Universidad de las Ciencias Informáticas

Facultad 2

Trabajo de diploma para optar por el título de Ingeniero en Ciencias Informáticas.

Título:

Propuesta de Modelo de Datos basado en la suite de estándares Frameworx para la Gestión de Fraude en las telecomunicaciones.

Autor: Dany Mendibur Crespo.

Tutores: Ing. Martha Mesa Silva, Ing. Norbelis Leyva Montero.

Co-tutor: Msc. Jorge Luis Olmedo Flores.

Ciudad de La Habana, Junio 2013.

Pensamiento

"… No culpes a nadie, nunca te quejes de nada ni de nadie porque fundamentalmente tú has hecho tu vida. Acepta la responsabilidad de edificarte a ti mismo y el valor de acusarte en el fracaso para volver a empezar, corrigiéndote. El triunfo del verdadero hombre surge de las cenizas del error.

No olvides que la causa de tu presente es tu pasado, como la causa de tu futuro es tu presente. Aprende de los fuertes, de los activos, de los audaces, imita a los valientes, a los energéticos, a los vencedores, a quienes no aceptan situaciones imposibles, a quienes no les atrae las cosas fáciles y a cambio aceptan el reto de lo exigente pero realizable; a quienes vencieron a pesar de todo…"

Pablo Neruda.

DECLARACIÓN DE AUTORÍA

Declaro que soy el único autor de este trabajo y autorizo a la Facultad 2 de la Universidad de las Ciencias Informáticas hacer uso del mismo en su beneficio.

Para que así conste firmo la presente a los ____ días del mes de _____ del año _____.

Autor: Dany Mendibur Crespo. _____ .

Tutores: Ing. Martha Mesa Silva. _____ . Ing. Norbelis Leyva Montero. _____ .

Co-tutor: Msc. Jorge Luis Olmedo Flores. _____ .

DATOS DE CONTACTO

Tutores: Ing. Martha Mesa Silva[1] & Ing. Norbelis Leyva Montero[2]

Síntesis de los Tutores:

[1] mmsilva@uci.cu

Ing. Ciencias Informáticas, graduada en la Universidad de Ciencias Informáticas en el año 2009. Trabaja en la Facultad 2 de dicho centro de enseñanza superior con categoría docente de Instructor. Pertenece al Centro de Telemática, específicamente al proyecto Sistema Integral de Análisis de Información con el rol de analista principal.

[2] norbelis.leyva@etecsa.cu

Ing. Ciencias Informáticas, graduada en la Universidad de Ciencias Informáticas en el año 2008. Trabajó por 4 años en la Facultad 2 de dicho centro de enseñanza suprior con categoría docente de Instructor, donde se desempeñaba específicamente en el proyecto Sistema Integral de Análisis de Información con el rol de asesora de calidad. Actualmente trabaja en ETECSA desempeñándose con el rol de Especialista en Telemática.

AGRADECIMIENTOS

A mis padres y mi hermana: Por su sacrificio, por creer en mí, por ser la fuerza, el motivo fundamental que me alienta a superarme, a ser cada vez mejor. Por ser siempre mi luz al final del camino.

A mis abuelos: Por sus atenciones, por transmitirme su sabiduría y conocimiento de la vida.

Agradezco a mis tíos Ania, Kaki, Humberto y Elsa, gracias por ser parte de mi familia, por su ayuda incondicional, por siempre estar presentes compartiendo mis alegrías y tristezas. Sin ustedes este momento no hubiera sido posible.

A Reidys y al Kima mis amigos en las buenas y en las malas, mis hermanos.

A mis tutoras Marthica y Norbelis por dedicar su tiempo, conocimiento y empeño en la realización de esta tesis, al igual que Lili, Husse, Sandy, Olmedo, Yaily, Erik, Alberto, el Denis, Jova, Pack, Pedro, el Chami, Rogelio, todos mis compañeros del SIAI. Sobre todo, ¡Gracias por ser mis amigos!, por formar parte de esta gran familia y aula que es SIAI.

A mi tías Norma, Anabel, a mi prima Blanquita, a Adrián, el Filio, Tan, Deylert, Karim, Tatica, Willi, Jorgito, a la Jima, Angelita, Orlando, Carlos, Tomas Alexis, a mis compañeros de aula y profesores en estos 5 años, a todo aquel que a lo largo de mi carrera ha influido en mi formación.

Gracias a la vida por darme la posibilidad de conocer a estas personas, por permitirme estar hoy aquí, expresando mi agradecimiento, admiración y compartiendo este resultado con ustedes que han hecho posible este momento.

DEDICATORIA

Dedico este trabajo a mis padres y mi hermana. Ustedes son los principales autores de este trabajo, los responsables de mis resultados. Ustedes que han sabido darme el amor, educación, apoyo y principios necesarios para convertirme en un hombre de bien. Para ustedes y por ustedes que son la razón fundamental de mi vida.

Dany

RESUMEN

El Fórum de Telegestión (TM Forum *por sus siglas en inglés*) es la organización mundial que ofrece orientación, directrices, estratégicas y soluciones prácticas para mejorar la gestión y el funcionamiento de los servicios de información y comunicaciones en las empresas de telecomunicaciones. Como fruto de la colaboración en dicha comunidad surge Frameworx, una suite de estándares que ofrecen un plan detallado para las operaciones de negocio. La suite ha sido adoptada por aproximadamente más del 90%[1] de los proveedores de servicios más grandes del mundo. Con su uso se logra un acercamiento orientado a servicios y a la informatización de procesos para lograr la ejecución del negocio de un proveedor de servicios de telecomunicaciones a través de un conjunto de componentes interrelacionados como lo son el eTOM (*del inglés*: **e**nhanced **T**elecomunication **O**perations **M**ap) y el SID (*del inglés*: **S**hared **I**nformation / **D**ata), este último carente hasta el momento de un modelo de datos en el área Gestión de Riesgos Empresariales, específicamente en la **Gestión de Fraude** que permita la interacción, desarrollo e innovación en el área, todo esto en concordancia con las especificaciones de la comunidad. Con el presente trabajo se pretende dar una **propuesta de solución al modelo de datos aún no definido**, cumpliendo con los requisitos de calidad establecidos por la comunidad, para su adopción por el sector de las telecomunicaciones y su inclusión en la iniciativa Frameworx.

Palabras clave: ABE, Dominio, Entidad, eTOM, Fraude, Frameworx, Modelo de datos, SID, Telecomunicaciones.

[1] Tomado del sitio oficial de la comunidad TM Forum www.tmforum.org en el año 2012.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

"Las compañías fracasan por muchas razones. Algunas veces son administradas en forma deficiente, algunas veces simplemente no crean los productos que los clientes quieren. No obstante creo que el mayor asesino de una compañía, especialmente en las industrias de rápido cambio como la nuestra, es el rechazo a adaptarse al cambio. El cambio es inevitable. La tecnología siempre evolucionará, los mercados siempre cambiarán y las personas siempre querrán más de los productos."

Bill Gates

El incremento de las empresas de telecomunicaciones, así como el alcance y aceptación de los servicios brindados ha dado lugar a una férrea competencia en el mercado, surgiendo nuevas tecnologías y tendencias que se muestran como la vía para lograr la excelencia en las operaciones de negocio y éxito empresarial. La influencia de una rápida evolución tecnológica y fuertes exigencias por parte de sus clientes y competidores propicia un acelerado desarrollo del sector así como vulnerabilidades que pueden ser utilizadas como vías para la ejecución de actividades fraudulentas. A medida que se demanda calidad y eficiencia en los servicios brindados, las empresas deben estar preparadas para afrontar los cambios necesarios, incluyendo en las soluciones creadas las operaciones que permitan un programa exitoso de *Gestión de Fraude*. Para que esto suceda, deben buscar soluciones que persigan la reducción de recursos en sus operaciones de negocio, centrándose en servicios innovadores y con la calidad requerida, que garanticen la fiabilidad e integridad de la información y los activos de la empresa. Como resultado se está observando un mayor interés en los enfoques estandarizados, como el propuesto por la comunidad TM Forum[2], un grupo compuesto por proveedores de servicios y empresas con gran éxito y prestigio internacional que colaboran para establecer las mejores prácticas dentro de la industria de las telecomunicaciones. Esta organización ofrece orientación y soluciones prácticas para lograr y mejorar la gestión, el funcionamiento e interoperabilidad de los servicios de información y comunicaciones.

El trabajo conjunto de los miembros asociados y los responsables del funcionamiento de la comunidad, dio lugar a la creación y adopción de la iniciativa Frameworx; una suite de estándares que ofrecen un plan detallado para las operaciones de negocio, permitiendo evaluar y mejorar su rendimiento. Brinda solución a los problemas de estandarización, riesgos e integración, poniendo a disposición de las empresas pertenecientes al sector de las telecomunicaciones, la inteligencia y contenidos necesarios para garantizar el éxito del negocio en el mercado.

[2] Forum de Telegestión (*del inglés*: TM Forum).

La suite ha sido adoptada por aproximadamente más del 90%[3] de los proveedores de servicios más grandes del mundo como son AT&T (del inglés: American Telegraph and Telephone), Vodafone, Deutsche Telekom entre otros y enfoca sus esfuerzos en lograr y mejorar la ejecución del negocio de un proveedor de servicios de telecomunicaciones a través de un conjunto de componentes interrelacionados. La presente investigación se centra en dos de ellos, por su contenido para el problema al que se desea dar solución y por ser la base para el uso de Frameworx.

Primero el eTOM[4], un marco referencial, que estandariza y da estructura coherente a los procesos de negocio dentro de la empresa. Así como el eTOM se encarga de representar los procesos, el SID[5] es el responsable de representar y almacenar los conceptos de negocio o información que está presente o se debe tener en consideración cuando son ejecutados dichos procesos. Esta información es representada en una manera independiente de implementación a través de diagramas UML, enfocándose en qué es la información y sus relaciones. Brinda los conceptos y principios necesarios para definir un marco de información común, modelada haciendo uso de diagramas, que proveen una vista de los datos presentes en cada proceso. (1)

El eTOM arrojó una descripción estándar del proceso de Gestión de Fraude pero en el SID, se identificaron deficiencias, al no contar con la información requerida, obstaculizando así el desarrollo en el ámbito de las telecomunicaciones y los objetivos de Frameworx. Por ello, los departamentos dedicados a esta tarea se ven imposibilitados de beneficiarse de las ventajas de integración, colaboración y estandarización que presenta esta iniciativa.

Las empresas dedicadas a las prestación de servicios de telecomunicaciones, que deseen adoptar Frameworx como directriz en su desempeño, como lo es la Empresa de Telecomunicaciones de Cuba S.A, se ven limitadas en la ejecución de los procesos de Gestión de Fraude perteneciente al área de Gestión Empresarial, debido a que el SID no cuenta aún con las entidades y relaciones estandarizadas que intervienen en este proceso. Esto trae consigo una repercusión negativa en el soporte de las demás operaciones dentro de la empresa y en el desarrollo de la industria en general porque aún, cuando cada una de ellas puede desarrollar el proceso de acuerdo a sus necesidades, siguen presente problemas de estandarización, integración y elevados costos de desarrollo, entre otros que TM Forum desea erradicar y que afectan al sector de las telecomunicaciones.

---

[3]Tomado del sitio oficial de la comunidad Tele Management Forum http://www.tmforum.org en el año 2012.

[4]eTOM: (del inglés: enhanced **T**elecomunication **O**perations **M**ap) Marco referencial de procesos de negocio para las empresas de telecomunicaciones.

[5]SID: (del inglés: **S**hared **I**nformation / **D**ata) Marco de Información / Datos Compartidos para las empresas de telecomunicaciones.

El amplio alcance e implicación de los procesos en el área de la Gestión Empresarial hacen imprescindible la búsqueda de una solución que cumpla con los requisitos para formar parte de la suite Frameworx, siendo aprobada por la comunidad TM Forum.

Teniendo en cuenta la **situación problemática** referida con anterioridad se plantea como **problema a resolver** el siguiente: Las especificaciones del SID para los procesos de la Gestión de Fraude no satisfacen las necesidades de ETECSA.

A partir del problema planteado se define como el **objeto de estudio** las especificaciones propuestas por Frameworx para la Gestión de Fraude en las empresas de telecomunicaciones y el campo de acción queda enmarcado en los procesos asociados a la Gestión de Fraude en ETECSA.

El **objetivo general** consiste en diseñar un **Modelo de Datos** basado en las especificaciones de Frameworx para la Gestión de Fraude, que satisfaga las necesidades de ETECSA.

Las **tareas** que se deben desarrollar para cumplir con el objetivo general son:

1. Elaborar el marco teórico de trabajo, para realizar la propuesta del Modelo de Datos basado en los estándares que propone Frameworx.
2. Estudiar el conjunto de marcos de trabajo propuestos por Frameworx, para el análisis exhaustivo del proceso de Gestión de Fraude.
3. Analizar, diseñar y elaborar un Modelo de Datos basados en las especificaciones de Frameworx.
4. Seleccionar las tecnologías y herramientas relacionadas con la creación del Modelo de Datos.
5. Desplegar la Base de Datos con el Modelo de Datos propuesto en el área de Gestión de Fraude de ETECSA.
6. Elaborar una adecuada documentación del Modelo de Datos propuesto.

Para realizar las tareas se emplearán los siguientes **métodos**:

Teóricos:

Analítico - Sintético: Este método permitirá analizar las teorías y los documentos referentes al objetivo de la investigación, facilitando de esta forma la extracción de los elementos más importantes relacionados con el objeto de estudio. Además de que posibilitará construir el camino a seguir, a partir del análisis detallado de cada uno de los documentos previamente mencionados.

Histórico - Lógico: Se utiliza para realizar un estudio de los antecedentes y tendencias actuales de Frameworx y los procesos de Gestión Fraude.

Empíricos:

Entrevista: Se realizó la entrevista a los especialistas de ETECSA encargados de la gestión y detección de incidentes anómalos así como a los tutores de la investigación para la recopilación de datos y mejor compresión de los procesos llevados a cabo para una efectiva modelación y representación de los datos requeridos.

CAPÍTULO 1: FUNDAMENTACIÓN TEÓRICA

1.1. Introducción

El fraude ha evolucionado a la par de la industria de las telecomunicaciones y el desarrollo tecnológico, ocasionando pérdidas de más de $40 billones por año[6], esta cantidad no comprende los gastos asociados a los procesos de detección y eliminación de acciones fraudulentas. Este crecimiento ha sido atenuado en gran parte debido a la amplia adopción de procesos de Gestión de Fraude y herramientas por los proveedores de servicios. Actualmente hay identificados más de 70 tipos de fraude[7] los cuales no solo afectan al proveedor de servicios sino también a toda la cadena asociada a la ejecución de negocio. Con la latente necesidad de buscar una solución a la problemática planteada mediante el desarrollo de la investigación, se hace imprescindible profundizar en los principales conceptos e interrogantes, que representan el punto de partida en la búsqueda de la solución esperada, basada sobre los principios y especificaciones de TM Forum. Además en el presente capítulo se llevará a cabo el estudio de las herramientas y tecnologías necesarias para bridar una propuesta de solución y su correspondiente validación, así como otros aspectos que se consideren necesarios para el comienzo de la investigación.

1.2. Iniciativa Frameworx de TM Forum

1.2.1. Comunidad TM Forum

Fundada en 1988, la razón de ser de TM Forum es la colaboración, con el objetivo de establecer las mejores prácticas, mejorar la eficiencia en los procesos y negocios existentes en las empresas de telecomunicaciones y acelerar la disponibilidad de productos de gestión de red inter-operables. Es una comunidad mundial sin fines lucrativos, compuesta por proveedores de servicio de telecomunicaciones, fabricantes de equipamiento, desarrolladores de software, creadores de contenido e integradores de sistemas. "…*Esta organización crea un proyecto conocido como: Software y Sistemas de Operación de Nueva Generación (NGOSS, por sus siglas en inglés). El cual usa un mapa común de procesos, descripción de sistemas y modelos de información, unido a interfaces de integración predefinidas, principios de arquitectura y criterios de cumplimiento, con el objetivo de lograr la interoperabilidad, gestión de las operaciones y aplicaciones de soporte a las operaciones y servicios…*" **(Rodríguez, 2008)**. Sus miembros se benefician del conocimiento, capital intelectual y colaboración, promoviendo el uso de soluciones en pos de la estandarización de la industria. Compuesto por una comunidad de más de 65000

[6] Dato tomado del sitio oficial de la comunidad TM Forum http://tmforum.org en el año 2013.
[7] Dato tomado del sitio oficial de la comunidad TM Forum http://tmforum.org en el año 2013.

profesionales pertenecientes a las 900 compañías miembros.[8] Experimentados en la industria y dedicados al desarrollo de la comunidad Frameworx. (1)

Frameworx es la evolución o sucesor de NGOSS, desarrollada y respaldada por la comunidad TMForum. Es una *suite* de estándares y buenas prácticas para las empresas de telecomunicaciones, que ofrece un plan detallado para las operaciones de negocio, evaluando y mejorando su rendimiento. Constituye una vía para lograr la integración, estandarización de la industria y eficiencia empresarial. Frameworx es impulsado por las necesidades de servicios y está en constante evolución. Su fortaleza e idoneidad radica en que permite:

- Comprender al cliente a través de un modelo común de gestión de la información.
- Reducir los costos operativos, permitiendo la automatización y el estándar de la industria.
- Reducir los costos de integración y los riesgos a través de un modelo de información común.
- Eliminar barreras generadas por factores sociales, culturales y económicos, proporcionando un campo común para el lenguaje estándar de la industria.
- Crear alianzas esenciales de forma rápida y fácil a través de un proceso común y la comprensión de la información y la terminología. (2)

1.2.1.1. Componentes de Frameworx

Frameworx logra sus objetivos a través de un grupo de componentes interrelacionados, enfocados en aspectos fundamentales del negocio dentro de la empresa. Proponen herramientas, estructura de procesos y bases de datos, además de otras buenas prácticas que desembocan en resultados de calidad y dentro del estándar para el desarrollo en las telecomunicaciones. La investigación se centra en el Marco de Procesos de Negocio (**eTOM**) y el Marco de Información / Datos Compartidos (**SID**) sin dejar de hacer referencia a los restantes componentes como el Mapa de Aplicación (**TAM**) y el **Marco de Integración**, los cuales juegan un papel fundamental en el éxito de Frameworx.

[8]Tomados del sitio oficial la comunidad Tele Management Forum http://www.tmforum.org en el año 2012.

