUESTA	TABLE	Catálogo de Tipo Respuesta de la transacción
TRANSACCION	TABLE	Tablas de fecha y hora de la transacción
TRANSACCIONDIFF	TABLE	

TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.308.746328831
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.309.746328857
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.310.746328883
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.311.746328907
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.312.746328933
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.313.746328957
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.330.746329387
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.413.746331489
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.448.746332371
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.449.746332397
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.450.746332421
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.451.746332447
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.452.746332471
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.453.746332497
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.454.746332523
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.460.746332673
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.461.746332699
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.463.746332749
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.464.746332775
TBS_IDX2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx2_renaut.298.746328579
TBS_IDX2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx2_renaut.304.746328731
TBS_IDX2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx2_renaut.307.746328807
TBS_IDX2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx2_renaut.347.746329815
TBS_IDX2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx2_renaut.356.746330041
TBS_IDX2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx2_renaut.455.746332547
TBS_IDX2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx2_renaut.456.746332573
TBS_IDX2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx2_renaut.457.746332597

Anexo 2

Almacenamiento físico

TABLESPACE	DATAFILE
TBS_CATIDX_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_catidx_renaut.515.746333435
TBS_CAT_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_cat_renaut.514.746333435
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.279.757887637
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.280.757888139
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.281.757888493
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.282.757888685
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.283.757888877
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.284.757889113
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.285.757889291
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.286.757889517
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.287.757889689
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.288.757889895
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.289.757890121
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.290.757890393
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.291.757890545
TBS_DAT1_RENAUT	+DGDATAT0_CURP/dbcurp/datafile/tbs_dat1_renaut.292.757890655
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.262.746327501
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.265.746327637
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.266.746327683
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.267.746327727
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.269.746327819
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.272.746327923
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.273.746327949
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.274.746327975
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.303.746328705
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.444.746332271
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.445.746332295
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.446.746332321
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.447.746332345
TBS_DAT2_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_dat2_renaut.538.748224745
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.297.746328555
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.299.746328605
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.300.746328631
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.305.746328757
TBS_IDX1_RENAUT	+DGDATAT1_DBCURP/dbcurp/datafile/tbs_idx1_renaut.306.746328781