Servicio de Normalización y Detección de Anomalías.

Descripción General

Autor:	*Desarrollo de Negocio y Gestión de Servicios*
Título del documento:	*Servicio de Normalización y Detección de Anomalías. Descripción General*
Número de páginas	*26(portada incluida)*
Código:	*340_SDA_PLA_DOC*
Versión:	*02*
Fecha de última modificación:	*9 de octubre de 2007*
Distribución:	*Externa*
	Compruebe que esta es la última versión del documento
Contactar en :	*www.tirea.es / E-mail: sau@tirea.es / Tel: 902 132 142*

1. Índice

2. Introducción

El servicio SENDA (Servicio de Normalización y detección de Anomalías) descrito en este documento, tiene como objetivo detectar anomalías e incongruencias de información en los nuevos movimientos de pólizas y siniestros de cada entidad, mediante la aplicación de reglas de negocio sobre datos históricos de la propia entidad.

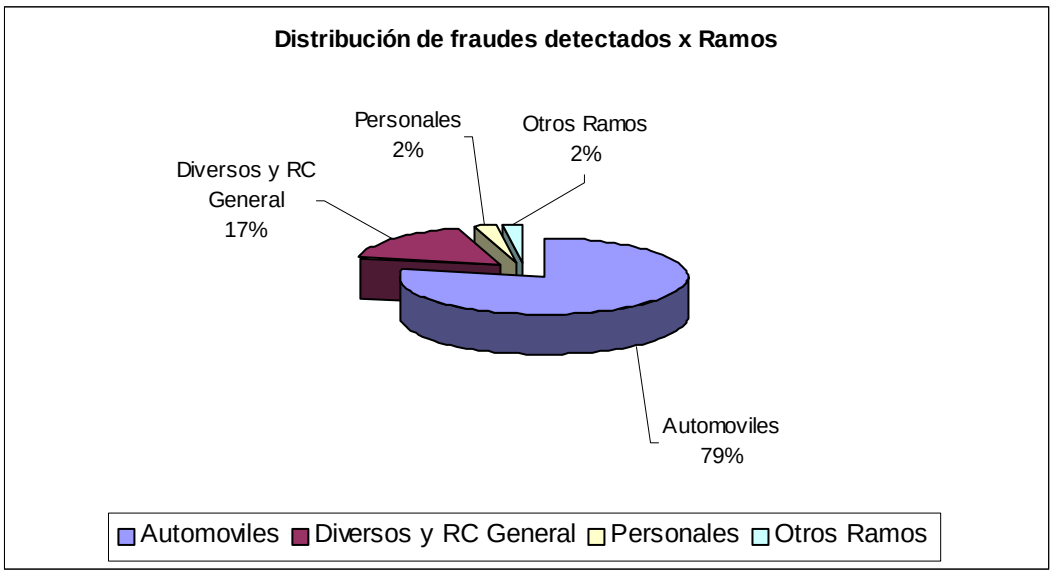
El presente documento se estructura en los siguientes capítulos:

- Antecedentes
- Objetivos del servicio
- Descripción General
- Funcionalidades
- Actividades según fases del servicio
- Nivel de Servicio
- Seguridad

3. Antecedentes

Según fuentes del sector, las entidades aseguradoras soportan, en su conjunto, un impacto en su cuenta de resultados de más de 600 millones de euros al año por IE_LCS.

El ramo en el que se producen más situaciones anómalas y fraudulentas es en el de Automóviles:



Las causas de fraude más comunes en el ramo de automóviles son las siguientes:

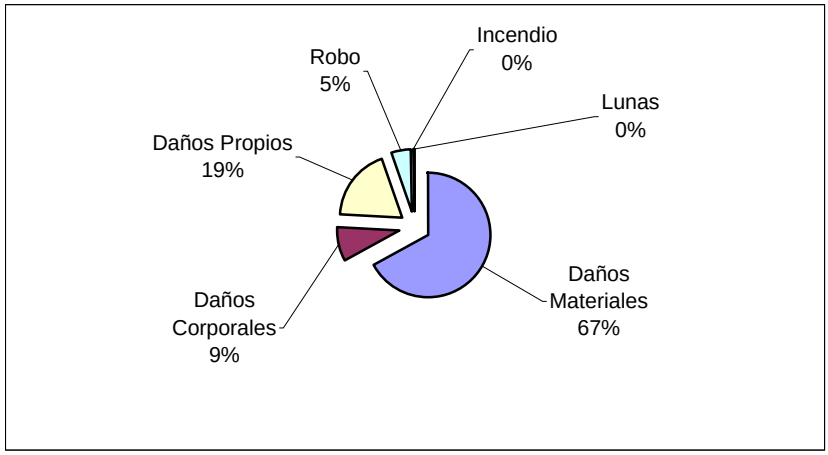
Fraude de solicitud

- Omisión de partes anteriores.
- Edad del conductor principal diferente a la declarada.
- Uso no adecuado del vehículo (por ejemplo para negocios)
- No mencionar a otros conductores.
- Fronting: Padres que aseguran el vehículo siendo el conductor principal un adolescente.
- Intentos de modificación del tipo de cobertura tras un accidente.
- Fraude de identidad.