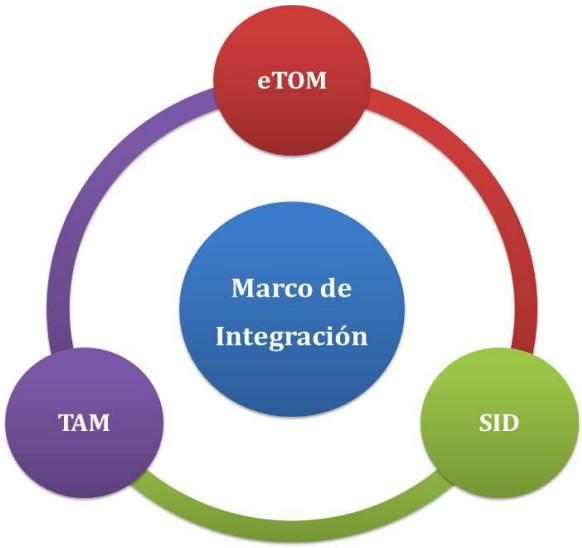


Fig. 1: Estructura de Frameworx.

El **eTOM** fue diseñado y desarrollado para describir y brindar un lenguaje común para los procesos de negocio llevado a cabo en las empresas pertenecientes al sector de las telecomunicaciones. Ha sido adoptado por la Unión Internacional de Telecomunicaciones (UIT) la cual recoge todo su contenido en la Recomendación M.3050[9] desde julio del 2004. Constituye un marco referencial de procesos para la industria de las telecomunicaciones, brindando una vista común de los elementos y actividades que deben formar parte del marco de negocio de cualquier empresa del sector. Hoy en día posee información fundamental y pretende entre otras cosas, estandarizar los procesos de negocio estableciendo la información necesaria para la modificación de la estructura u optimización de los procesos de negocio ejecutados.

Los procesos comprendidos en el eTOM representan el entorno empresarial de un proveedor de servicios mediante una jerarquía de elementos de procesos que representan sus detalles a varios niveles. El nivel 0 representado a continuación en la figura 2, cubre las actividades del negocio en tres áreas principales (Infraestructura - Producto - Estrategia, Operaciones y Gestión Empresarial). Los siguientes niveles presentan un mayor nivel de detalle y se enfocan principalmente en aspectos relacionados con la agrupación, procesos base y flujos de procesos de negocio.

[9] Las Recomendaciones UIT-R, constituyen una serie de normas técnicas. Estas son el resultado de estudios efectuados por las Comisiones de Estudio de Radiocomunicaciones. Éstas son el resultado de estudios efectuados por las Comisiones de Estudio de Radiocomunicaciones. El proceso de su aprobación es mediante consensos entre los Estados Miembros de la UIT. Su aplicación no es obligatoria; sin embargo, puesto que éstas son elaboradas por expertos de las administraciones, los operadores, el sector industrial y otras organizaciones dedicadas a las radiocomunicaciones en todo el mundo, disfrutan de una prestigiosa reputación y se aplican a escala mundial.

Fig. 2: eTOM: Estructura.

El área de procesos que comprende la Gestión Empresarial es la encargada de cubrir la gestión corporativa o de soporte al negocio. En ella se concentran los procesos que toda empresa debe tener para su normal funcionamiento, incluyendo los que gestionan las necesidades de la empresa y ofrecen soporte, así como procesos para la administración financiera, legal, administración de costos y calidad. La Gestión de Riesgo Empresarial es una de las áreas de procesos comprendidas en el marco de la Gestión Empresarial, de vital importancia para el soporte de las operaciones en la ejecución del negocio.

Fig. 3: eTOM Área de Procesos: Gestión Empresarial.

Los procesos que en ella se enmarcan, se encargan, entre otras cosas de identificar posibles riesgos o vulnerabilidades en la empresa, que pueden atentar contra la solvencia económica e influir negativamente en la reputación de la empresa. De esta manera, tomar medidas para mitigarlos o eliminarlos y trazar estrategias para mantener la seguridad y continuidad del negocio son tareas fundamentales. Un exitoso programa de gestión de riesgos asegura que la empresa se encuentre en condiciones de brindar soporte a

sus operaciones, procesos y aplicaciones, además de enfrentar exitosamente incidentes adversos y amenazas de seguridad.

La Gestión de Fraude, como se ilustra a continuación en la figura 4, forma parte del grupo de procesos imprescindibles para un eficaz programa de Gestión de Riesgos.

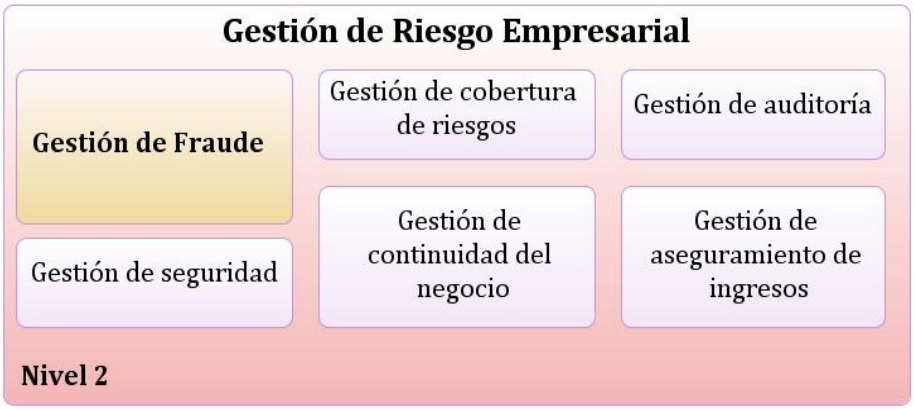


Fig. 4: eTOM Área de Procesos: Gestión de Riesgo Empresarial.

Dentro de los principales riesgos que puede correr una empresa en su desarrollo es la exposición continua a las acciones fraudulentas de toda índole, por lo que la Gestión de Fraude está comprendida como uno de los riesgos empresariales que pueden ocurrir y que debe ser eficazmente tratado. Los procesos en esta sección contribuyen a lograr los objetivos que se persiguen con la ejecución de los procesos en la Gestión de Riesgo Empresarial. Principalmente el área se enfoca en el aseguramiento contra violaciones de seguridad y normativas trazadas, tanto para clientes como empleados. Su correcta ejecución garantiza la continuidad y salud en general del negocio.

Por su parte el **SID** permite la simplificación en la gestión de la información, reduciendo la redundancia y variaciones mediante una terminología común, y la unificación de la información entre los proveedores de servicios, integradores de sistemas u otra parte involucrada. Como complemento de eTOM, SID se enfoca en los datos e informaciones que se relacionan en procesos de negocios, personas, finanzas, productos y servicios y gestión empresarial. *"… Brinda los conceptos y principios necesarios para definir un modelo de información compartida y diagramas UML para proveer una vista de la información y los datos desde el punto de vista del sistema… "* **(Rodríguez, 2008)**. (1)

Es un facilitador del éxito, no una garantía para ello. Las ventajas sobre otras compañías adoptando el Frameworx vendrán de la calidad en la implementación del negocio y su nivel de integración. El alcance del SID cubre toda la información requerida para implementar casos de uso basados en los procesos de negocio, está siendo aún desarrollado y mientras que los documentos existentes abarcan una gran parte de la información que los proveedores de servicios necesitan, aún no es suficiente. (36)

Este marco de trabajo juega un papel importante y decisivo para la investigación en curso, ya que comprende un modelo conceptual o de análisis genérico y alejado de la implementación. Se enfoca en las cosas sobre las que el proceso de negocio actúa, dígase entidades de negocio, sus características y relaciones; todo ello basado en las especificaciones de los procesos presentes en cada área del eTOM, el cual usa para definir su alcance y que es importante para el proveedor de servicios. Constituye una vía eficiente para lograr la integración con otros sistemas desarrollados, manteniendo el estándar dentro de la industria mediante un modelo de datos e información común. Es necesario esclarecer que el SID no es un modelo de base de datos, ni una definición de como el software debe ser implementado, ni tampoco de sus clases. No es una definición de plataformas, protocolos, lenguajes o herramientas. Solo un modelo de análisis que provee definiciones de negocios como base para lograr los objetivos propuestos con la ejecución de un determinado proceso.

El SID se encuentra estructurado mediante ABEs (*del inglés: Agregate Business Entities*), las cuales aparecen asociadas a un área de administración específica llamadas "*Dominios*" permitiendo la segmentación de problemas de negocio y la posibilidad de enfocarse en la información deseada. Esta estructura también permite su alineación con los conceptos de negocio y áreas existentes en el eTOM. Entre los dominios existe uno al que se debe prestar especial atención por su importancia dentro del modelo, se hace alusión al Dominio de Entidades Comunes (*del inglés: Common Bussines Entities*), que no son más que entidades compartidas entre dos o más dominios, son clases genéricas (súper clases) recurrentes dentro del modelo y que están presentes en la mayoría de las operaciones dentro de la empresa. Los restantes dominios: Cliente (*del inglés: Customer*), Producto (*del inglés: Product*), Servicio (*del inglés: Service*), Recurso (*del inglés: Resource*) comprenden información específica y se centran en conceptos sobre los procesos que agrupan abarcando un área claramente delimitada. Así mismo existen dominios que no han sido cubiertos totalmente, encontrándose bajo construcción por parte de la comunidad como es el caso de "*Gestión Empresarial*". La "*Gestión de Riesgos Empresariales*", forma parte del grupo de procesos que en este dominio deben llevarse a cabo y comprende dentro de su estructura el ABE "*Gestión de Fraude*", aún sin desarrollar.

El desarrollo y uso del dominio Gestión Empresarial mediante la identificación de la información y las relaciones que deben formar parte del ABE Gestión de Fraude representa un paso fundamental para el logro de los objetivos propuestos con la presente investigación. Para ello se debe realizar un estudio previo de los procesos de una empresa de telecomunicaciones dedicados a esta tarea como complemento a los definidos por el eTOM, cuyo resultado debe arrojar una propuesta de las entidades y relaciones a incluir en la "*Gestión de Fraude*".

1.2.2. Aplicando Frameworx.

1.2.1.2. Verizon Communications Inc.

En 2007 la organización norteamericana Verizon Communications Inc. comenzó un programa para implementar un comprensivo conjunto de controles de aseguramiento de ingresos en toda la empresa. En un tiempo de 3 años implementó un comprensivo programa de aseguramiento de ingresos para los clientes minoristas, basado en el principio de la prevención. Originalmente el programa tenía que ejecutarse durante 5 años pero su notable éxito incluso antes de la total implementación hizo que el plazo se acortara a 3 años solamente. La compañía afirma que el tamaño, el alcance y enfoque de este programa no tiene precedentes para un proveedor de servicios de Nivel 1 y que el plazo de 3 años habría sido extremadamente difícil sin el uso de los estándares de TM Forum. En 2010 la organización logró un aumento en sus ganancias valorado en más de 60 millones de dólares por conceptos de ahorros y ganancias o compensaciones. La empresa sigue avanzando a buen ritmo, trabajando en estrecha colaboración con TM Forum.

Influencia de Frameworx en los resultados alcanzados:

El eTOM fue utilizado para examinar las funciones de negocio que tenían impacto en el proceso de aseguramiento de ingresos. Aseguró que todas estas operaciones con un efecto en el proceso fueran incluidas en los controles construidos para el programa de 3 años a llevar a cabo por la empresa. El SID fue usado para profundizar en el eTOM y asegurar que el equipo capturó los datos apropiados de relevancia para el sistema. (4)

1.2.1.3. Vodafone D2

El programa de garantía de servicio de nueva generación de Vodafone D2 es el mayor proyecto de transformación llevado a cabo por la compañía. Compuesto por más de 12 sub proyectos, más de 1000 procesos y un enorme número de dependencias. El uso de TM Forum Frameworx fue crucial para el éxito del proyecto que contribuyó a un ahorro del 47% en el gasto del capital y el 68% en gastos operacionales o de funcionamiento. La mayor contribución a la reducción de costos la tuvo el SID, responsable de más del 40% de los ahorros obtenidos. En un futuro la compañía espera un ahorro del 30% por conceptos de integración y personalización. La empresa desea comenzar un proyecto de transformación mayor, basándose en el éxito del proyecto.

Influencia de Frameworx en los resultados alcanzados:

El eTOM fue usado como la guía principal para asegurar y facilitar una transición sin problemas. Por su parte el SID fue utilizado paralelamente para identificar la información y lograr la transición segura entre

modelos de datos mediante la extensión de las entidades que propone, sin poner el riesgo el éxito del resultado final. (5)

1.2.1.4. MIMO Tech Co. Ltd.

MIMO Tech Co. Ltd. compañía Tailandesa proveedora de servicios y agregados de beneficios como valor añadido como la banda ancha móvil y el contenido. La prestación de servicios de valor añadido fue tornándose cada vez más complejo y más importante para su negocio en términos de competitividad y participación en el mercado. La arquitectura para mantener estos servicios no era flexible para soportar el marketing dinámico y los cambios tecnológicos y nuevos modelos de negocio. Para solucionar esta situación adversa para el negocio recurrió a soluciones en línea con la suite Frameworx para lograr la transformación necesaria. La solución obtenida redujo los costos operativos en más del 20% mediante una mayor eficiencia en el modelado de servicios y la monitorización. La mejora en la eficiencia y la oferta de nuevos servicios de valor añadido alcanza un 50% mayor en relación a la forma en la que solía trabajar.

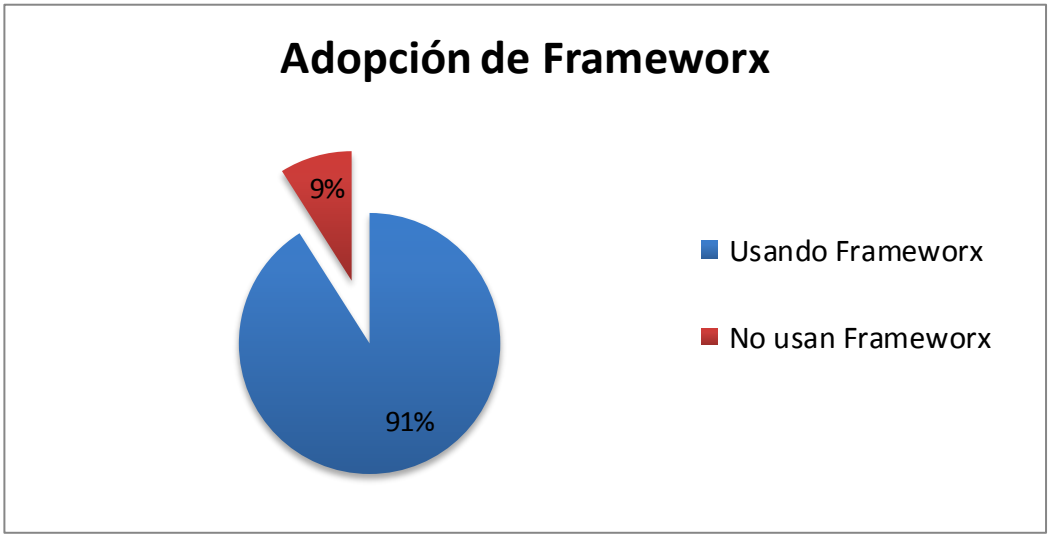
Influencia de Frameworx en los resultados alcanzados:

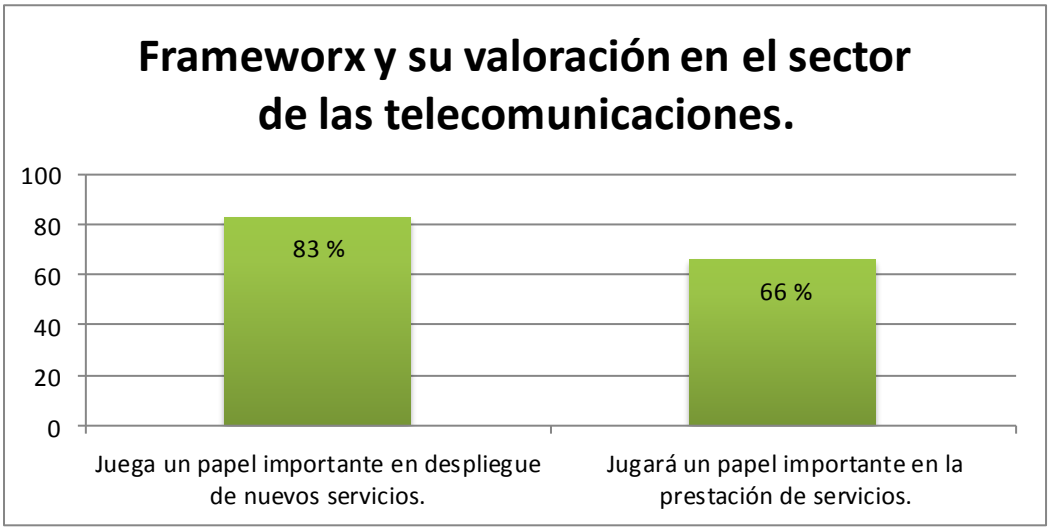
La compañía hizo uso del eTOM para consolidar el despliegue de servicios y la gestión de procesos en los dominios correspondientes. El uso de SID como guía para el diseño de su modelo de datos, enfocándose principalmente en las entidades críticas para la solución de sus necesidades. (6)

1.2.3. Necesidad de adoptar Frameworx.

Un amplio estudio de los miembros de la comunidad evaluó la experiencia, adopción y planes para comenzar a usar la iniciativa Frameworx. Los resultados demostraron que el futuro de las empresas de telecomunicaciones y proveedores de servicios estará fuertemente relacionado con la comunidad y su forma de proceder. "… *Más de 130 participantes procedentes de 87 empresas líderes en prestaciones de servicios fueron encuestados. Los resultados de la encuesta confirman la profundidad y amplitud de la continua adopción de Frameworx. El 91% de las empresas representadas ya se encuentra utilizando la iniciativa Frameworx. Los proveedores de servicios de todo el mundo están utilizando Frameworx, con el objetivo de hacer más eficientes sus operaciones, reducir costos y permitir el rápido diseño, desarrollo y despliegue de nuevos servicios. Un 83% de los encuestados afirmó que Frameworx juega un papel clave en el despliegue de nuevos servicios y el 66% dijo que jugará un papel importante en la prestación de los mismos. TM Forum continúa trabajando con los miembros de su comunidad en colaboración para asegurarse de que las normas, mejores prácticas y herramientas que comprende Frameworx contribuyan a satisfacer las necesidades de la industria…* " **(TM Forum Community, 2012)**. (7)

TM Forum se plantea como la organización rectora en el desarrollo del sector de las telecomunicaciones debido a la calidad y adopción de sus productos, componentes como eTOM y SID así lo ratifican. Aunque no son los únicos, constituyen la base o puntos imprescindibles en el uso de Frameworx y para la presente investigación. El trabajo en conjunto con otras organizaciones donde prime la colaboración y ayuda mutua empresarial ha ayudado a que sea reconocido mundialmente el trabajo realizado y el mérito que actualmente posee. Todo ello conlleva a una reflexión: TM Forum y Frameworx comienzan a tomar el control del desarrollo de la industria de las telecomunicaciones, en un futuro no muy lejano sus normas e iniciativas no serán solamente una opción, sino una necesidad para la salud y solvencia económica de las empresas, así como para la interaccción y permanencia en el mercado. Cuba y especificamente la Empresa de Telecomunicaciones de Cuba SA no puede estar ajeno a estas nuevas tendencias por todo lo que representan hoy día.





1.3. Lenguajes

1.3.1. Lenguaje de Modelado

UML *(del inglés: Unified Modeling Language) "… es un lenguaje visual de modelado de propósito general para "visualizar, especificar, construir y documentar los artefactos de un sistema software", accesible a todos es usado para entender, diseñar, controlar información de los sistemas. Incorpora las mejores prácticas agregando un enfoque estandarizado. UML es ante todo un lenguaje gráfico que estandariza la forma de crear diagramas, el significado preciso de los mismos, y las relaciones existentes entre ellos que cuenta con herramientas que proveen generación de código en varios lenguajes… ".* **(IBM, 2004)** (8)

UML posee la característica de ser adaptable a cualquier metodología de desarrollo de software, los complementos visuales que proporciona para la modelación son usados mundialmente con un éxito probado dentro de la industria de desarrollo de software. Es utilizado por los analistas de la comunidad TM Forum para el desarrollo del modelo SID, por lo que se hace indispensable el uso de este para el análisis del modelo y para representar los conceptos de negocio que formaran parte de la Gestión de Fraude.

1.3.2. Lenguaje declarativo de acceso a bases de datos.

SQL (*de inglés: Structured Query Language*) "*… lenguaje de acceso a bases de datos que explota la flexibilidad y potencia de los sistemas relacionales, permitiendo gran variedad de operaciones sobre los mismos. Es un lenguaje declarativo de alto nivel o de no procedimiento, que gracias a su fuerte base teórica y su orientación al manejo de conjuntos de registros, y no a registros individuales, permite una alta productividad en codificación. De esta forma una sola sentencia puede equivaler a uno o más programas*

que utilicen un lenguaje de bajo nivel orientado a registro… ". (**EcuRed, 2012)** (9) Asume el papel de lenguaje de definición de datos (DDL), lenguaje de definición de vistas (VDL) y lenguaje de manipulación de datos (DML). Además permite la concesión y denegación de permisos, la implementación de restricciones de integridad y controles de transacción, y la alteración de esquemas. El sistema de base de datos Oracle, empleado en el entorno empresarial donde tendrá lugar la validación de la propuesta de solución es accedida actualmente usando SQL, lo cual incluyendo las ventajas y características anteriormente expuestas justifican su uso en la presente investigación.

1.4. Herramienta CASE

Se seleccionó Visual Paradigm para UML en su versión 8.0, ya que es una herramienta profesional que tiene disponibilidad de integración con ORACLE, facilitando la generación de la base de datos a partir del modelo Entidad – Relación extendido que surgirá como resultado de la investigación. Con soporte completo de notaciones UML, siendo compatible con la selección del lenguaje de modelado seleccionado. Permite el análisis de diagramas e información modelada a través de diagramas u otros artefactos generados en procesos de análisis de sistemas o procesos de negocio. Provisto de alta interoperabilidad permite la importación y exportación de ficheros XML y establece conexión con Rational Rose en sus archivos de proyecto, lo que facilitará el estudio del modelo SID brindado por la comunidad. Posee herramientas de calidad para la generación de documentación. Es fácil de instalar y actualizar manteniendo la compatibilidad entre ediciones, con opciones en cuanto al uso del idioma deseado. Posee una edición comunitaria lo que elimina riesgos de licencias a pagar u otro tipo de restricciones asociadas.

1.5. Servidor de Base de Datos

Oracle 11g es un sistema de gestión de base de datos relacional fabricado por Oracle Corporation, disponible sobre plataforma Linux, con rendimiento probado, rentabilidad, seguridad y escalabilidad. "… *La última versión de la base de datos más popular del mundo, con más de 400 funcionalidades, 15 millones de horas de test y 36.000 meses - hombre de esfuerzo de desarrollo, la Base de datos Oracle 11g es el producto más innovador y de mayor calidad que Oracle ha anunciado hasta la fecha*. *Es la primera base de datos del mundo en incluir funcionalidades que permiten hacer pruebas de cambios en aplicaciones simulando las cargas reales generadas por los usuarios en los entornos de producción utilizando la funcionalidad Real Application Testing, con esta los clientes ganan en flexibilidad puesto que pueden responder de manera más efectiva a los requerimientos cambiantes del negocio y hacer una gestión del cambio más efectiva…* ". (**Redacción LaFlecha, 2007)** (10)

Dotado de gran facilidad de instalación, configuración y administración, adaptable para su utilización en pequeñas empresas, departamentos y entornos distribuidos, aspectos que lo hacen idóneo para su utilización y adaptación a las necesidades de cada empresa. Brinda la posibilidad de administración de memoria y almacenamiento, realizando copias de seguridad y recuperación automática. Facilita el acceso a los datos mediante interfaces estandarizadas como SQL y JDBC. El departamento encargado de la Gestión de Fraude en ETECSA, escenario donde se llevará a cabo la validación de la propuesta, actualmente lleva a cabo el desarrollo del proyecto SIAI[10], en el cual se ha apostado por la alternativa de que exista solo un SGBD logrando así mantener la línea de trabajo de ETECSA además de una eficiente interoperabilidad. La calidad, robustez y la reducción riesgos asociados a la pérdida de información han sido cualidades por las que las empresas han apostado por el uso de esta herramienta, a pesar del pago de su licencia. ETECSA cuenta con la licencia para su utilización y especialistas capacitados en su uso, lo que se traduce en garantía, integridad y óptima gestión de los datos almacenados.

1.6. Conclusiones

Se han definido los principales conceptos que se manejaran a lo largo de la investigación así como las herramientas, metodología y lenguajes a utilizar para dar cumplimiento a los objetivos planteados. Ha quedado demostrada la importancia y novedad del tema además de su repercusión e influencia en el sector de las telecomunicaciones, por lo que urge la búsqueda de la solución adecuada. Principalmente se abordaron los componentes de Frameworx en los cuales se centrará la investigación y donde surge la problemática asociada.

Se puede afirmar que una de las grandes fortalezas de TM Forum y Frameworx radica en que persiguen la coexistencia y alineación con todos los estándares desarrollados hasta la fecha, solo que con un enfoque hacia la industria de las telecomunicaciones. Su intención no es crear nuevos paradigmas y hacer obsoletos los que hasta el momento existían, si no mejorar los procesos y especificaciones existentes y que de una manera u otra se relacionen con el trabajo realizado por una empresa de telecomunicaciones.

[10] Sistema Integral de Análisis de la Información. Proyecto creado como fruto de la colaboración entre la Universidad de las Ciencias Informáticas UCI y La Empresa de Telecomunicaciones de Cuba SA ETECSA con el objetivo de desarrollar un sistema para la Gestión de Fraude (FMS: por sus siglas en inglés).

CAPÍTULO 2: MODELO SID

2.1. Introducción

El SID ha sido estructurado de manera que sus dominios se vean alineados con los procesos presentes en el eTOM, de manera modular, pretendiendo representar toda la información presente en las operaciones de negocio. Los dominios mantienen una estrecha relación, colaborando para proporcionar los datos necesarios en la estructuración de cada modelo. De manera abstracta y genérica hasta el momento, el SID abarca una gran parte de la información requerida, siendo víctima por decirlo de alguna manera del poco tiempo de desarrollo que presenta la iniciativa. El dominio Gestión Empresarial se encuentra rezagado con relación a los demás existentes; no por ello se debe pensar que es menos importante, sólo que las empresas necesitan alcanzar un desarrollo y presencia considerable en el mercado que le permita sustentar las operaciones básicas mediante la obtención de ganancias. El soporte a toda la infraestructura empresarial, como por ejemplo una buena Gestión de Fraude son pasos que se debe ir desarrollando para evitar riesgos y garantizar la salud del negocio. El presente capítulo tendrá la responsabilidad de plasmar las principales características sobre el modelo SID, su estructura, así como las pautas a seguir para su correcta utilización.

2.2. Estructura del Modelo SID.

2.2.1. Dominios SID

2.2.1.1. Service Domain:

Consiste en un grupo de ABEs que son usadas para gestionar la definición, desarrollo y los aspectos operacionales de los servicios provistos por el sistema NGOSS[11]. Las entidades en este dominio representan la información relacionada con los procesos del eTOM que están relacionados con la definición, desarrollo y gestión de los servicios ofrecidos por una empresa. Este dominio comprende acuerdos en cuanto a nivel de servicio, implementación y configuración de servicios así como la gestión de problemas en la instalación del servicio, uso y desempeño del mismo. También incluye a las entidades para llevar a cabo la planificación de futuras ofertas, retiro o mejora de servicio.

[11]Software y Sistemas de Operación de Nueva Generación, proyecto desarrollado por la comunidad TM Forum conocido como NGOSS por sus siglas en inglés.

2.2.1.2. Resource Domain:

En este domino están presentes ABEs usadas para los aspectos relacionados con el cómputo de la información e infraestructura de procesamiento en un sistema NGOSS. Incluye los productos y servicios que usa dicha infraestructura. Las entidades en dicha dominio también están asociadas con procesos para mejorar, ampliar o retirar servicios brindados por la empresa.

Persigue tres objetivos fundamentales:

1. Asociar Recursos a Productos y Servicios, así como proveer un detallado grupo de entidades para facilitar dicha asociación.
2. Asegurar que los recursos tengan la capacidad y calidad para soportar y completar los servicios ofrecidos por la empresa.
3. Crear estrategias y planificación para los procesos que sean definidos relacionados con los recursos que gestiona la empresa.

2.2.1.3. Customer Domain:

En este dominio se encuentran las ABEs usadas para los aspectos relacionados con la gestión de operaciones relacionadas con el cliente en un sistema NGOSS con soporte para los procesos del eTOM. Sus entidades de negocio se centran en manejar datos, necesidades, solicitudes y relaciones del cliente con la empresa mediante algún tipo de servicio ofrecido. Provee entidades para una exitosa interacción, recopilación de datos, identificación de patrones, resolución de problemas y manejo de asuntos legales entre otros. Todo ello garantiza el cumplimiento de las responsabilidades del cliente y de la empresa para con el servicio en el mercado.

2.2.1.4. Product Domain:

Conjunto de información que intenta representar los aspectos fundamentales de los productos ofrecidos por la empresa y su representación al cliente. Representa los datos fundamentales como, precio, catálogos y condiciones de uso. Abarca el desarrollo de planes y estrategias para el desarrollo y despliegue de productos, así como su retiro del mercado. Mantiene registros relacionados con su uso y comportamiento, permitiendo la evaluación y facilitando la toma de decisiones.

2.2.1.5. Market / Sales Domain:

Es el dominio que brinda soporte a las estrategias y planes de la empresa en el mercado, identificando los productos y canales apropiados. Propone entidades para gestionar los segmentos del mercado, competencias, campañas de marketing y canales de venta en el ciclo de vida del producto. La

identificación de nuevos requerimientos, necesidad del cliente, todo ello mediante el estudio de estadísticas de venta e indicadores de desempeño que permiten la rectificación de errores y la mejora constante del proceso llevado a cabo.

2.2.1.6. Common Business Entities Domain:

Representan las entidades de negocio compartidas entre dos o más dominios dentro del SID. Las entidades contenidas en este dominio constituyen una abstracción genérica de la información fundamental que interviene en la mayoría de los procesos ejecutados dentro del negocio de un proveedor de servicios.

2.2.2. Diagrama de paquetes

Los dominios anteriormente descritos interactúan entre sí, como se muestra a continuación en la figura 5, brindando una estructura coherente de los datos que se manejan en los diferentes procesos ejecutados en la empresa y alineados con eTOM. Esta vista además proporciona una medida de la importancia del domino *Common Business Entities* dentro del modelo, así como el dominio Gestión Empresarial, encargado del soporte de las operaciones dentro de la empresa y carente del contenido necesario para la ejecución de los procesos de Gestión de Fraude.

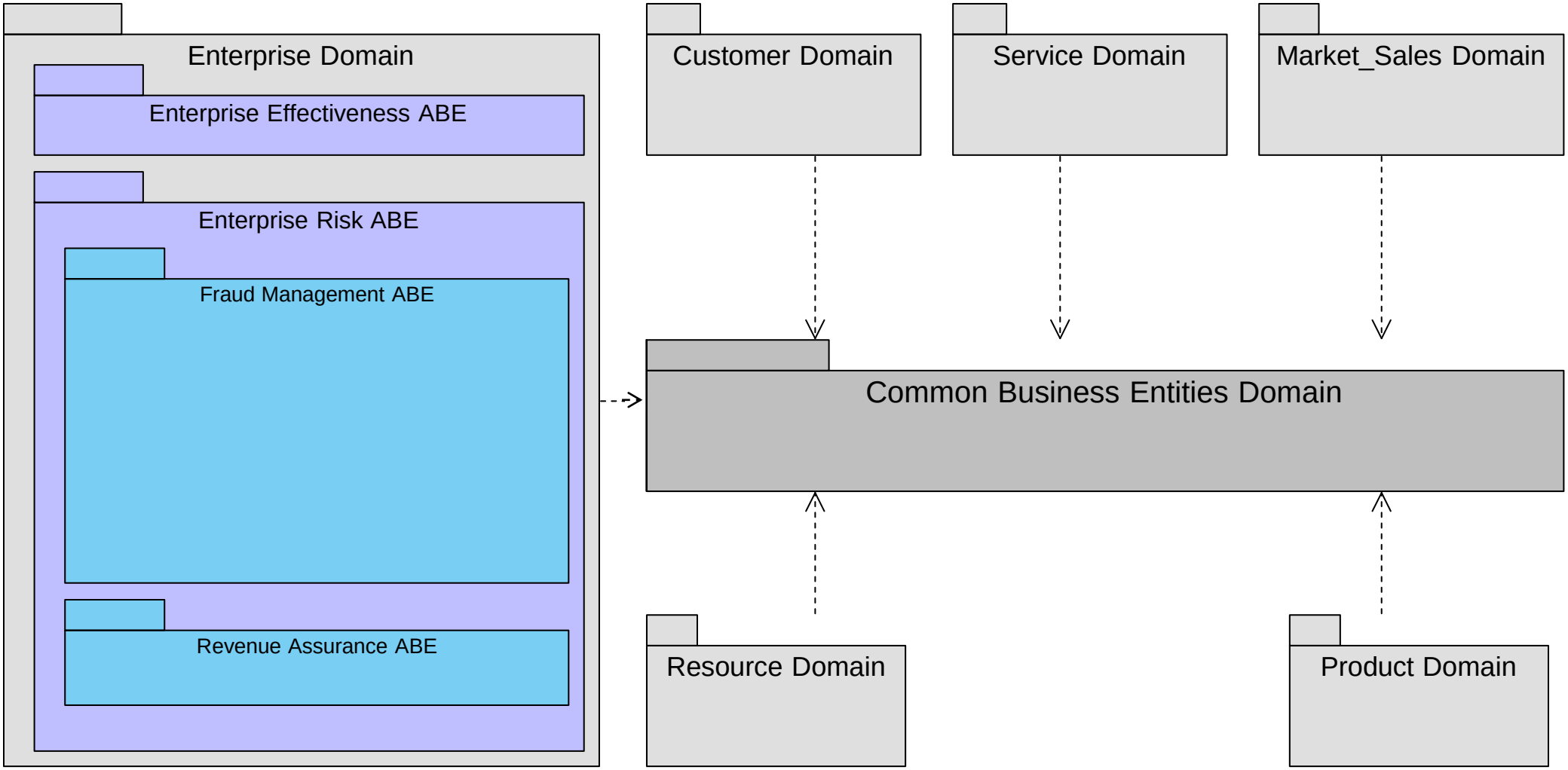


Fig. 5: Estructura de paquetes SID R9.0.

2.3. Análisis de los procesos de Gestión de Fraude en el eTOM R9.0.

A continuación se presenta un flujo de actividades que describen los procesos de Gestión de Fraude, perteneciente al eTOM y brindado por la comunidad, que serán utilizados para definir las ABEs necesarias para dicho proceso en el modelo SID.

La Gestión de Fraude se descompone en tres grupos de procesos principales como se muestra a continuación en la figura 6. En estos está contenido la mayor parte de los conceptos y descripción de procesos de negocio que deben ser ejecutados. El nivel de detalle es adecuado y logra su razón de ser, proponiendo, hasta un punto un marco de desarrollo con la flexibilidad requerida para que el nivel de detalle que diferencia a cada empresa pueda ser adicionado por el analista o desarrollador de acuerdo a sus necesidades.

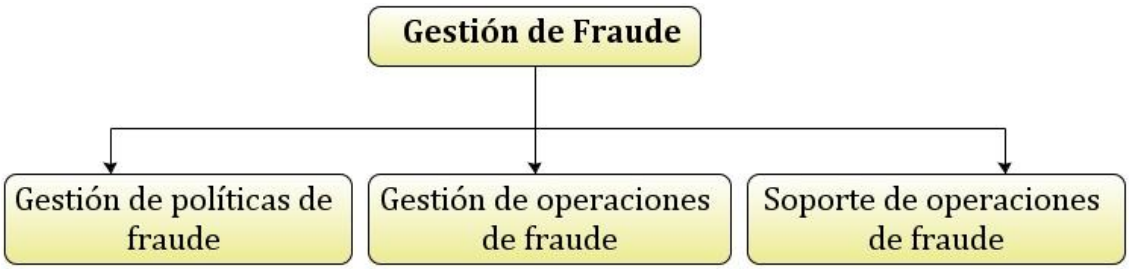


Fig. 6: Proceso de Gestión de Fraude. Procesos de Nivel 3.