Fraude en siniestros

- Reclamación relacionada a un accidente anterior a la contratación de la póliza.
- Reclamación por robo de vehículo cuando este no se ha producido.

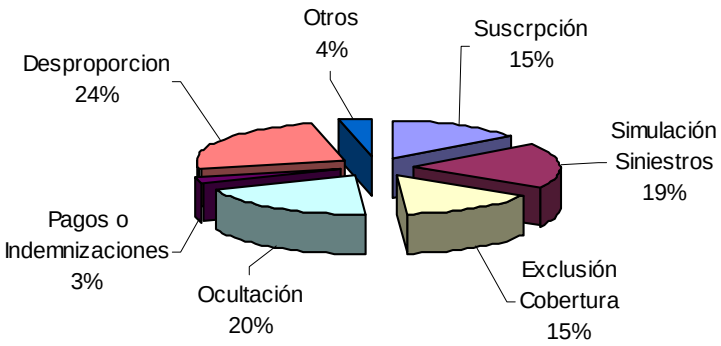
- Reclamación por daños y perjuicios superiores a los reales.
- Relación familiar entre los reclamantes.
- Daños materiales importantes sin daños personales.
- Accidente con un vecino ocurrido lejos del domicilio.
- Daño material poco importante con daño personal alto.
- Conductor y pasajero se intercambian después del accidente.
- Motocicletas – Posibilidad de competiciones.
- Alcohol.
- Partes en más de una póliza.
- Relación entre reclamante y empleado en la compañía de seguro.
- Costes excesivos en el parte.
- Largo período de baja médica sin ninguna lesión seria.
- Relación entre el reclamante y personal del taller de reparación del automóvil.
- Colusión : Relación entre reclamante y personal de la Entidad.
- Fallo de control de la Entidad y obtención de beneficio del mismo.



En los últimos años, las entidades han incluido elementos de control en sus procedimientos operativos que permiten un mejor análisis y detección de las anomalías o inconsistencias que pueden ser consideradas fraude. A continuación se citan algunos:

- Creación de Departamentos de Verificación Técnica de Siniestros.
- Establecimiento de catálogos de circunstancias sospechosas.
- Definición de normas y procesos operativos.
- Instauración de programas de seguimiento informático que permiten conocer la evolución de los siniestros.
- Mentalización en el seno de las entidades.
- Colaboración entre las entidades.
- Mayor utilización de peritos e investigadores.

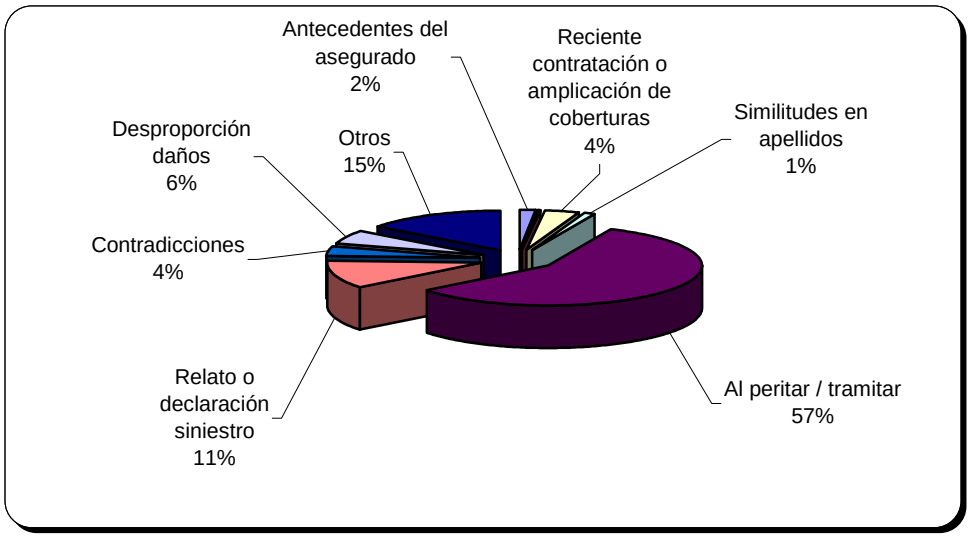
Tipología de Fraude Detectado



En la fase de detección de fraude, la utilización de herramientas basadas en ficheros históricos de datos y reglas lógicas de análisis, se posiciona en segundo lugar en cuanto a eficiencia y resultados, de tal forma que los indicios de actos fraudulentos pueden ser contrastados con eficacia mediante la utilización de herramientas de tratamiento de datos, como son:

- Antecedentes de asegurados
- Análisis de fechas
- Similitudes de apellidos, cercanía de domicilios, relación de parentesco...
- Fronting
- Inconsistencia de datos...
- Comparación de datos aportados por otras entidades.
- Prácticas anómalas.
- ...

Indicios que permiten la detección de fraude:



TIPOLOGIA DE LAS AMENAZAS:

En términos de fraude, algunas de las amenazas que acechan a las compañías aseguradoras en forma de delito económico se pueden agrupar en las siguientes categorías:

- **Robo o fabricación de identidad:** Utilizar la identidad de otra persona real para cometer un delito.
- **Colusión:** Una persona actúa conjuntamente con un empleado de la entidad para cometer un delito
- **Fraude oportunista:** Una persona percibe un fallo en los controles de la entidad y decide aprovecharse del mismo para obtener un beneficio deshonesto.
- **Ataques sincronizados:** Es el siguiente paso del defraudador oportunista. Consiste en actuar junto a otras personas para obtener el mayor beneficio en el menor tiempo posible.
- **Redes organizadas:** Organización cuya misión es cometer fraude de forma sistemática, estructurada y planificada.