2.3.1. Gestión de Políticas de Fraude.

El objetivo de las funciones en esta ABE es la gestión y mantenimiento de las políticas necesarias para un programa exitoso de operaciones de fraude dentro de la compañía. Dichas políticas deben ser adecuadas a los productos ofrecidos, región geográfica donde está enmarcado el papel de la empresa, estructura interna de la red u otro factor con influencia sobre los resultados del negocio. Incluye la identificación de prácticas para el proceso de detección, investigación, educación del personal y los clientes. Propone una adecuada retroalimentación y trabajo con fraudes ya identificados e información resultante de relaciones con agentes externos. Dentro de los procesos que garantizan su realización se encuentra el *Análisis e identificación de políticas*, *Gestión de la clasificación de fraudes*, *Políticas de procesos internos*, *Código de ética* entre otros, como se puede apreciar en la figura 7.

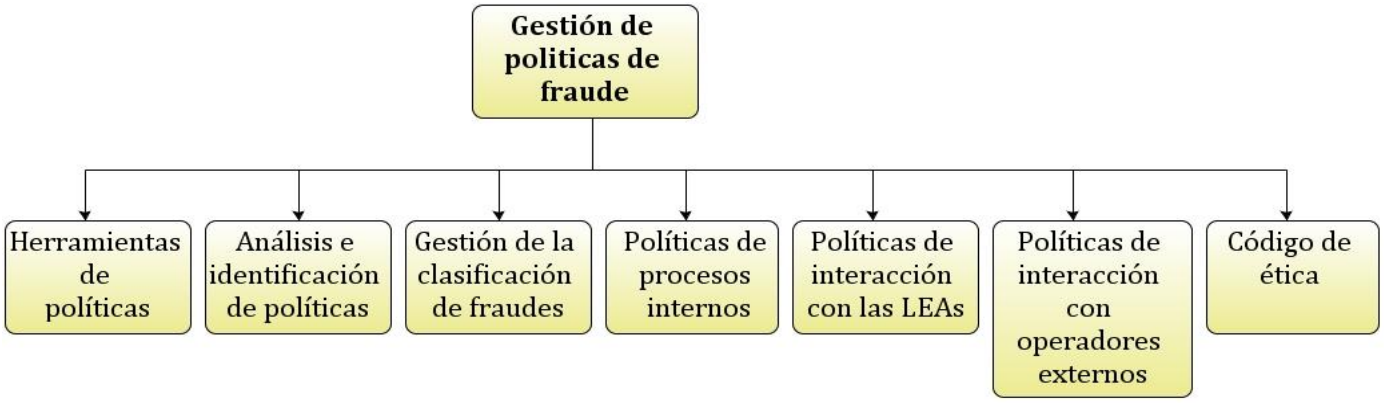


Fig. 7: Gestión de Políticas de Fraude. Procesos de Nivel 4.

2.3.2. Gestión de Operaciones de Fraude.

Representado como el segundo grupo de procesos a ejecutar, es el núcleo funcional y donde tienen lugar el grueso de las operaciones. En este juegan un papel activo y se maneja información fundamental como, el equipo encargado de la detección, investigación, resolución, cuantificación de daños y acciones de prevención para hacer frente a sospechas, actividades y entidades fraudulentas. Las operaciones y la información que comprende lo hace responsable por la protección del negocio de existentes y futuras amenazas. También provee comunicación mediante audiencias internas y externas de las actividades de fraude jugando un papel importante en la educación del personal y la prevención del fraude en otras empresas del sector. Se encuentra subdividido en tres principales áreas como: *Información y Procesamiento de Datos*, *Análisis de Fraude* y *Acciones de Fraude*. Estos a su vez comprenden una secuencia de acciones necesarias para el logro de los objetivos propuestos, como se puede apreciar en la figura 8.

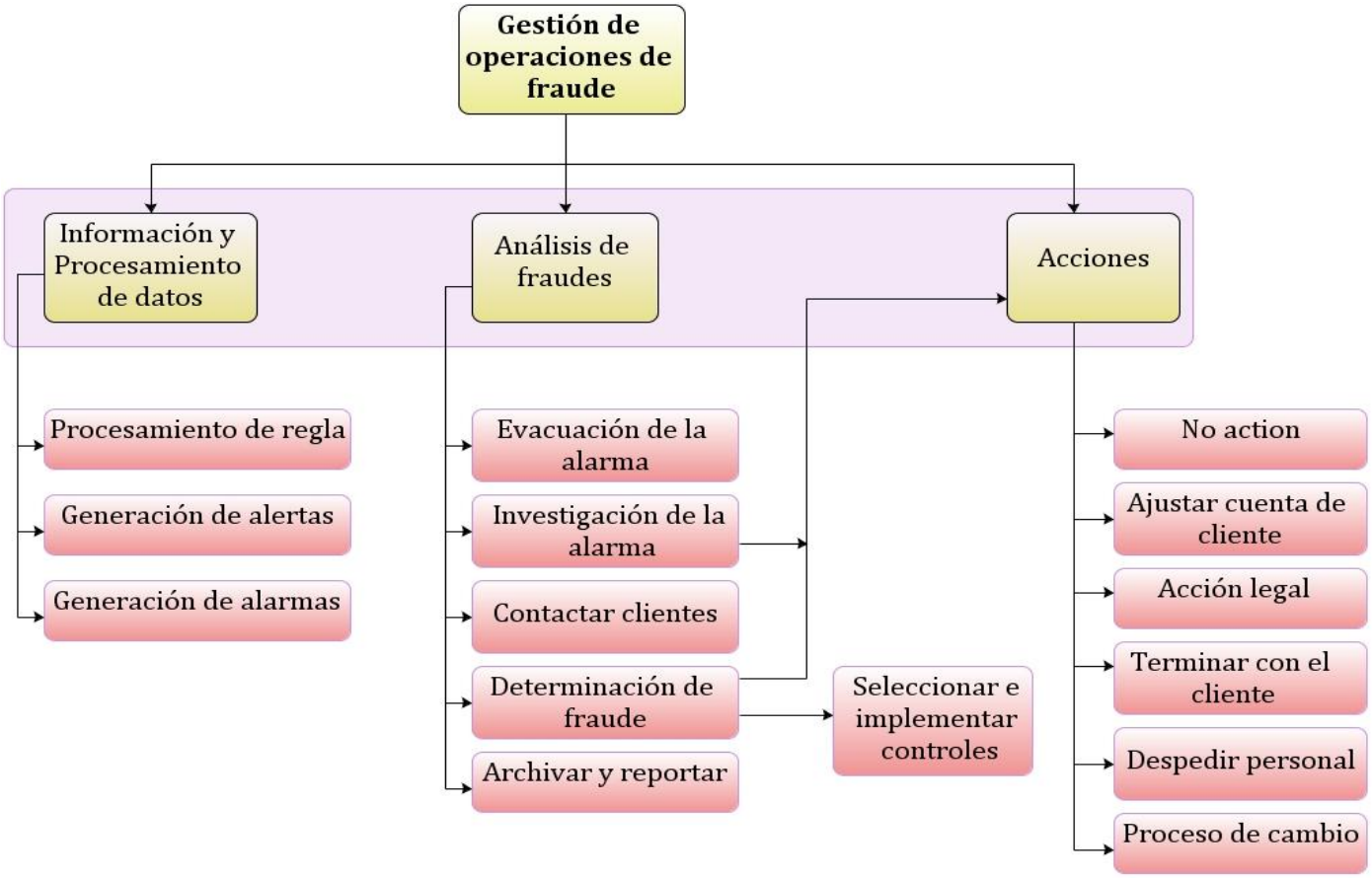


Fig. 8: Operaciones de Fraude. Procesos de Nivel 4.

2.3.3. Soporte de Operaciones de Fraude.

El Soporte de Operaciones comprende funciones que permiten la prevención y detección de fraude, así como soporte para la adopción de prácticas para la reducción de amenazas. Pretende el alcance de sus objetivos mediante la recolección y análisis de información, monitoreo del negocio incluyendo la gestión del aprendizaje y desempeño de los procesos de negocio. La *Recolección de Inteligencia*, *Prevención y Reducción de Amenazas* y *Gestión de la Configuración del Sistema*, forman parte de un acertado proceso de retroalimentación, análisis, colaboración y uso de la información compartida por otros proveedores de servicios.

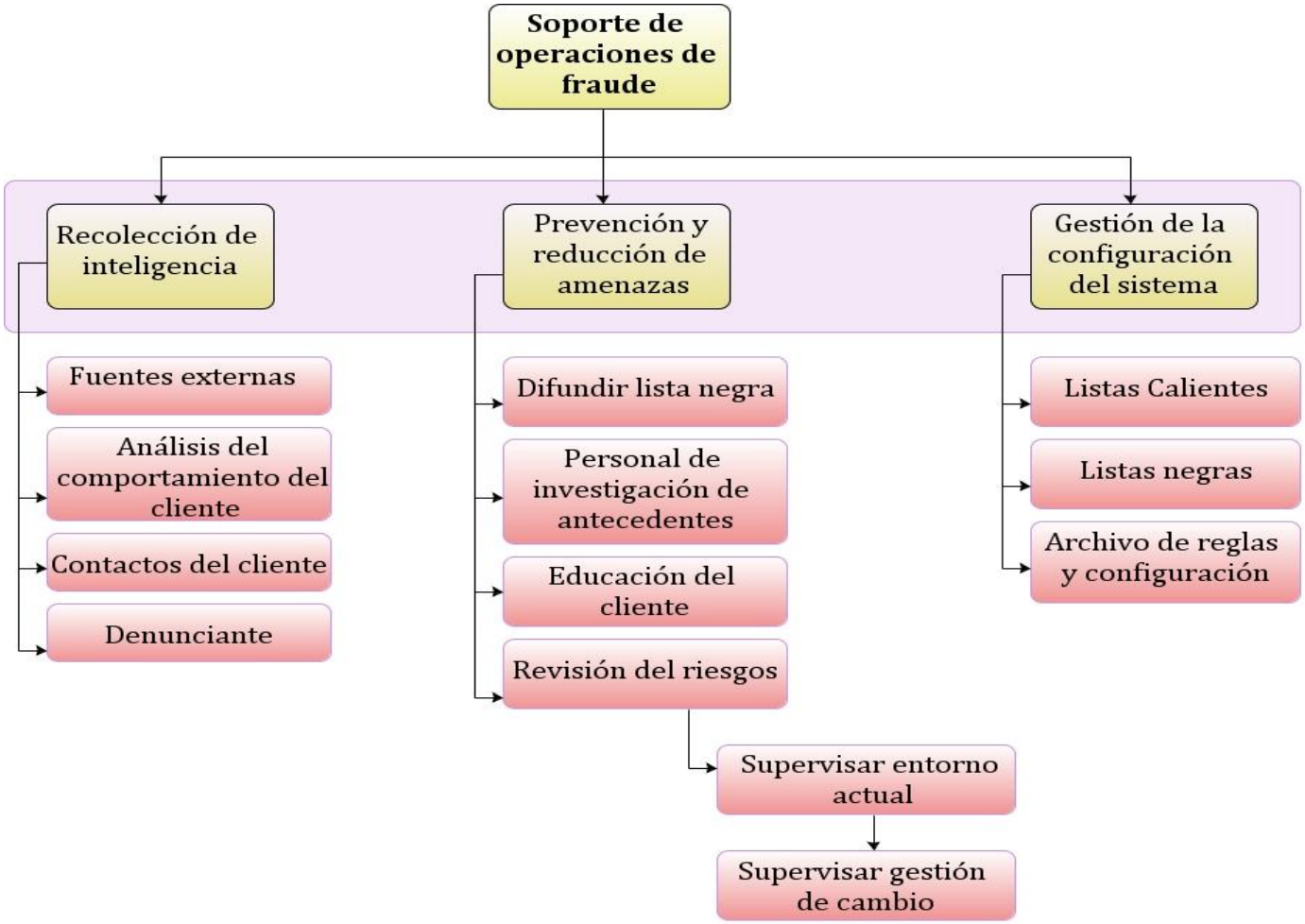


Fig. 9: Operaciones de soporte. Procesos de Nivel 4

2.4. ABEs incorporadas al Modelo SID

A partir de este momento se está en la capacidad de definir la información necesaria, basado en el análisis previamente efectuado sobre la descripción obtenida del eTOM para la Gestión de Fraude y la investigación realizada sobre la ejecución de este proceso actualmente en ETECSA, empresa que hará uso de los resultados obtenidos y que será el escenario para la validación de la propuesta.

Como resultado son creadas tres ABEs como se muestra en la figura 10, teniendo como objetivo la agrupación de las entidades, funciones y relaciones presentes, atendiendo a sus características y su aporte en la ejecución del proceso como parte de la Gestión Empresarial.

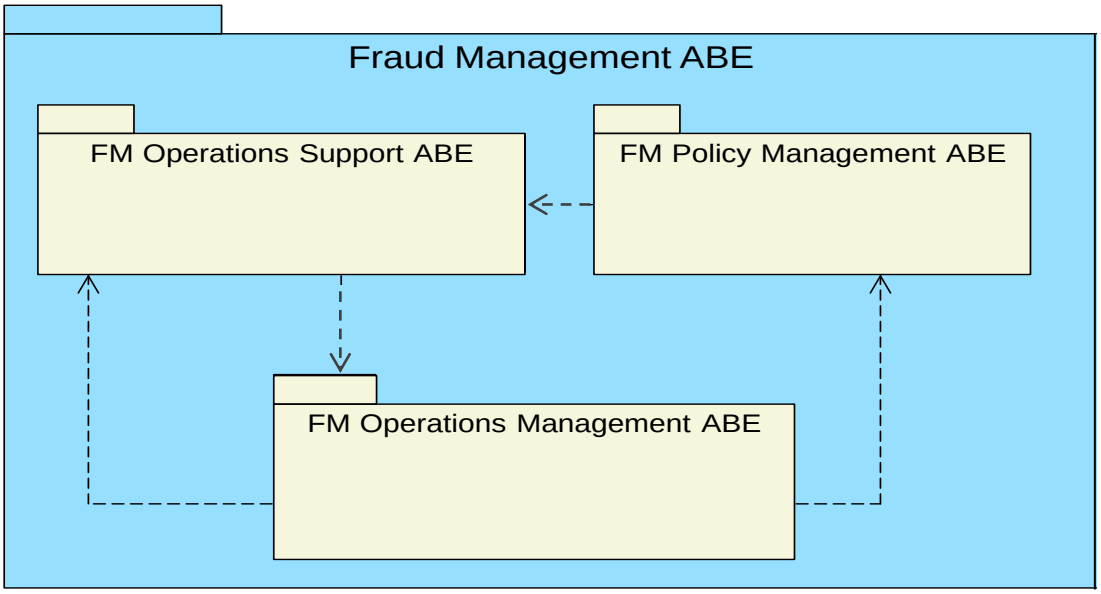


Fig. 10: Interacciones entre ABE pertenecientes a la Gestión de Fraude.

Las interacciones entre la información y operaciones contenidas en cada ABEs perteneciente al SID forman un modelo eficiente para la Gestión de Fraude, adaptable a las necesidades y características de cada empresa, garantizando el mantenimiento de la eficiencia y viabilidad mediante la retroalimentación. Se observa al ABE *Operations Management* como contenedor para el grueso de las actividades y centro de las operaciones con *Policy Management* y *Operations Support* como soportes para la realización del proceso.

Enfocado hacia la construcción del dominio empresarial y debido a la incorporación en el modelo SID del resultado obtenido, se tiene una nueva visión del modelo de paquetes mostrado en la figura 5, quedando de la siguiente manera.

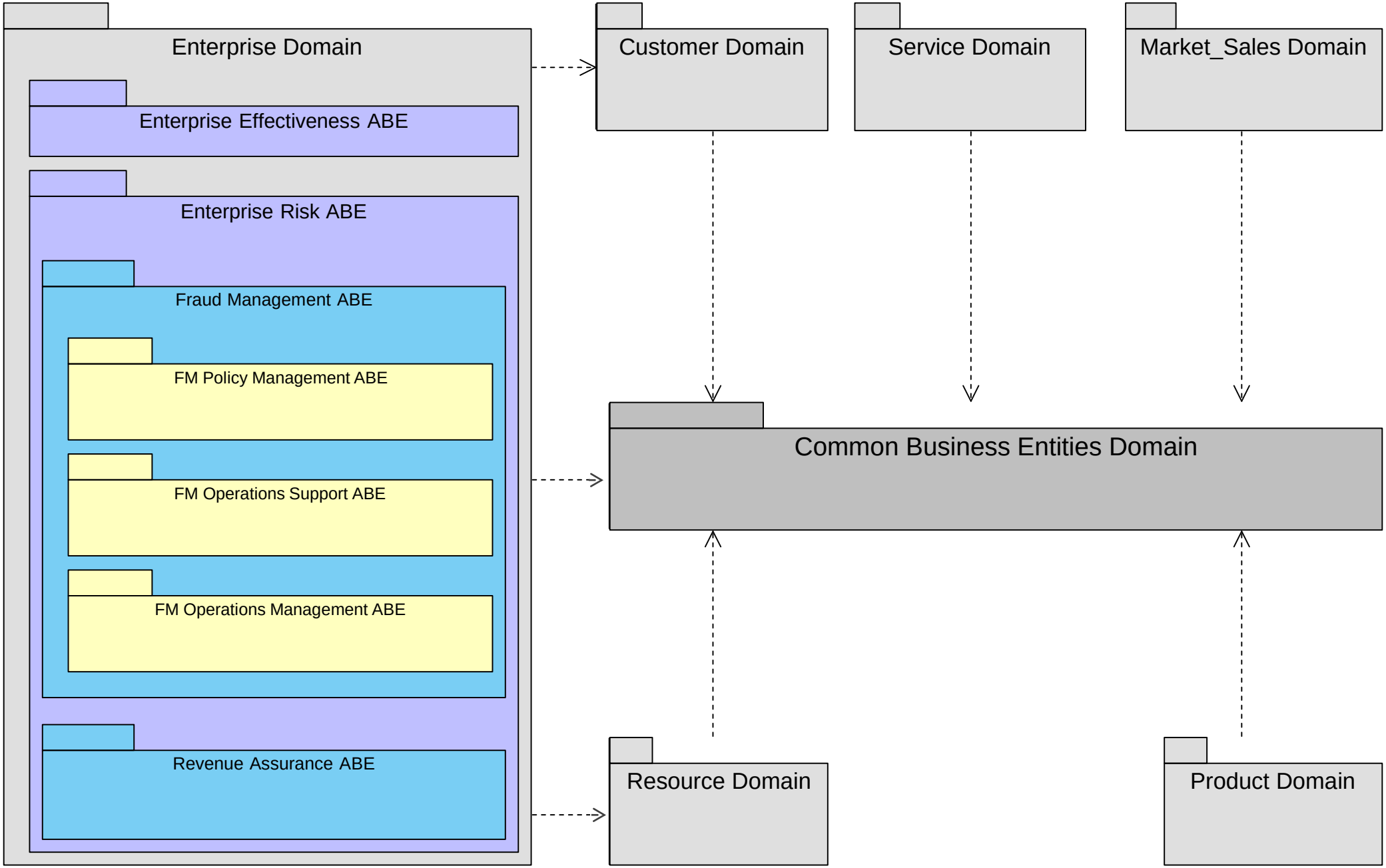


Fig. 11: Modelo de paquetes SID R9.0.