4. Objetivos y Requerimientos

El objetivo general es contar con **un Servicio** para la detección y prevención del fraude mediante la utilización de una **plataforma tecnológica** de apoyo que permita:

- Normalización de información.
- Detección de anomalías, inconsistencias y errores en los datos aportados.
- Establecer alertas de presuntos casos de fraude a analizar por parte de la entidad.
- Generación de Estadísticas.

Los objetivos específicos son los siguientes:

- Solución común para todas las Entidades y el futuro modelo sectorial.
- Servicio modular que permita a cada entidad trabajar en el escenario que requiera.

El servicio debe cubrir los siguientes requerimientos:

- Debe contemplar un enfoque multirramo, si bien, en una primera fase se centrará única y exclusivamente en el ramo de automóvil.
- Debe permitir la posibilidad de configurar la información que aporten las entidades en base a su disponibilidad.
- Debe admitir múltiples figuras relacionadas con las pólizas y siniestros que serán configurables dependiendo del caso.
- Las reglas a aplicar para establecer las alertas serán configurables.
- Debe proporcionar herramientas que permitan el análisis e investigación de las reglas detectadas permitiendo añadir la información adicional a la investigación que se necesite.

5. Descripción general del Servicio.

El servicio persigue la detección de anomalías en los procesos de suscripción, declaración y tramitación de siniestros, al comparar la información enviada diariamente por la Entidad, con los datos históricos de pólizas y siniestros de la propia Entidad, cargados previamente, mediante la aplicación de una serie de reglas de negocio.

El histórico con el que se comparan los nuevos movimientos está formado únicamente con la información de la propia entidad (modelo fichero entidad) Inicialmente el histórico estará compuesto por pólizas vigentes en el momento de la carga (última situación) con todos sus siniestros de los últimos tres años.

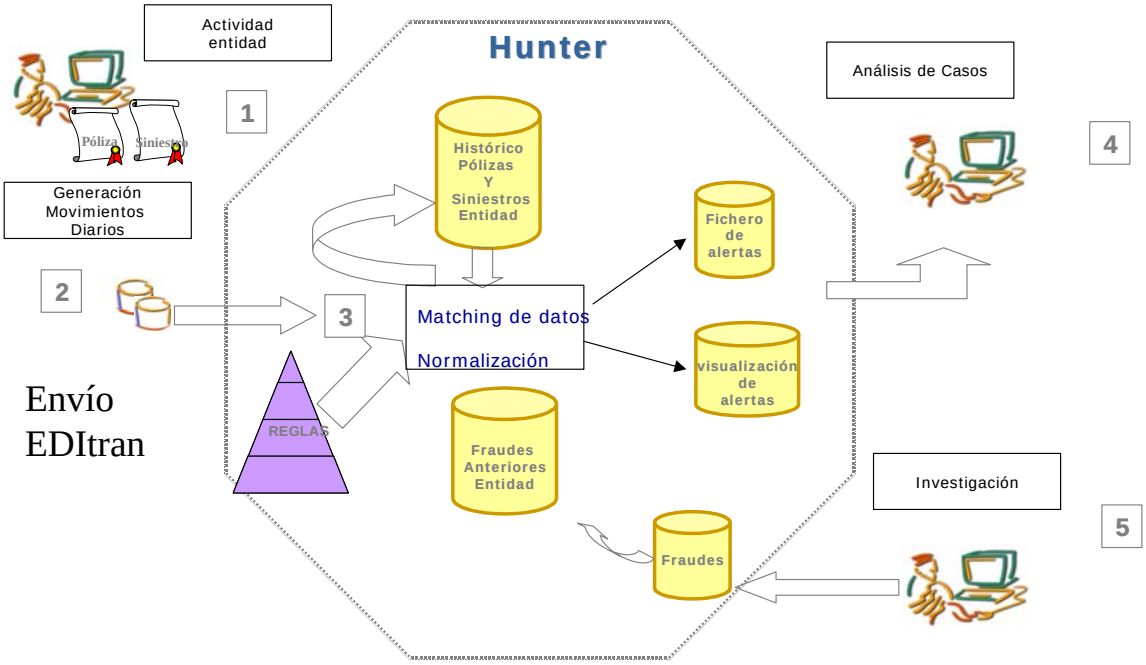
Periódicamente, esta base de datos se actualiza, tanto incluyendo los movimientos diarios de pólizas (nueva producción), solicitudes, suplementos y siniestros, como eliminado la información obsoleta. Cada modificación de una póliza o un siniestro se considera como una nueva versión de la póliza o el siniestro.

Antes de ejecutar los proceso de carga y de cruce de datos se realiza una depuración de la información mediante un proceso de normalización de datos (direcciones y nombres) y de devolución de registros erróneos.