***Nota**: Una explicación más detallada sobre el resultado anterior se realizará en el capítulo 3.*

2.5. Pautas para la creación de nuevas entidades.

Para llevar a cabo el análisis del SID y la creación de las entidades que formarán parte de las ABEs mencionadas anteriormente, es necesario tener en cuenta un conjunto de pautas y buenas prácticas necesarias para el trabajo con el SID y el modelado de los datos.

2.5.1. Entidad / Especificación de la Entidad.

Patrón usado a través de todo el modelo de datos. Este patrón permite establecer los atributos invariantes, métodos y relaciones de las entidades creadas. Este patrón no debe ser aplicado a ABEs existentes pero si debe tomarse en cuenta a la hora de agregar nuevas entidades o detallar una existente que aún no ha sido desarrollada. Además garantiza que prevalezca la propuesta de ciertos datos que se consideren imprescindibles dentro del modelo.

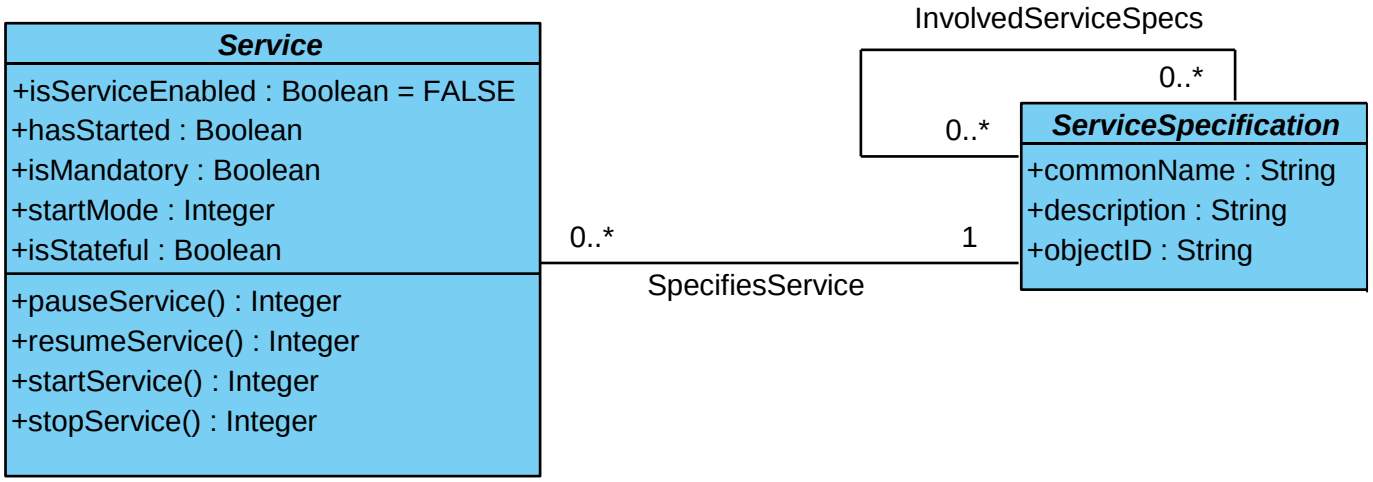


Fig. 12: Ejemplo de la Pauta: Entidad / Especificación de la Entidad.

2.5.2. Entidad / Rol de la Entidad.

Se hace uso de este patrón debido a que varias de las entidades presentes dentro del modelo toman diferentes roles durante su ciclo de vida, por ejemplo, una entidad puede ser empleado, un cliente o un proveedor de servicios. Es decir, la misma información puede estar presente en un proceso realizando diferentes actividades. El uso de este patrón se ilustra a continuación mediante el modelado de las partes involucradas que maneja el SID actualmente. El análisis del siguiente diagrama modelado dentro del SID juega un papel importante dentro del resultado final de la investigación, por lo que se recomienda que sea analizado exhaustivamente.

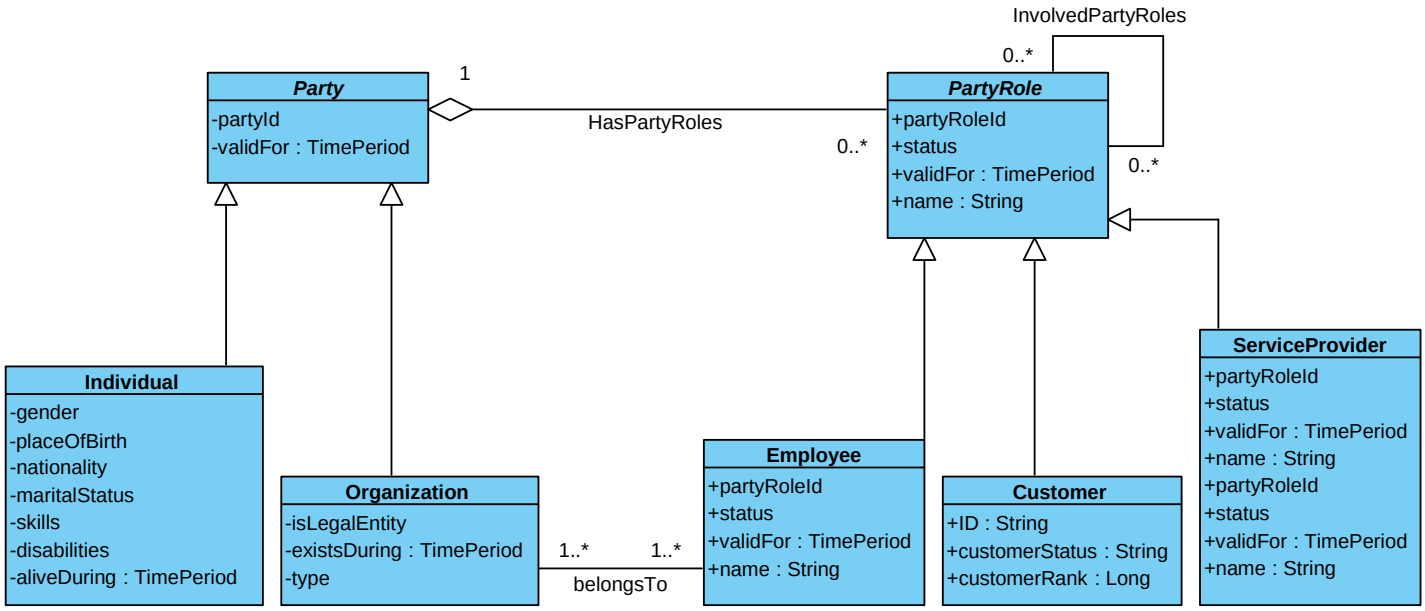


Fig. 13: Ejemplo de la Pauta: Entidad - Rol de la entidad.

2.5.3. Características de la especificación de la entidad / Características de la entidad.

En la construcción de cualquier modelo es casi imposible identificar todos los atributos que definen la entidad de negocio. Incluso si los atributos son añadidos siempre existirá la necesidad de añadir información acorde a las necesidades de cada cual, mediante el uso y extensión del modelo. La pauta utilizada brinda flexibilidad y capacidad para la gestión de la información y servicios ofertados por la empresa.

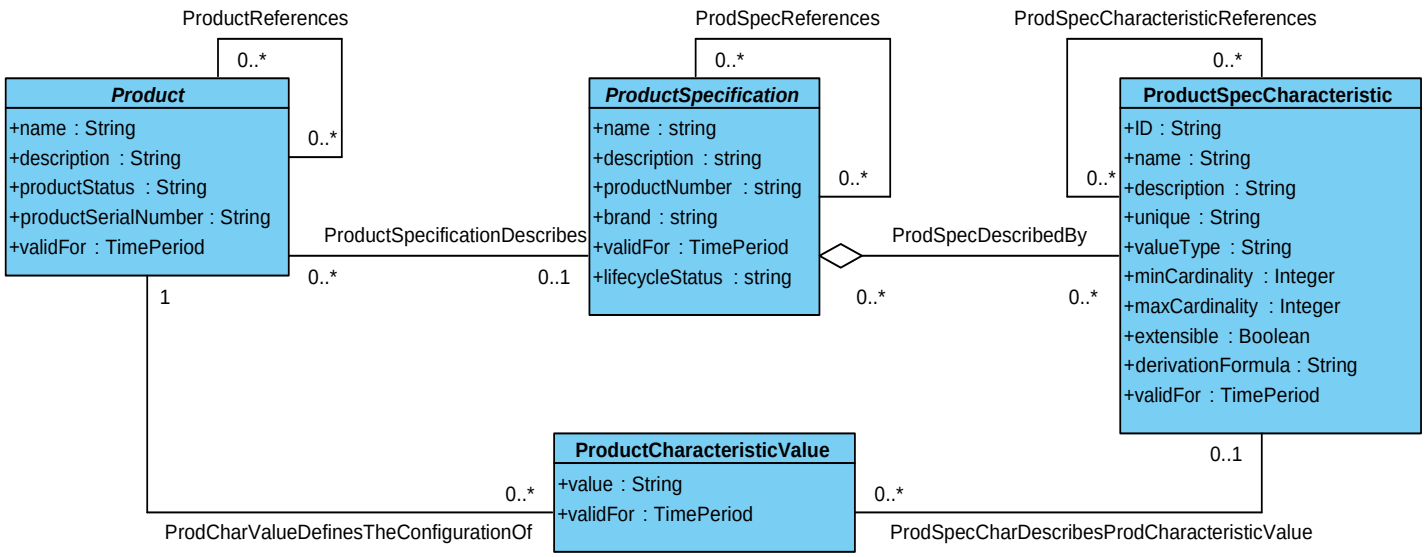


Fig. 14: Características de la Especificación / Características.

2.6. Pautas para la extensión de entidades existentes.

Los patrones descritos a continuación deben ser usados a la hora de extender un ABE existente dentro del modelo, esto garantiza que la estructura del SID y su contenido no se vea comprometido por el uso de la comunidad. En caso de que el SID sea objeto de cambio, la utilización de estas pautas minimiza su impacto sobre extensiones desarrolladas.

2.6.1. Creando paquetes contenedores para las extensiones.

La manera de organización en paquetes permite el soporte a nuevas versiones del modelo SID, organización y movilidad hacia otros modelos. Este paquete contendrá todas las entidades, relaciones y asociaciones incorporadas para extender el modelo SID.

Los pasos a seguir en correspondencia con las pautas que propone Frameworx son los siguientes:

1. Crear el paquete contenedor dentro del ABE que se desea extender.
2. Nombrar con el mismo nombre del ABE donde estará contenida, agregando el sufijo "*Extensions*".

2.6.2. Adicionando atributos.

Los atributos no deben ser directamente agregados. Para ellos se utilizan subclases que contendrán la información que se desea añadir. Estas subclases heredan todos los atributos y asociaciones procedentes del SID manteniendo así la integridad del modelo. El nombre de la entidad creada debe mantener el nombre, agregando el sufijo "*Extension*", otra alternativa es agregar el sufijo "*Specialization*". Por su parte

el nombre del atributo debe ser claro y estar en correspondencia con la información que representa, evitando ambigüedades en cada caso. Ejemplificando lo anteriormente explicado tenemos que, una entidad con nombre *"Employee Extension"* sería el resultado de extender la entidad existente dentro del SID *"Employee"*

2.6.3. Adicionando entidades.

De la misma forma que cuando se desean agregar atributos, cuando se realiza el proceso de añadir una nueva entidad, este no debe hacerse directamente al ABE existente. En la figura 15 mostrada a continuación queda plasmado la forma en que fueron agregadas nuevas entidades como es el caso de *EmployeeCharge* y *EmployeeLevel,* además de incluir nuevos atributos necesarios para el uso de la entidad ya existente dentro del SID, *Employee* a través de *EmployeeExtension*.

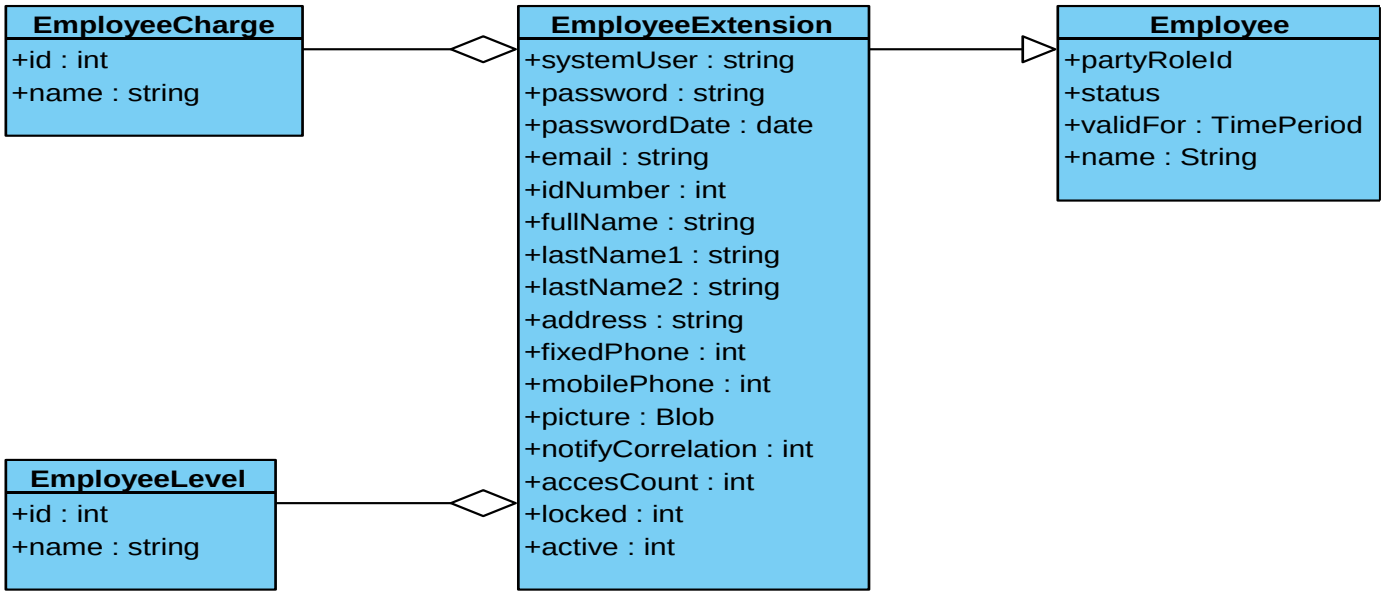


Fig. 15: Ejemplo que agrupa las pautas para la extensión de entidades.

2.6.4. Relacionando entidades.

Las relaciones pueden ser añadidas sin restricción alguna, siempre y cuando sea especificado el papel que juegan mediante una corta descripción que contenga al menos el nombre de una entidad acompañado de información que refleje su razón de ser. En la figura 14 se muestra un ejemplo de realizar

este proceso, si es observada la relación establecida entre las entidades *Product* y *ProductSpecification* serán evacuadas todas las dudas al respecto.

2.6.5. Nomenclatura en el dominio Gestión Empresarial.

En el caso de las entidades que pertenecen al dominio de Gestión Empresarial es importante aclarar la nomenclatura que es usado en el mismo. Manteniendo todas las pautas anteriormente descritas se añade un detalle particular. Las entidades de esta área posee el prefijo que identifica al ABE a la que pertenecen. Como ejemplo tenemos el ABE ***R**evenue **A**ssurance*, en este, las entidades presentes poseen el prefijo **RA.** De igual manera a la hora de insertar las entidades que conformaran la Gestión de Fraude estas contendrán las iniciales **FM** incluida en su nombre, por las iniciales de las palabras que en inglés conforman el nombre del ABE (***F**raud **M**anagement*) siguiendo así las pautas utilizadas por la comunidad para el desarrollo de Frameworx.

2.7. Conclusiones

El trabajo en el presente capítulo arrojó un minucioso estudio y conocimiento sobre los dominios que componen el SID, el análisis de las dependencias existentes entre el domino empresarial y los restantes, necesarios para dar solución a la problemática en cuestión, la identificación de las ABEs que hasta el momento no existían en el área de Gestión de Fraude, los pasos y pautas estudiadas para su correcta utilización y aplicación en la implementación de sistemas de soporte a las operaciones los cuales fueron de gran utilidad, proporcionaron un mayor dominio del SID y una manera adecuada de modelar y estructurar el contenido generado por la investigación. Por todo lo anteriormente expuesto, se está en condiciones de definir las entidades y relaciones que darán solución a los problemas de fraude existentes. Este capítulo crea las bases para la utilización del SID, para la agrupación de entidades, atendiendo a su razón de ser, dentro del modelo, manteniendo una estructura estandarizada y modular. Para el trabajo con el componente de Frameworx, se han definido un conjunto de buenas prácticas, que manejan el cambio hacia futuras versiones o corrección de errores, minimizando el impacto que estas puedan tener sobre proceso de negocio desarrollado y que mantienen la flexibilidad y adaptabilidad de modelo.

CAPÍTULO 3: PROPUESTA DE SOLUCIÓN

3.1. Introducción

El modelado de la información, incluyendo la descripción de los elementos presentes en cada uno de los artefactos creados y de cada uno de los recursos introducidos o utilizados del SID, constituyen y justifican los resultados esperados a estas alturas de la investigación. El SID ha sido examinado minuciosamente y del eTOM, apoyado en los procesos antifraudes ejecutados en ETECSA se ha extraído la información necesaria para dar una propuesta de solución ajustada a los requisitos necesarios propuestos por Frameworx.

3.2. Propuesta del Modelo de Datos.

El trabajo realizado, enfocado en el SID y los procesos proporcionados por el eTOM además de la información recopilada en ETECSA, han arrojado un conjunto de entidades y relaciones que están presentes en los procesos de Gestión de Fraude. Para ello se han seguido las pautas propuestas y se ha mantenido la integridad y flexibilidad del modelo, además de su alineación con los procesos del eTOM. La construcción del ABE Gestión de Fraude constituye un paso importante en el desarrollo de la Gestión Empresarial y del SID en general.