Los procesos de comparación pueden ser tanto en el momento de la captura de datos por parte de la entidad (on-line), como al final del día (batch) Los datos obtenidos de forma on-line, estarán basados en reglas básicas para así agilizar el tiempo de respuesta de los mismos.

Las anomalías detectadas como consecuencia del contraste diario con el histórico serán investigadas por parte de cada entidad para analizar si hay indicios de fraude.

El siguiente diagrama muestra el esquema general del servicio propuesto:



Diariamente la Entidad genera los movimientos relativos a pólizas y siniestros que deberán ser incluidos en el servicio. El envío diario se realiza mediante la plataforma EDItran.

Una vez recibidos en TIREA los ficheros con los movimientos diarios, estos son normalizados y validados de acuerdo con las normas establecidas, generándose un fichero de respuesta para la Entidad que incluye, en su caso, los registros rechazados con su correspondiente código de error. Este fichero debe ser analizado y depurado por la Entidad. Cuando los errores hayan sido corregidos, los registros podrán ser finalmente integrados en la base de datos de SENDA.

Sobre estos movimientos ya normalizados y validados, se realiza el cruce de datos con el histórico, aplicando las reglas de negocio establecidas y se generan en la base de datos las correspondientes alertas que podrán ser visualizadas por la Entidad vía web.

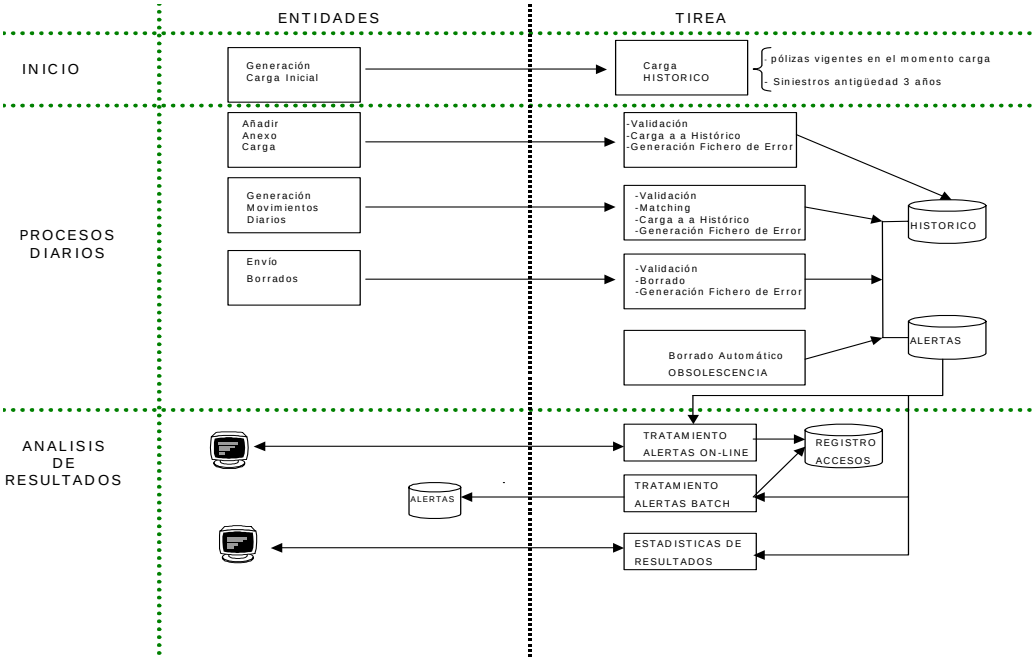
Del resultado de la investigación por parte de la Entidad, pueden surgir nuevos registros a incluir dentro del fichero de referencia. En este caso, los envíos se realizan mediante EDItran, de la misma manera que los envíos diarios, y son incluidos en dicho fichero.

La cronología de procesos entre la Entidad y TIREA es la siguiente:

PERIODICIDAD	PROCESOS DE LA ENTIDAD	PROCESOS DE TIREA
Adhesión al servicio	Carga inicial	• Validación del fichero • Normalización • Fichero de respuesta (con errores si procede) • Integración en la base de datos histórica
Diariamente (al final del día)	Actualizaciones (incluye reciclado de errores y petición de borrados)	• Validación del fichero • Normalización • Fichero de respuesta (con errores si procede) • Cruce de datos con el histórico • Generación de alertas (batch) • Integración de los movimientos en la base de datos histórica • Borrado de los movimientos solicitados manteniendo la coherencia.
Diariamente (al final del día)	Anexo carga inicial (incluye reciclado de errores, tanto de carga inicial como de anexo de carga inicial)	• Validación del fichero • Normalización • Fichero de respuesta (con errores si procede) • Integración en la base de datos histórica
Diariamente (proceso nocturno)	---	• Borrado por obsolescencia

Diariamente	Consulta on-line	• Validación del fichero y mensaje de respuesta • Normalización • Cruce de datos con el histórico • Generación de alertas (on-line) • Registro de acceso
Diariamente	Análisis de alertas (online)	• Registro de acceso
Diariamente	Análisis de alertas (batch) tras la integración en sistema de información de la Entidad	• Registro de acceso
A petición	---	• Generación de informes y estadísticas
A petición	---	• Utilidades de administración

El esquema de los procesos diarios, sigue el siguiente esquema:



6. Módulos funcionales

Los módulos funcionales de los que consta el servicio son los siguientes:

- MODELIZACIÓN
- NORMALIZACIÓN
- MANTENIMIENTO HISTÓRICO
- ENFRENTAMIENTO DE NUEVA PRODUCCIÓN CON EL HISTORICO
- TRATAMIENTO DE ALERTAS
- EXPLOTACIÓN DE RESULTADOS

A continuación se describe cada uno de estos módulos:

Modelización

El servicio debe ser flexible, generalizado y adaptable a los requerimientos de las Entidades que se adhieran. Para ello existe un diccionario de datos común que permite el envío de datos unificados para las entidades. Partiendo de esta base común, cada entidad podrá tener su modelo de datos específico, pero siempre como un subconjunto del modelo común.

Configuración estructuras de Datos:

Se definen las estructuras de datos en el servicio, indicando los campos que se van a utilizar.

Existe una estructura general que se particulariza para cada entidad.

Configuración Reglas de Negocio:

Utilizando los datos definidos en la estructura de datos se configuran las reglas de negocio a aplicar sobre el histórico ya almacenado. Hay reglas básicas (sub-reglas) que se combinan para formar reglas más complejas.

Existen **Reglas Comunes** para todas las entidades y **Reglas Específicas** de cada entidad, según sus propias necesidades.

A cada regla se le asigna una puntuación. Esa puntuación, que cada entidad asigna según su propio criterio, es la que permite a la entidad priorizar las reglas a aplicar y las alertas a analizar posteriormente.

Algunos ejemplos de reglas a aplicar en el servicio, son las siguientes:

- Mismo DNI, diferente nombre
- Mismo Nombre, diferente DNI
- Misma cuenta bancaria, diferente domicilio
- Mismo titular de póliza y cancelaciones sospechosas anteriores
- Múltiples pólizas canceladas con la misma matrícula
- Mismo reclamante, diferentes pólizas, múltiples siniestros
- Diferentes siniestros con las figuras del contrario y del reclamante intercambiadas
- etc...

Normalización

Toda la información recibida por las entidades, ya sea para cargar el histórico o los datos a validar en los envíos diarios, son normalizados antes de ser procesados.

Se normalizan los datos correspondientes a identidades de personas físicas, nombres, apellidos, datos de localización y domicilios.

Mantenimiento histórico

Los procesos asociados a la carga y mantenimiento de los datos históricos son los siguientes:

- **Carga inicial:** Esta primera carga de la cartera de cada Entidad contendrá las pólizas vigentes en ese momento junto con todos sus siniestros de los últimos tres años.
- **Actualizaciones periódicas:** envío diario vía EDItran de todos los movimientos de nueva producción, suplementos y siniestros generados desde el último envío junto con el reciclado de errores. Además podrán enviarse también peticiones de borrado de los registros solicitados de forma específica por la entidad.
- **Anexo de carga inicial:** Cuando la entidad lo requiera, podrá enviar un fichero con todos aquellos registros nuevos que quiera incorporar al histórico sin tener que cruzar con el histórico anterior.
- **Borrado datos antiguos:** Mediante este proceso diario se realizará el borrado de datos obsoletos de acuerdo con las reglas de borrado establecidas.

6.1.1. Carga inicial

El envío de cartera se realiza cuando una Entidad Aseguradora se adhiere al Servicio **Senda.** Antes de iniciar su operatividad en el servicio, la entidad debe enviar la cartera con las pólizas vivas en ese momento (última situación) así como los siniestros asociados a las mismas, siempre y cuando tengan una antigüedad (fecha de ocurrencia) menor o igual a 3 años, con independencia de que se encuentren abiertos o cerrados. Debido a la magnitud de los datos, este envío se podrá realizar mediante soporte magnético.

Para la carga inicial la Entidad debe enviar los siguientes **ficheros**:

- **Fichero histórico de pólizas:** información relativa a la última situación de todas las pólizas que estén en vigor en el momento de generar el fichero

- **Fichero histórico de siniestros:** información relativa a todos los siniestros de las pólizas en vigor, siempre y cuando la fecha de ocurrencia del siniestro tenga una antigüedad menor o igual a 3 años, con independencia de que estos se encuentren abiertos o cerrados.

- **Fichero de referencia:** Fichero adicional que podrá enviar la Entidad para incluirlo en el contraste diario si lo desea y que contiene información relativa a personas, físicas o jurídicas, tales como usuarios, empleados, clientes, listas negras, marcas, etc. De esta forma, los ficheros que se envían a diario para cruzar con el histórico se podrán cruzar también contra este fichero, mediante la aplicación de las reglas de negocio establecida.

6.1.2. Actualizaciones periódicas

Mediante este proceso diario, cada Entidad Aseguradora envía una serie de ficheros de movimientos que actualizan la información de la base de datos histórica. Su objetivo es doble: en primer lugar conseguir que la información del Servicio refleje en todo momento la situación más exacta y actualizada posible y, en segundo lugar, realizar el chequeo de estos mismos datos contra el histórico, mediante la aplicación de las reglas de negocio establecidas.