3.2.1. Modelado de la información.

El modelado de la información realizado en el presente epígrafe es el resultado del análisis de los procesos de Gestión de Fraude proporcionados por el eTOM, expuestos anteriormente en la figura 6 y la información recopilada mediante la entrevista a los analistas de fraude de ETECSA dedicados a esta tarea actualmente. El estudio del modelo de datos brindado, evitó que se cometieran errores en el proceso como violación de la estructura y nomenclatura del modelo, la existencia de información redundante e incompatibilidad entre el eTOM y el SID.

Durante el análisis de la propuesta de solución se verán involucradas entidades, las cuales debido a su magnitud e implicación en los procesos de Gestión de Fraude son objetos de un modelado adicional. Estas entidades son: *FMFraudTeam*, *FMAction*, *FMFraudType*, *FMPenalty*, *FMInvestigationProcedure*, *FMSupportInformation*, *FMSupportData*, *FMCase* y *BusinessInteraction* y pueden ser visualizadas en el anexo de la investigación.

3.2.1.1. ABE Gestión de Políticas de Fraude

Análisis e identificación de políticas.

El siguiente flujo de información y relaciones representado, pretende abarcar la información necesaria para dar solución a las tareas de análisis e identificación de políticas. La razón de ser de dichos procesos es mantener las mejores prácticas para el análisis de fraude y el trabajo de identificación a partir del análisis y recopilación de inteligencia dando soporte a los trabajos de investigación. Establece criterios para determinar cuándo un determinado caso es en realidad fraude incluyendo los procedimientos para ello.

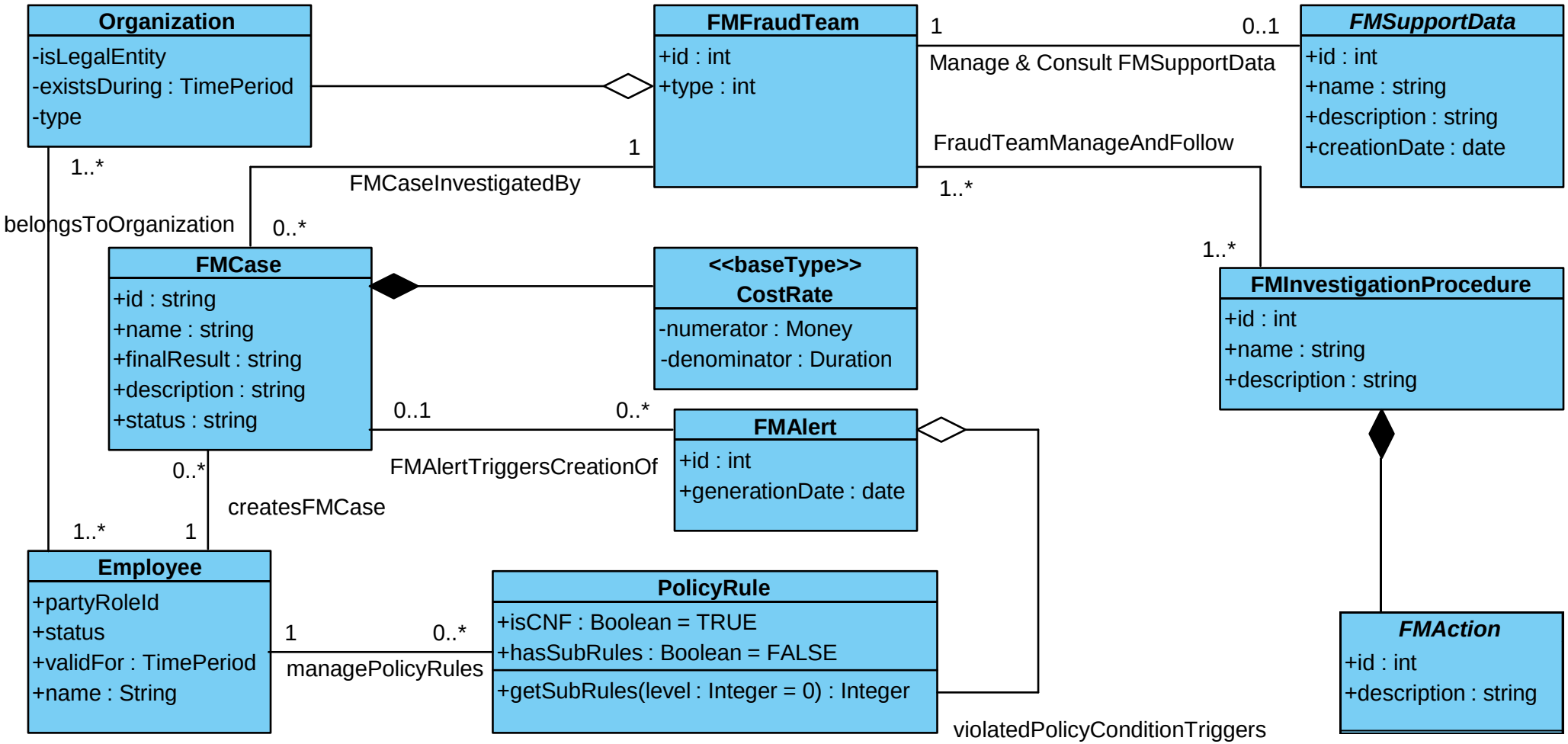


Fig. 16: Análisis e identificación de políticas.

Gestión de la clasificación de fraude.

La gestión de la clasificación de fraude constituye un aspecto fundamental como parte de la Gestión de políticas para las acciones antifraude. Este grupo de procesos funcionan como un repositorio para las clasificaciones de fraude existentes, identificadas internamente o recopiladas mediante el análisis de la información compartida por otras instituciones. Sus principales objetivos se centran en la gestión eficiente de información acerca de clasificaciones de fraude y prácticas de detección; definiendo acciones, procedimientos e interactuando con otros agentes dentro de la industria. Estos procesos son críticos para el éxito de cualquier programa de protección contra fraude.

Para este proceso se recomienda el análisis del anexo representado en la figura 35, el cual complementa el flujo modelado a continuación, especificando la información que maneja la entidad *BusinessInteractions* para la Gestión de Fraude.

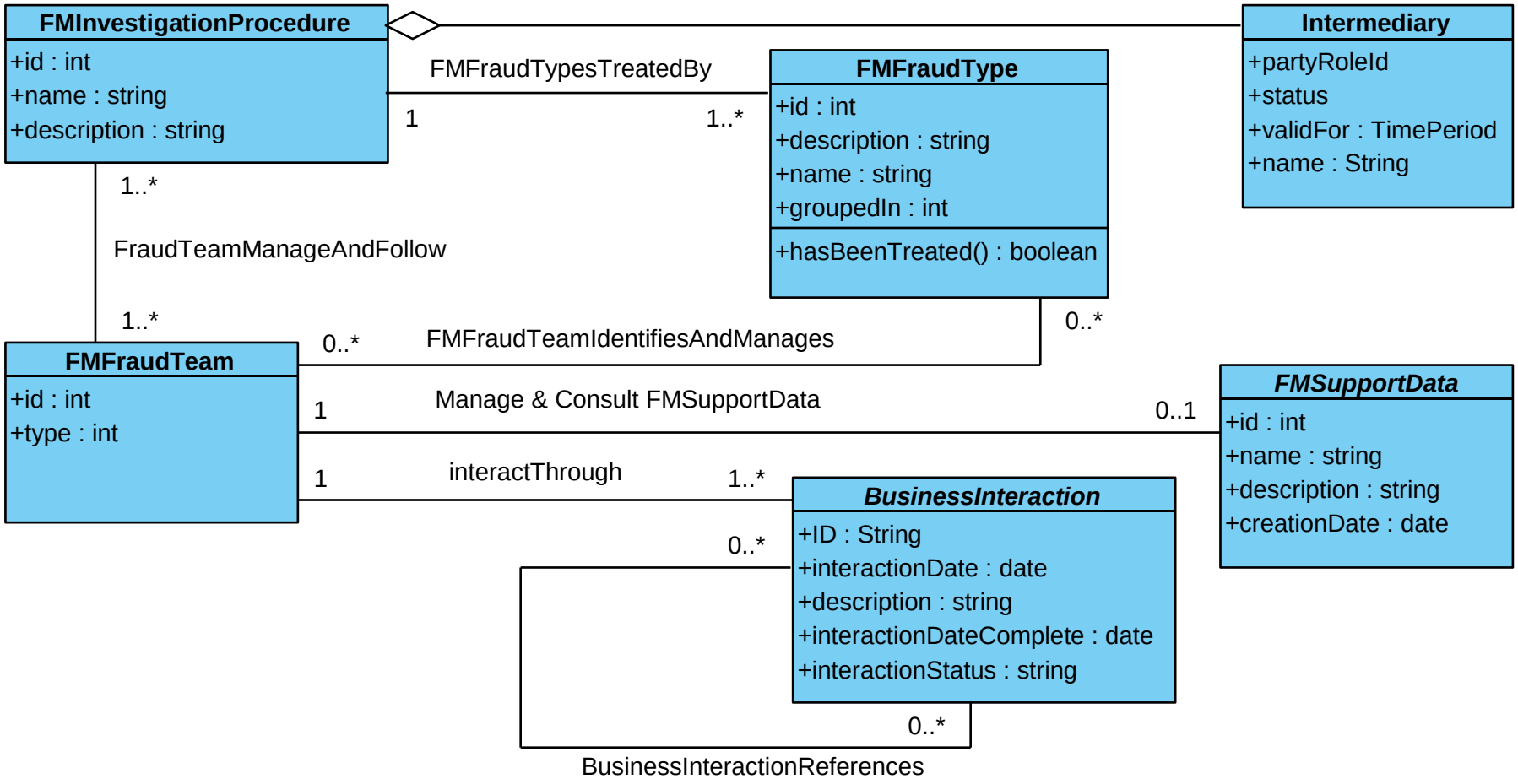


Fig. 17: Gestión de la clasificación de fraude.

Procesos internos y Código de Ética.

La información definida a continuación intenta describir las pautas para el comportamiento de todas aquellas personas dentro y fuera de la empresa así como la interacción con agentes externos como parte de los procesos de investigación. Son realizados por lo tanto, métodos y procedimientos a seguir,códigos de ética u otro soporte, registrando el dominio y aprobación del empleado o asociado. Con estas acciones se establece una guía imprescindible para el buen funcionamiento de la empresa y se garantiza que en caso de violaciones o procedimientos erróneos, la entidad cuente con los recursos pertinentes y esté en condiciones de aplicar un adecuado tratamiento.

En este caso se recomienda el análisis del anexo representado en la figura 31, el cual complementa el flujo modelado a continuación, especificando la información que maneja la entidad *FMPenalty*.

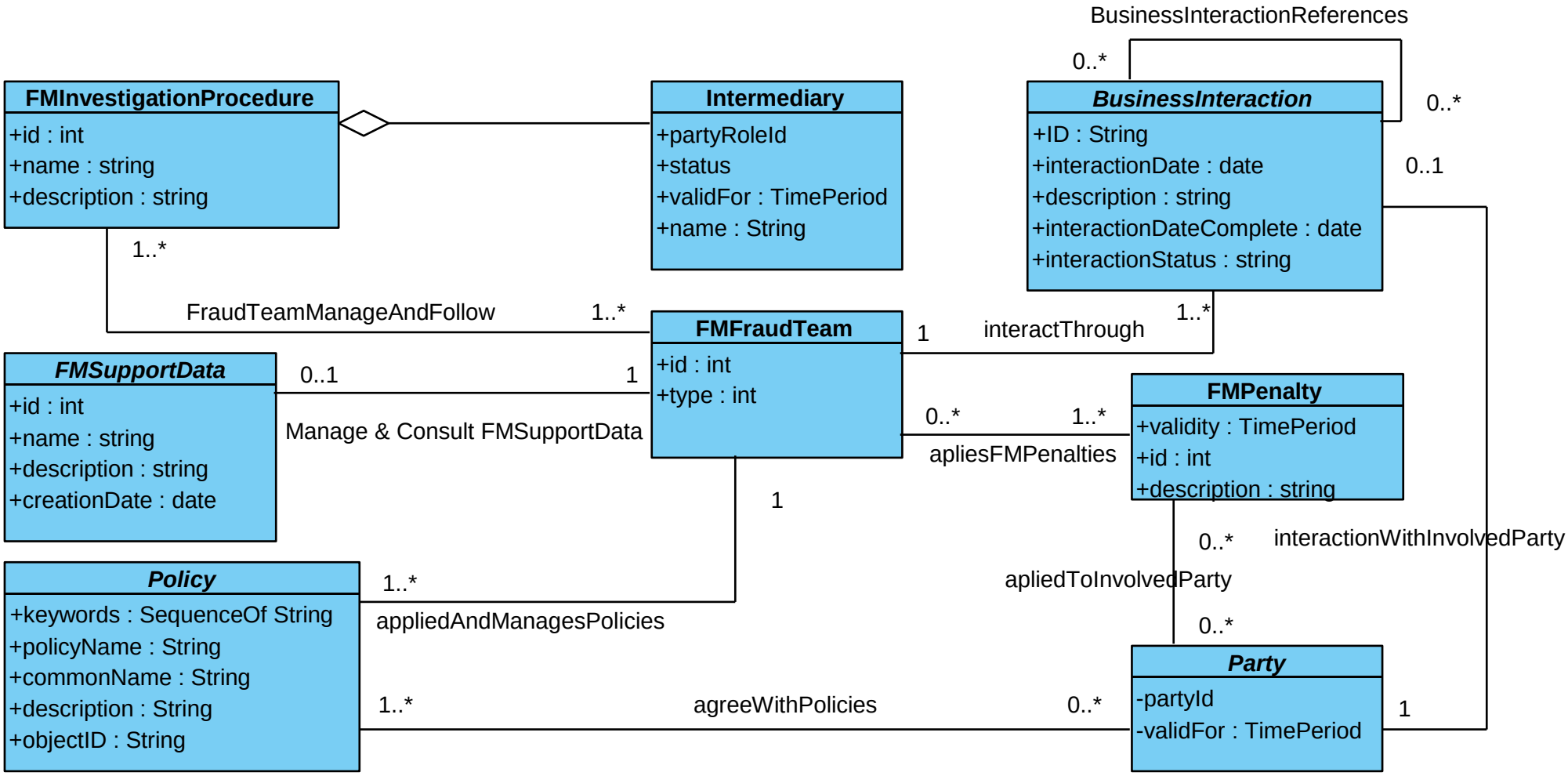


Fig. 18: Procesos internos y Código de ética.

Políticas de interacción con las Agencias Legales (LEA: por sus siglas en inglés).

Los equipos de fraude deben definir en sus procedimientos, requisitos en los cuales las agencias legales, manejadas como (*LEA: del inglés Law Enforcement Agency*) deban intervenir. Aquellos casos en los que una simple interrupción del servicio no es suficiente debido a su magnitud, realizando acciones ya sea para apoyar el proceso de investigación o para culminarlo. Los criterios bajo los cuales dichas agencias deben tomar parte pueden depender del alcance del fraude, daños a la empresa o pérdidas económicas. En otros casos para determinar todas las personas involucradas en la ejecución del fraude. Los departamentos del fraude deben tener definidos los contactos necesarios dentro de las agencias legales y proporcionar información recopilada sobre el caso en cuestión, sin violar las restricciones de confidencialidad de la empresa para con los clientes formando parte del proceso de interacción.

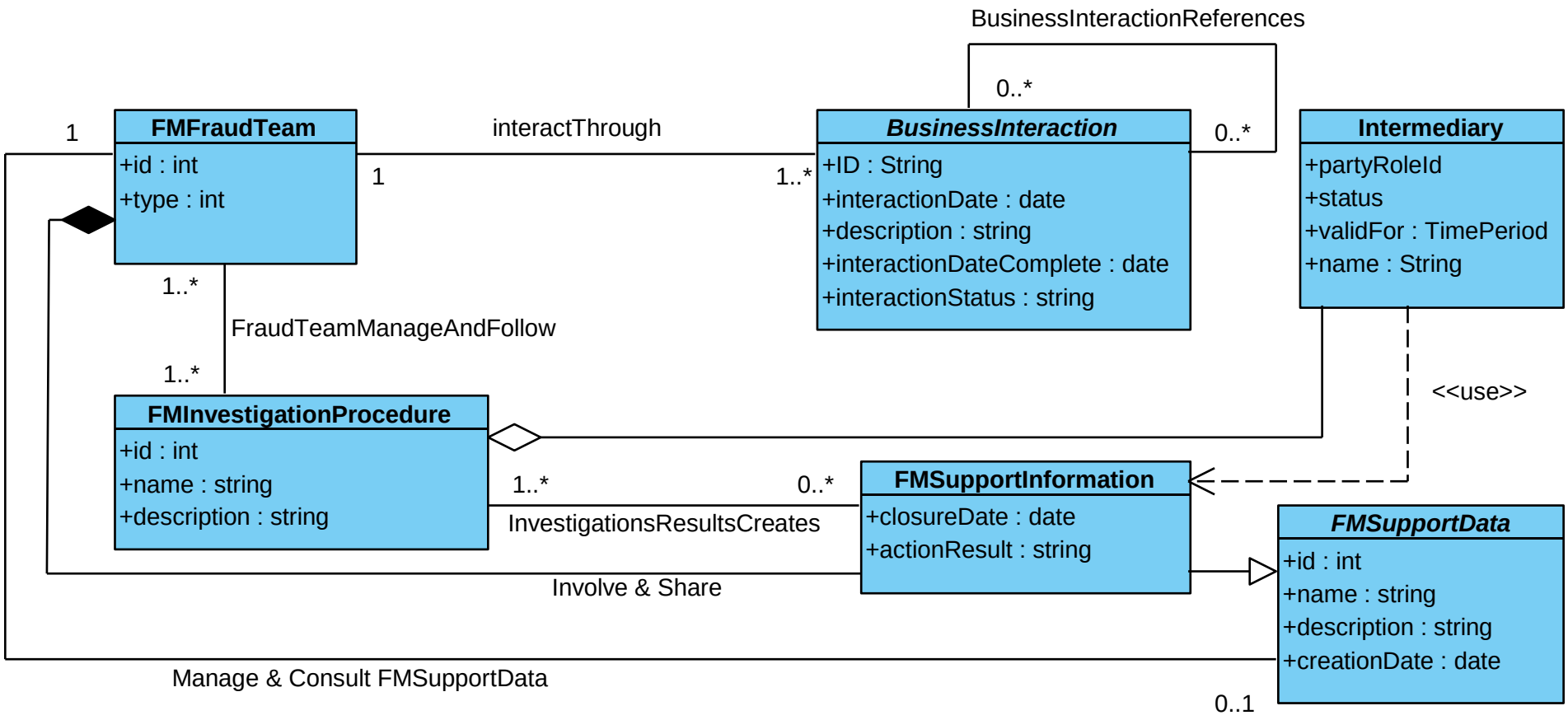


Fig. 19: Políticas de interacción con las Agencias Legales.