Para las actualizaciones periódicas la Entidad debe enviar los siguientes **ficheros**:

- **Fichero de actualizaciones de pólizas:** Fichero con todos movimientos de cartera generados desde el último envío (pólizas nuevas, suplementos, cancelaciones...) También se incluirán en este fichero los registros correspondientes al reciclado de errores (registros rechazados en procesos anteriores de actualización y ya corregidos por la Entidad)

- **Fichero de solicitudes:** Si la Entidad lo desea, también podrá enviar un fichero de solicitudes. El tratamiento de este fichero será idéntico al del fichero de pólizas. Por ello ambos ficheros tendrán la misma estructura, cambiando en este el campo número de póliza por número de solicitud. Si se envían modificaciones de solicitudes ya enviadas con anterioridad, estas se integrarán como una nueva versión.

  También se incluirán en este fichero los registros correspondientes al reciclado de errores (registros rechazados en procesos anteriores y ya corregidos por la Entidad)

- **Fichero de actualizaciones de siniestros:** Fichero con todos movimientos de siniestros generados desde el último envío (aperturas, modificaciones, rehabilitaciones y cierres) Si se envían modificaciones de siniestros ya enviados con anterioridad, estas se integrarán como una nueva versión.

  También se incluirán en este fichero los registros correspondientes al reciclado de errores (registros rechazados en procesos anteriores de actualización y ya corregidos por la Entidad)

- **Fichero de actualizaciones del fichero de referencia:** Fichero con todos aquellos movimientos relativos a modificaciones del fichero de referencia y que la Entidad quiera mantener actualizados. También se incluirán en este fichero los registros correspondientes al reciclado de errores (registros rechazados en procesos anteriores y ya corregidos)

6.1.3. Anexo de carga inicial

Cuando la entidad lo requiera, podrá enviar un fichero con todos aquellos registros nuevos que quiera incorporar al histórico pero no quiera cruzar contra la base de datos (sin aplicar reglas de negocio) Este tipo de envío puede hacerse, incluso, a diario.

Estos ficheros incluirán el reciclado de errores (registros rechazados en procesos anteriores y ya corregidos por la Entidad) tanto si estos se produjeron en el proceso de carga inicial, como en la carga de ficheros de anexo anteriores

Para este proceso la Entidad podrá enviar tres tipos de ficheros:

- Fichero de pólizas
- Fichero de siniestros
- Fichero de referencia

Estos ficheros tendrán la misma estructura que sus equivalentes utilizados para la carga inicial del histórico de pólizas.

6.1.4. Borrado de datos anteriores

Siempre que la entidad lo requiera, podrá enviar en los ficheros diarios todos aquellos documentos (pólizas, solicitudes y/o siniestros) que quiera eliminar de la base de datos del Servicio. Las peticiones de borrado vendrán en el mismo fichero que los movimientos diarios enviados para integración y cruce de datos. Uno de los campos del fichero indicará que debe hacerse con cada registro (borrarlo, integrarlo en el histórico sin contrastar o contrastarlo e integrarlo)

Cuando se solicite algún tipo de borrado se mantendrá la coherencia de la información histórica. Por ello se seguirán los siguientes **criterios de eliminación de registros:**

- Siempre que se solicite el borrado de una póliza, se borrarán también todos sus suplementos y siniestros, con todas sus versiones, aunque la entidad no haya solicitado dichos borrados.
- Cuando se solicite el borrado de un documento de cualquier otro fichero este se borrará con todas sus versiones.

Además, dado que se mantiene un histórico de 3 años, diariamente se borrarán todas las pólizas que lleven mas de 3 años anuladas. Para mantener la coherencia se borran con todos sus siniestros y suplementos y en todas sus versiones. Igualmente se borrarán todos los siniestros que tengan mas de 3 años desde su fecha de ocurrencia (todas sus versiones) Las solicitudes se borrarán a los 3 meses, contando desde su fecha de solicitud.

Enfrentamiento de datos de nueva producción

Este proceso consiste en la aplicación de las reglas de negocio, definidas para cada Entidad, sobre los datos de movimientos diarios de producción, siniestros y suplementos.

Existen dos formas diferentes de validación:

6.1.1. Enfrentamiento on-line

La Entidad podrá incorporar en su sistema, si lo desea, la posibilidad de hacer un cruce on-line contra la base de datos histórica del servicio SENDA. De esta forma, cuando la entidad este mecanizando cualquier operación de alta de póliza, suplemento o siniestro (apertura, modificación, rehabilitación o cierre) antes de finalizar dicha operación, puede enviar al Servicio SENDA de forma on-line, el registro con los datos de la misma, para realizar el proceso de aplicación de reglas de negocio en ese momento, recibiendo respuesta inmediata por parte del Servicio.

Las reglas de negocio aplicadas en este caso serán solo las reglas simples, por lo que solo se obtendrán dos tipos de respuestas:

- Válido: no se ha generado ninguna alerta
- A estudiar: se ha generado alguna alerta

Los movimientos que se hayan incorporado en el cruce de forma on-line se deben reenviar al final del día, en el fichero correspondiente, para realizar el tratamiento de forma batch, aplicándose esta vez, todas las reglas de negocio (no solo las reglas simples) y almacenarlos en el histórico.

6.1.2. Enfrentamiento Batch

Diariamente la entidad envía todas los movimientos que necesiten ser validados aplicando las reglas de negocio establecidas. Es la entidad quién decide qué movimientos deben validarse. Con carácter general son:

- Nueva producción de pólizas.
- Rehabilitaciones, modificaciones.
- Nuevas solicitudes.
- Suplementos de pólizas
- Nuevos siniestros.
- Variaciones en siniestros (Pagos, reservas, cambios de posición...)

Como mínimo, la Entidad debe enviar la nueva producción de pólizas y los nuevos siniestros.

Todos los movimientos recibidos en el día se procesan en batch aplicando las reglas de negocio definidas contra la información contenida en el histórico.

Este proceso marca todos aquellos movimientos para el que se haya cumplido una o varias reglas de negocio. A cada movimiento se le suma la puntación de todas las reglas de negocio que haya cumplido.

Tratamientos de Alertas

Las anomalías detectadas son investigadas por cada Entidad para, en su caso, determinar si hay algún indicio de anomalías.

Todas las alertas generadas para una entidad pueden ser tratadas por dos vías:

6.1.1. Tratamiento On-line

En cualquier momento, los usuarios de la Entidad que hayan sido autorizados, podrán conectarse directamente a la base de datos SENDA, centralizada en TIREA, para realizar, de forma on-line, el análisis y tratamiento de todas las alertas generadas hasta la ejecución del último proceso de cruce de tatos con el histórico.

Las alertas se distribuirán entre los usuarios repartiéndolas entre distintas listas de trabajo para su análisis por parte de los usuarios gestores.

Esta interfase permite visualizar todas las alertas disponibles así como las reglas que las han generado, y se presentarán calificadas con su correspondiente puntuación (score) Se puede acceder a cualquier elemento de la lista, directamente o a través de un buscador. Para cada movimiento, se pueden visualizar los datos del mismo, comparándolos con el movimiento de histórico con el que se ha cruzado, provocando la alerta. Además, permite investigar en el resto de movimientos del histórico para localizar elementos comunes con otros casos (anillos de fraude)

En cada movimiento el usuario puede añadir notas adicionales de su investigación y calificar el caso, separando los falsos positivos de los casos a investigar.

6.1.2. Tratamiento Batch

Para la entidad que lo requiera, se pueden generar ficheros que recibirá diariamente vía EDItran con los datos de las alertas generadas en el servicio, de forma que la Entidad pueda explotar esa información con sus propios sistemas.

Estadísticas sobre resultados.

El servicio permite realizar diversos tipos de estadísticas, tanto relativas a los resultados obtenidos en el enfrentamiento de datos (alertas) como a los diversos procesos utilizados para su explotación (resultados de gestión) y que permiten valorar el ahorro producido en la detección de anomalías.

Esta captura de datos estadísticos por parte de la Entidad puede ser on-line o batch y los resultados pueden obtenerse diariamente o acumulados.

Algunos ejemplos de estas estadísticas son:

- Generación de informes, por generación de alertas y fecha de coincidencia de esas alertas, donde se muestran las reglas que han saltado para una aplicación determinada, para un periodo de tiempo determinado (el tiempo se puede seleccionar)

- Generación de estadísticas sobre alarmas trabajadas, pendientes, no trabajadas o bajo indicio, para un periodo de tiempo determinado. El periodo de tiempo analizado puede especificarse para cada informe

- Generación de estadísticas por grupo de aplicaciones: se pueden elaborar estadísticas e informes sobre que grupo de aplicaciones han sido calificadas de fraudulentos, libre, o sospechosos. Esta estadística se basa en reglas y tiempo determinado que puede ser especificado para cada caso.

- Se pueden generar informes relativos al tiempo dedicado por un usuario al análisis de una alerta o el empleado que ha trabajado en una alarma. El periodo de tiempo analizado puede especificarse para cada informe