3.2.1.2. ABE Gestión de Operaciones de Fraude.

Información y procesamiento de datos

El proceso relacionado con el procesamiento de información y datos para la detección de fraude consiste en el análisis constante del tráfico de información generado, verificando en cada caso el cumplimiento de las reglas establecidas por el equipo antifraude, para detectar posibles amenazas. Como medidas de prevención y detección, son generadas y reciben el adecuado tratamiento, las alertas, alarmas y casos que son investigados a fondo como posibles fraudes. Como parte de este proceso las notificaciones pueden ser tenidas en cuenta como una especie de alerta, relacionada a factores ajenos al tráfico como peticiones de inicio de un determinado proceso o de información requerida fuera del sistema, la realización de un determinado reporte entre otros.

Es fundamental esclarecer que los casos *FMCase* pueden ser creados con la aparición de solo una alerta *FMAlert*, la violación de una política *PolicyRule* relevante para la empresa puede inmediatamente desencadenar una profunda investigación como medida proactiva. Esto está en dependencia de la vía de implementación que se decida emplear para la automatización de este proceso.

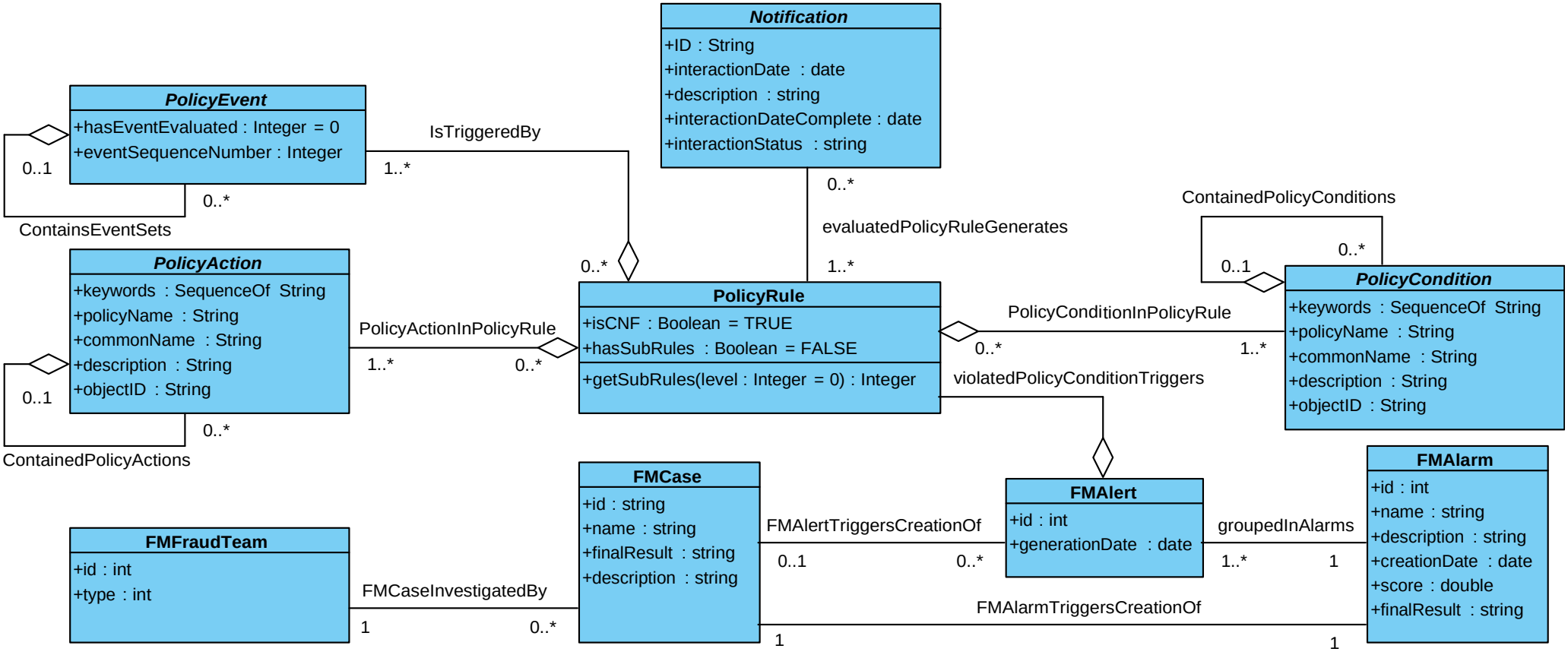


Fig. 20: Información y procesamiento de datos.

Análisis de Fraude

El análisis de fraude comprende una serie de subprocesos para dar solución a los resultados arrojados por el procesamiento de los datos e información, como resultado de aplicar los controles y reglas establecidas para el análisis del tráfico de datos generado. El modelo desarrollado a continuación, representa la información que interviene en el proceder del equipo de fraude para dicha tarea. Se enfoca principalmente en los procedimientos empleados, recopilación y consulta de información, brindando soporte a los procesos de análisis de tipos de fraudes, conformación de casos y seguimiento de alarmas y alertas por el equipo de fraude. La información generada, a partir de la ejecución de cada operación es registrada, garantizando la retroalimentación del sistema.

La estrecha relación entre el caso *FMCase* y la creación de expedientes *FMFile* propicia la inclusión de esta última entidad dentro del flujo e información presentado a continuación. Generalmente es necesario un análisis más exhaustivo para su creación formando parte del grupo de operaciones de soporte de operaciones para la Gestión de Fraude.

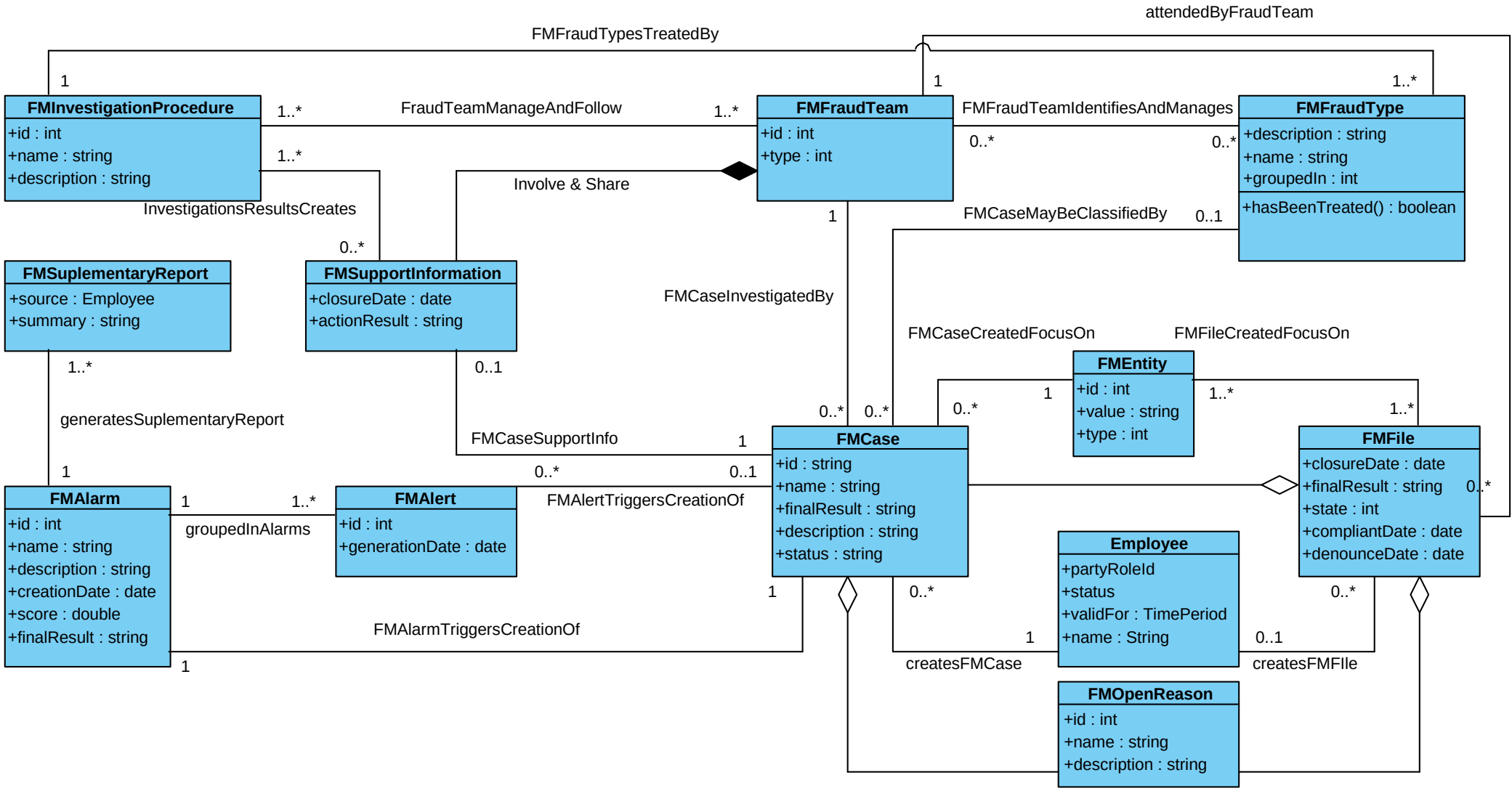


Fig. 21: Análisis de fraude.

Acciones antifraudes.

Las acciones de fraude constituyen el seguimiento inmediato al proceso de análisis de fraude. Generalmente acorde al resultado final de la investigación. Su carácter varía acorde a las características y datos obtenidos del análisis, siguiendo al pie de la letra los procedimientos de investigación establecidos. El final, dependiendo de las características y resultados que arroje dicho proceso conduce a una inmediata retroalimentación y actualización de los controles aplicados dentro de la empresa.

En este caso se recomienda el análisis del anexo presentado en la figura 28, el cual complementa el flujo modelado a continuación, especificando la información que maneja la entidad *FMAction*.

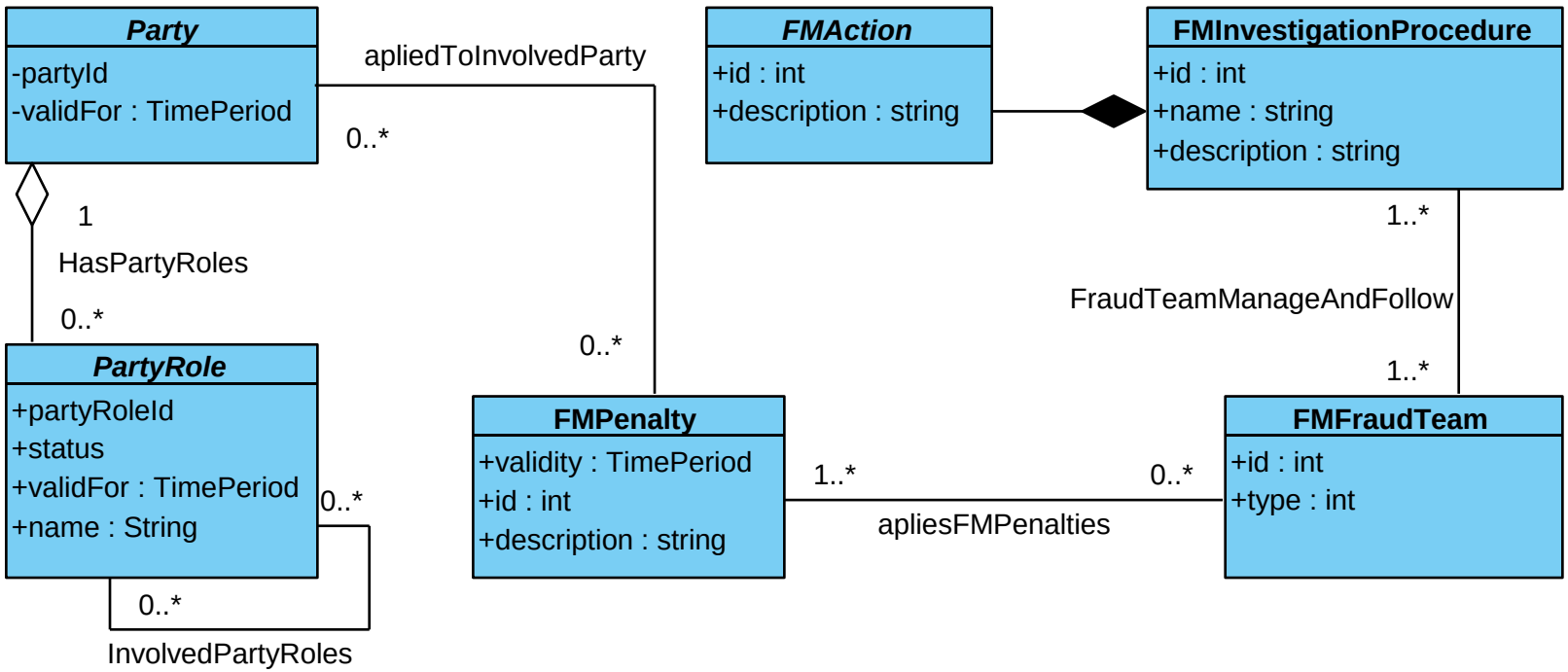


Fig. 22: Acciones antifraudes.

3.2.1.3. ABE Gestión de las Operaciones de Soporte

Recopilación de inteligencia.

Las acciones antifraudes no deben centrarse solo en las acciones e información a la hora de mitigar o eliminar un fraude una vez que este ocurra. Lo más importante para el proveedor de servicios es prevenir, implementar acciones proactivas, evitando que se ocasionen pérdidas económicas o brechas de seguridad. Es importante para ello la recopilación de información e inteligencia, haciendo uso de fuentes externas, analizando el comportamiento de los clientes, creando patrones a partir de tipos de fraudes identificados u otras medidas que permitan el fortalecimiento de los medios de protección contra fraudes. La implicación de los procesos de soporte garantiza integridad, seguridad entre otros. La visión que debe tener una empresa en cualquier entorno debe reflejarse también en su capacidad para evitar pérdidas o daños ocasionados por acciones fraudulentas.

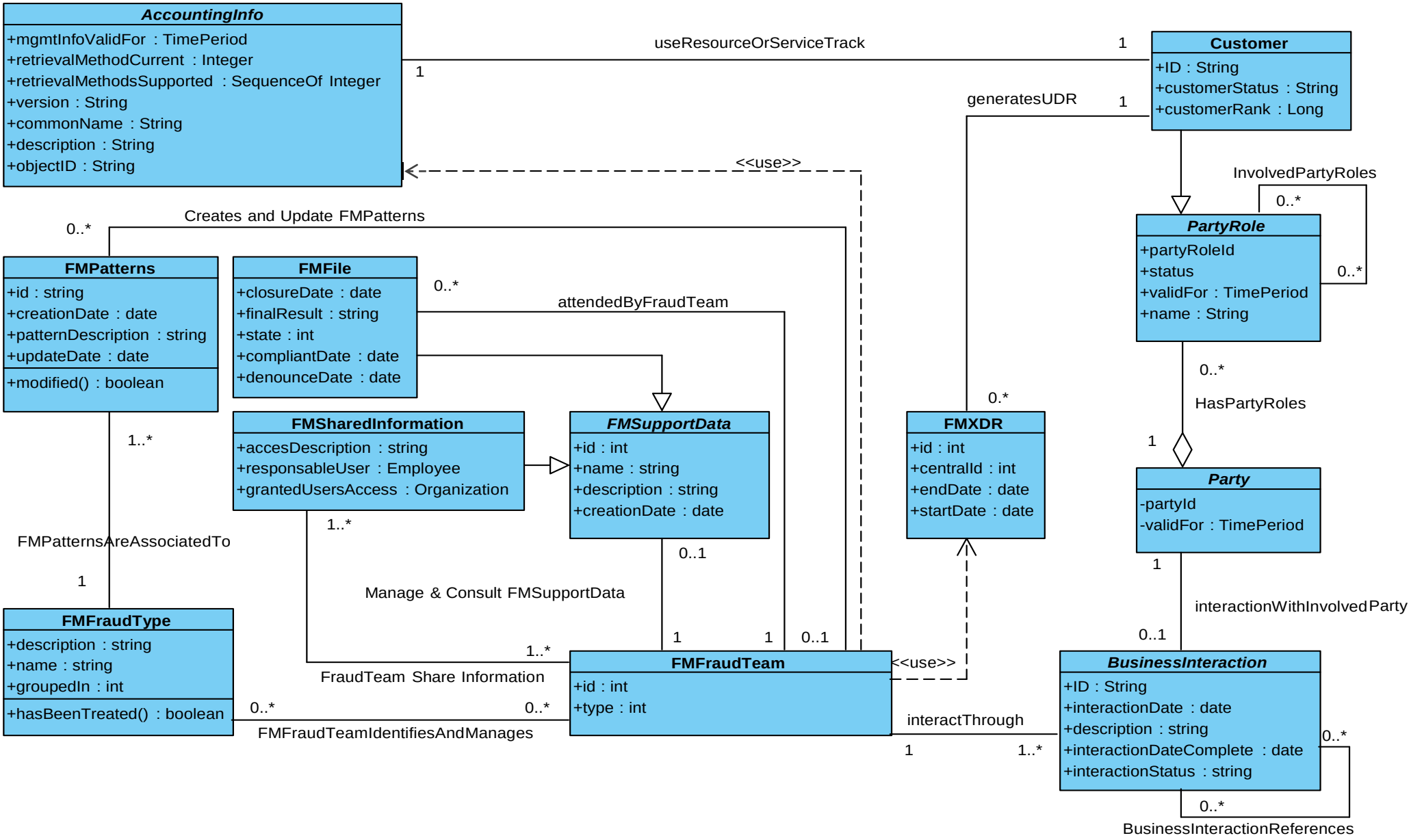


Fig. 23: Recopilación de inteligencia.

Gestión de la configuración del sistema

Por último y no menos importante hay que tener en cuenta la gestión de la configuración del sistema, responsable de generar, mantener e implementar toda la información, dígase listas, reportes suplementarios e información de soporte, indispensables para el correcto funcionamiento del programa antifraude. Estas entidades son las encargadas de registrar patrones de actividades y comportamientos que conducen a actividades fraudulentas, identidad de personas que han cometido fraude en alguna ocasión, reglas, fraudes detectados u otro tipo de información manejada.