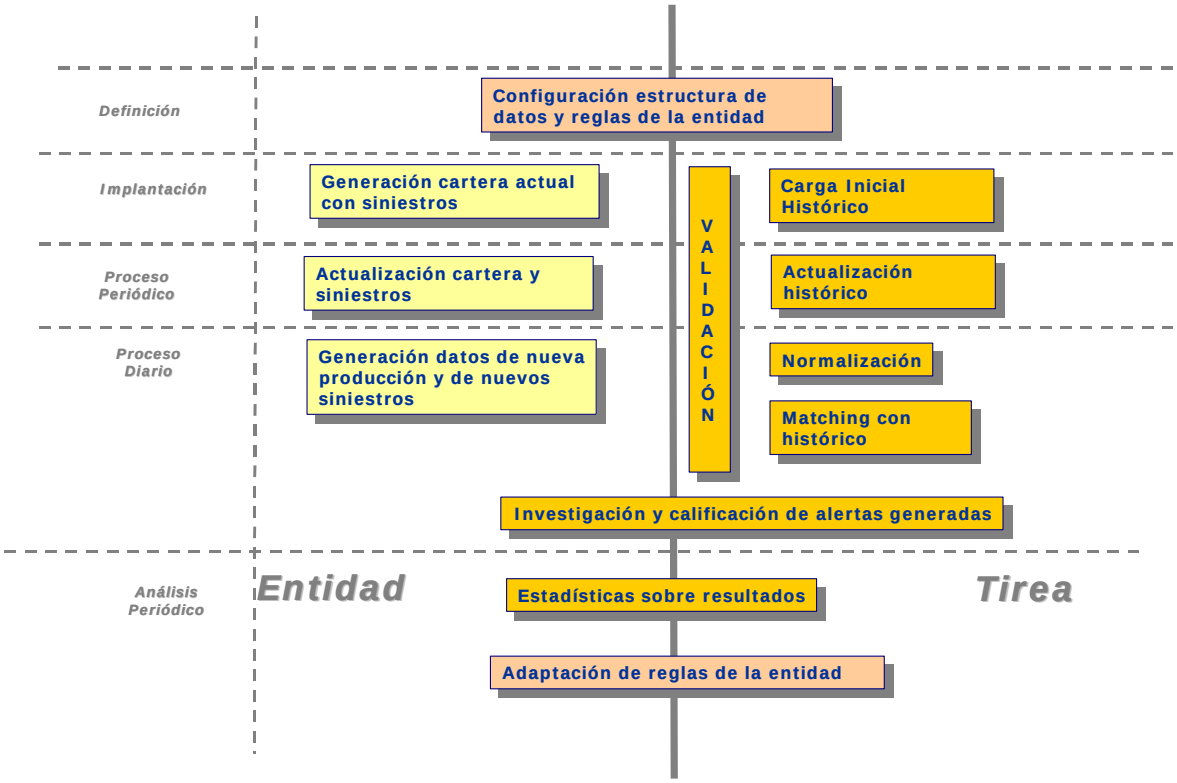
- Generación de informes sobre reglas más utilizadas y reglas analizadas por usuario, en un intervalo tiempo determinado.

- Generación de informe donde se especifican las coincidencias y las no coincidencias en un mismo lote enviado a la herramienta.

Analizando los resultados de alguna de estas estadísticas podrán modificarse o suprimirse las reglas menos efectivas o introducirse nuevas reglas.

7. Actividades según fases del Servicio

A continuación se muestra el flujo de trabajo entre la Entidad y TIREA en las diferentes fases por las que se va pasando en el ciclo de vida del servicio:



Definición: Antes de la implantación del servicio se contacta con la entidad para estudiar sus requerimientos y definir el modelo de datos a utilizar, las reglas de negocio a aplicar y la prioridad sobre las mismas.

Implantación: En la fase de implantación del servicio la entidad debe enviar las pólizas vigentes en ese momento con el historial de los siniestros de todas las garantías ocurridos en los últimos 3 años. Existe un proceso de validación previa sobre la cartera que devolverá a la entidad los registros erróneos, pudiendo ésta corregirlos y realizar un nuevo envío.

Proceso diario: Diariamente la entidad enviará todos los movimientos que haya habido sobre pólizas y siniestros desde el último envío, para realizar el enfrentamiento contra el histórico. Previamente los movimientos enviados serán normalizados y validados, devolviendo a la entidad los erróneos para que sean corregidos.

En este envío diario se podrá definir que datos deberán ser macheados y cuales no, separándolos en ficheros diferentes.

Una vez realizado el proceso, la entidad puede investigar las alertas generadas calificándolas para determinar si son falsos positivos, anomalías de información o presentan indicios de fraude.

Análisis periódico: Periódicamente en TIREA, en la entidad o en ambas se realiza un seguimiento de los resultados que permite ir ajustando y configurando las reglas de negocio que se aplican.

8. Nivel de Servicio

Operación

La operación del Servicio **SENDA** es de 24 horas al día, 7 días a la semana todos los días del año, incluyendo la supervisión de las comunicaciones, las aplicaciones y los procesos de los servicios y la ejecución de los procedimientos de operación de las infraestructuras (back-up/recuperación, arranque/parada, depuración de almacenamiento, etc.)

Disponibilidad de servicio

- TIREA garantiza una disponibilidad mensual del Servicio superior al 99%.
- TIREA se reserva el derecho a hacer una parada planificada al mes de un máximo de 8 h de duración en horario de fin de semana. Esta parada no está incluida en la disponibilidad anteriormente garantizada.
- En esta disponibilidad no se incluye tampoco:
  - Las líneas de comunicaciones con Entidades, Infovía o Ibernet.
  - El servicio de la red Ibernet de Telefónica Transmisión de Datos.
  - El servicio InfoVía.

TIREA informará por correo electrónico a los administradores que las Entidades designen, tanto de las incidencias ocurridas como de las paradas planificadas.

9. Seguridad

Para conseguir el nivel óptimo de seguridad del Servicio SENDA, se han definido los siguientes mecanismos:

1. **Procedimientos organizativos de control y seguridad**: Las Entidades que utilicen el Servicio deben suscribir el Protocolo y el Código de Utilización, asumiendo los procedimientos de control definidos y facilitando su aplicación con todos los medios puestos a su alcance.

2. **Gestión integral** de la seguridad, siguiendo las políticas generales definidas para todos los Servicios de TIREA.

3. **Estricto cumplimiento de la LOPD,** en cuanto a: Confidencialidad de los datos, Registro de Incidencias, Gestión de Soportes y Bloqueo de datos.