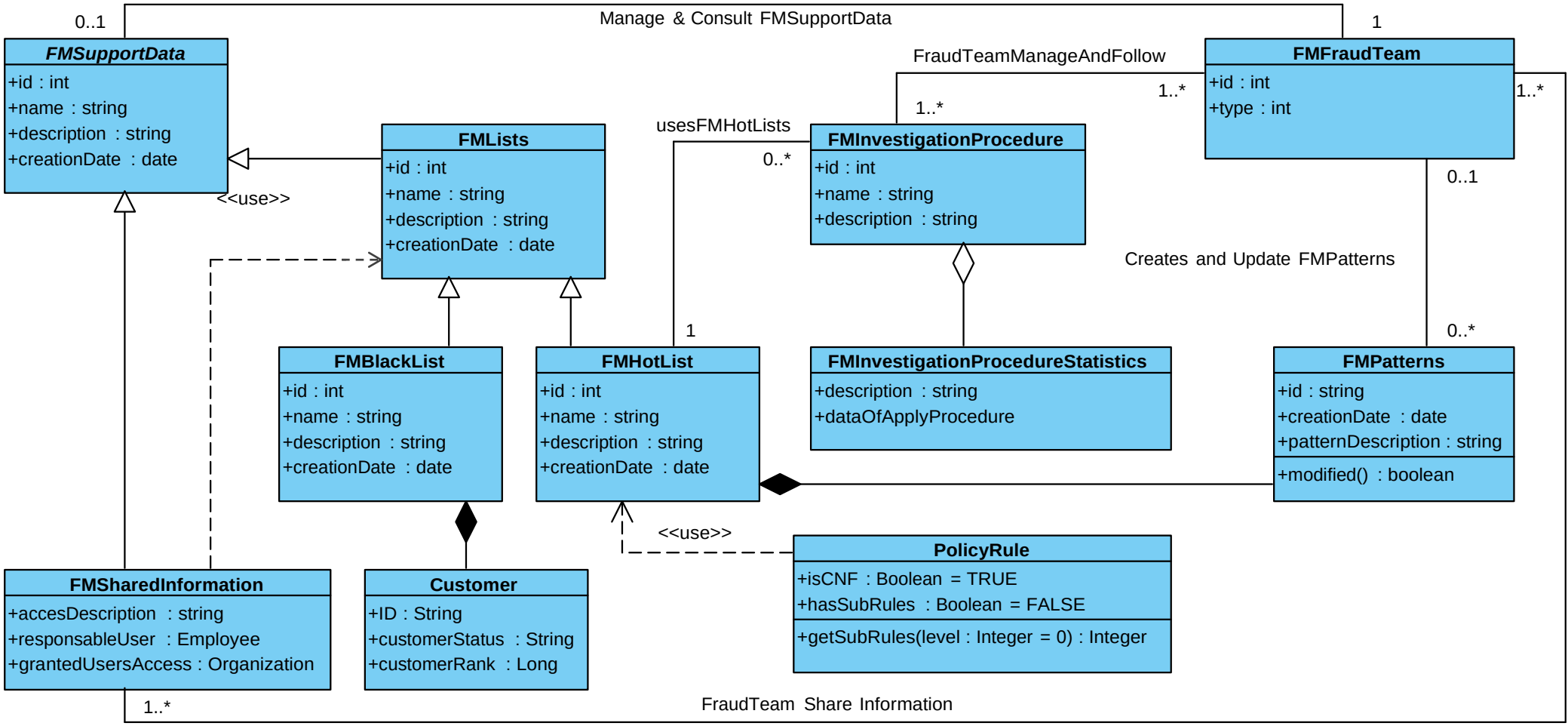


Fig. 24: Gestión de la configuración del sistema.

3.3. Descripción de las Entidades.

3.3.1. Entidades utilizadas, existentes dentro del SID

Activity

Entidad abstracta que representa una simple tarea en la ejecución de un proceso (12)

BussinessInteraction

Perteneciente al ABE *BusinessInteraction* del modelo SID, consiste en un acuerdo, contrato, comunicación o actividad conjunta entre uno o más partes involucradas, dígase tanto organizaciones como partes individuales, recursos o clientes. Existen 5 tipos de interacciones de negocio las cuales son *Requests*, *Response*, *Notification*, *Agreement* e *Instruction*. La relación *BusinessInteractionReferences* surge debido a que los distintos tipos de interacciones pueden estar relacionados con otras de este tipo, por ejemplo una petición (*Request*) de información a un proveedor de servicio debe estar complementada por otro tipo de interacción de negocio, en este caso una respuesta (*Response*) por lo que es necesario describir este tipo de interacción entre ellas mismas. (12)

Request

Entidad que abarca la información necesaria para que una petición sea realizada, generalmente involucra una entidad *Response* y es un tipo de *BusinessInteraction*. (12)

Response

Información que surge como respuesta a una entidad *Request*, es un tipo de *BusinessInteraction.* (12)

Notification

Es una especialización de la entidad *BusinessInteraction*, consiste en una especie de comunicación que informa que algo está pasando o que ocurrirá próximamente. Una *Notification* puede ser creada a partir de una petición (*Request*). La notificación típicamente es de un solo lado, o sea que se crea y no espera una respuesta. Por ejemplo, ante algún fallo del servicio la empresa puede enviar notificaciones a las partes afectadas por este. Es utilizado para tratar la ocurrencia de incidentes anómalos o violaciones del código de ética por parte de los empleados u otras personas involucradas en el proceso, también para prevenir el mal funcionamiento de un determinado dispositivo entre otros. (12)

Intermediary

Perteneciente al dominio *Party* ABE, no es más que uno de los roles con los que interactúa el proveedor de servicios, que cumple un papel de intermediario para alcanzar algún propósito. En este caso se utiliza para hacer referencia a las entidades legales que darán cobertura al negocio. Al hacer uso de la mencionada entidad se busca la flexibilidad en la interacción establecida. (12)

CostRate

Entidad perteneciente al dominio *Common Business* ABE, específicamente a las entidades bases, es usado para representar la pérdida monetaria. Se establece una correspondencia de costo por unidad de tiempo que permite priorizar las actividades sospechosas detectadas, para su atención por el equipo antifraude. (12)

Organization

Perteneciente al Dominio *Party* ABE, consiste en otro de las partes involucradas en el desarrollo del negocio con la que se interactúa, se comparte y consume información, a la que se presta determinado servicio. Esta entidad en sí, representa un grupo de personas o individuo que comparten un interés común o propósito como departamentos, empresas o negocios. (12)

Policy

Perteneciente al Dominio *Policy ABE*. Representan un conjunto de reglas establecidas que son usadas para la gestión y control del estado, de uno o varios objetos manejados. A continuación serán abordadas una serie de entidades contenidas dentro del ABE *Policy* de las que, se considera fundamental su estudio debido a la información que manejan. Aun cuando algunas de ellas no forman parte del modelado propuesto ayudaron a comprender y asimilar la información contenida en el amplio ABE *Policy*. (12)

- PolicyRule

Esta entidad es un contenedor de datos. Contiene datos que definen como esta entidad es usada en un entorno, puede ser también una especificación o comportamiento. La información contenida es de cuatro formas.

- Datos o metadatos que definen la semántica o comportamiento la regla y el comportamiento que impone al resto del sistema.
- Grupo de eventos que pueden ser usados para desencadenar la evaluación de una condición de una regla.
- Grupo de condiciones agregadas en la regla.
- Grupo de acciones agregadas en la regla.

En el modelo no es más que una tripleta definida como eventos, condiciones y acciones. Los eventos son usados para desencadenar la evaluación de una o más condiciones, si estas condiciones evaluadas arrojan el resultado esperado, entonces las acciones asociadas con esta política con ejecutadas.

- ✓ El atributo *isCNF* contenido dentro de la entidad es para especificar en qué forma se encuentra representada la *PolicyCondition*
  1. *Conjuntive Normal Form*

2. *Disjunctive Normal Form.*

- PolicyEvent

Es una ocurrencia de un importante evento, puede ser usado para desencadenar la evaluación de una *PolicyCondition* o un grupo de ellas en una regla.

- PolicyCondition

Define el estado necesario o prerrequisitos que definen cuándo las acciones agregadas en la regla deben ser ejecutadas.

- PolicyAction

Es una agregación de acciones; representa las acciones necesarias que deben ser ejecutadas cuando una *PolicyCondition* es evaluada. Estas acciones son aplicadas a un grupo de objetos gestionados y tiene una repercusión en su estado.

- PolicyConflict

No está presente en el modelo de datos propuesto. Ocurre cuando las condiciones de una o más *PolicyRules* que son aplicadas al mismo grupo de entidades son simultáneamente satisfechas pero las acciones a aplicar en cada caso entran en conflicto.

- PolicyTarget

No está presente en el modelo de datos propuesto. Consiste en un grupo de entidades dígase objetos y entidades que controla el sistema a los que les son aplicadas un grupo de políticas determinadas, el objetivo de estas políticas es la transición de estados.

- PolicyRepository

No está presente en el modelo de datos propuesto. Es un contenedor lógico administrativo que es usado para almacenar información de las políticas, esto significa *PolicyRules*, grupos y elementos que pueden ser usados en la evaluación o ejecución de una *PolicyCondition* y *PolicyActions*.

- PolicyStatement

No está presente en el modelo de datos propuesto. Es un modelo para estandarizar la estructura de la una *PolicyCondition* y una *PolicyAction* dentro de un objeto *PolicyStatement*. La diferencia entre ellos radica en el operador que usar, Ej. "*match*" para las *PolicyAction* "*set variable to value*" para las *PolicyCondition* donde el único operador permitido es el "*set*". La capacidad de utilizarla misma forma básica para escribir *PolicyConditions* y *PolicyActions* simplifica enormemente el diseño e implementación de un sistema de gestión de la política al permitir que tales declaraciones se generen automáticamente.

Employee

Domino *PartyRole ABE*, es una parte involucrada en el negocio del proveedor de servicio, a su vez puede desempeñarse como cliente de la empresa. (12)

Customer

Perteneciente al Dominio *Customer ABE* no es más que una persona u organización que compra los productos o servicios de la empresa o recibe ofertas de servicios. (12)

ManagementInfo

Representa información obtenida en el entorno gestionado. Esta clase es la base para definir diferentes tipos de información. El diseño de como la información gestionada es obtenida, usa estas clases para recopilar la información requerida y la clase relacionada *ManagementMethodEntity* define el uso del método apropiado para la recopilación de los datos. Recopila información de usuarios, clientes, recursos lógicos y físicos entre otros. (12)

Party

Es una entidad de negocio que participa en un determinado proceso. Puede ser una organización, un individuo que a su vez forman parte de los procesos mediante roles como empleados, proveedor de servicios, clientes, entre otros. Cualquier parte involucrada en un proceso de negocio puede ser clasificada como *Party*. (12)

En importante resaltar la relación establecida entre *BusinessInteraction* y *Party*, especificando que se realizan interacciones entre el equipo antifraude y varias partes involucradas, las cuales juegan roles específicos dentro del negocio. Para establecer una determinada relación, intercambio e interacciones, son usados procedimientos que mantengan la seguridad, integridad y control de los activos de la empresa. (12)

PartyRole

Perteneciente al dominio de las Common Bussines Entities, dicha entidad representa el rol jugado por una entidad en un determinado contexto. (12)

ServiceProvider

Perteneciente ABE Party dentro del dominio Common Business Entities. Representa los roles o partes que pueden estar involucradas dentro del negocio. (12)

Usage

Atributos o datos de uso que surgen como resultado del empleo o uso de un recurso, producto o servicio para un fin determinado. (12)

FaultInfo

Clase base para todas aquellas relacionadas con posibles faltas, errores o desperfectos dentro del negocio. Sus subclases definen detalladamente las características y comportamiento de un tipo específico de falta. (12)

AccountingInfo

Mantiene un registro detallado de como un recurso o servicio es usado. Esta entidad es asociada con un recurso o servicio definiendo mediante sus relaciones sus características y comportamientos. (12)

GeographicAddress

Perteneciente al ABE *Location* dentro del dominio *Common Business Entities* contiene una estructura o vía textual de brindar una ubicación geográfica. El modelado de esta entidad proporciona datos que permiten establecer la dirección del *FMFraudTeam*. (12)

ContactMedium

El equipo de fraude como parte de un proveedor de servicio establece la vía de comunicación con entidades externas o dentro del mismo negocio. La entidad *ContactMedium* permite definir qué forma va a ser utilizada. Esta comprende vías de comunicación o contacto como número telefónico, dirección de correo electrónico, fax entre otros. (12)

3.3.2. Entidades propuestas

Una vez modelada toda la información haciendo uso de diagramas UML surge la interrogante de que función tiene una determinada entidad dentro del flujo. Para solucionar dicho problema se ha desarrollado una vía, expuesta a continuación que responda a las interrogantes que puedan surgir durante el análisis de la propuesta de solución.

Tabla 1: Modelo para la descripción de entidades.

Nombre	Nombre de la entidad.
Entidades Relacionadas	Entidades con las que se relaciona para representar la información necesaria. Aquellas entidades cuyo formato de letra se ve resaltado con **Negrita** significan que las mismas ya formaban parte del SID por lo que su descripción está presente en el epígrafe anterior.
Breve descripción de la entidad.	
Atributos	Nombre del atributo
Descripción	Descripción del atributo

Tipo	Tipo de dato del atributo.
Requerido	Especifica si puede ser o no nulo dicho atributo.
Notas	Datos adicionales que se considere importante mencionar
Operaciones	En caso de tener operaciones. Son expuestos los siguientes datos: • Descripción • Retorno: Tipo de dato que retorna una vez ejecutada la operación. • Notas

Tabla 2: FMFraudTeam

Nombre	FMFraudTeam
Entidades Relacionadas	**1. BussinessInteraction** 2. FMSupportInformation **3. Organization** 4. FMSharedInformation 5. FMLists **6. Policy** 7. FMInvestigationProcedure 8. FMAlarm 9. FMFile 10. FMFraudType 11. FMPenalty 12. FMCase **13. ServiceProvider** **14. ContactMedium** **15. GeographicAddress**

Compuesto por departamentos que realizan el trabajo conjunto de detección de fraude esta entidad es considerada parte fundamental del modelo de datos propuesto. Dicha entidad es el centro de todo proceso ya que incluye las personas, los procedimientos y la información generada durante las investigaciones o interacciones con factores externos a la empresa.

Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
id	Identificador del equipo de fraude.	entero	sí	

type	Clasificación para el equipo de fraude de acuerdo a determinadas características como área de acción, acceso a datos contenido de trabajo y otros.	entero	sí	Números enteros positivos, según la clasificación. Ej.: 1: Externo. 2: Colaborador.

Tabla 3: FMSupportData

Nombre	FMSupportData
Entidades Relacionadas	1. FMLists 2. FMSupportInformation 3. FMSuplementaryReport 4. FMSharedInformation 5. FMFile 6. FMFraudTeam

Entidad genérica y abstracta que constituye la base para la gestión de datos dentro de la empresa. Estos datos pueden ser resultantes del proceso de Gestión de Fraude, de la interacción con proveedores externos u otras fuentes. Comprende todas las estructuras creadas para el control de datos dentro del departamento y agrupa sus características y funciones comunes. Algunas de estas estructuras son *FMLists*, *FMSharedInformation*, *FMSuplementaryReport*, *FMFile* entre otras. Estas entidades colaboran entre sí habilitando varios procesos dentro de la empresa y son referentes para la toma de decisiones como soporte para los procesos ejecutados en los departamentos involucrados en la prestación de servicios.

Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
description	Descripción de la estructura de datos. Comprende datos de interés que describen datos que contiene, propósito etc.	Date	sí	
name	Nombre que identificara la estructura de datos dentro de la empresa.	cadena	sí	
id	Identificador inequívoco de la entidad.	cadena	sí	

creationDate	Fecha de creación.	date	sí	Norma ISO 8601[12]

Tabla 4: FMSupportInformation

Nombre	FMSupportInformation
Entidades Relacionadas	1. FMFraudTeam 2. FMInvestigationProcedure 3. FMSharedInformation 4. FMAction 5. FMSupportData 6. FMCase **7. Intermediary**

Información generada en el transcurso de la investigación de una actividad sospechosa, sea fraude o no. Esta entidad contiene los datos recopilados sobre cada paso de la investigación y constituye la fuente de información requerida para todos los demás departamentos y equipos, además de dar soporte a las investigaciones por parte de las agencias legales. Parte de esta información es intercambiada con otras partes involucradas de una forma u otra en el negocio o con agencias que soliciten determinados recursos o servicios.

Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
closureDate	Fecha que se registrará cuando ya dicha información no tenga razón de ser y decida ser eliminada o almacenada.	Date	sí	
actionResult	Información sobre la acción que se realiza en el proceso de investigación de fraude.	cadena	sí	

Tabla 5: FMSharedInformation

Nombre	FMSharedInformation
Entidades Relacionadas	1. FMFraudTeam 2. FMLists 3. FMSupportInformation 4. FMSupportData

[12]La norma ISO 8601 especifica la notación estándar utilizada para representar instantes, intervalos e intervalos recurrentes de tiempo evitando ambigüedades.

	5. BusinessInteraction

Información que cumpla con las políticas establecidas por la empresa para ser intercambiada o compartida con otras agencias o proveedores de servicios, esta información va ser compartida por un usuario del sistema, encargado de esta actividad por lo que debe contar con los permisos necesarios para hacerlo además de responsabilizarse por las consecuencias que este proceso arroje.				
Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
accessDescription	Descripción de los aspectos técnicos para el acceso a la información compartida.	cadena	sí	Ej.: 1. Protocolo 2. Aplicación 3. Passwords
responsableUser	Usuario responsable de la información que la empresa expone a otros proveedores de servicios.	Employee	sí	
grantedUsersAccess	Grupo de usuarios pertenecientes a empresas u otros organismos que tendrán acceso a la información compartida.	Organization	no	

Tabla 6: FMHotList

Nombre	FMHotList
Entidades Relacionadas	**1. PolicyRule** 2. FMInvestigationProcedure 3. FMPatterns 4. FMLists

Contiene patrones de actividades y comportamientos de tipos de fraudes ya identificados. Estos patrones pueden ser analizados en el proceso de investigación para detectar de inmediato posibles fraudes.				
Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
description	Descripción de la entidad.	cadena	no	

name	Nombre por el cual será identificada dentro del negocio.	cadena	sí	
creationDate	Fecha de creación, inserción en la base de datos.	date		Norma ISO 8601

Tabla 7: FMXDR

Nombre	FMXDR
Entidades Relacionadas	**1. Usage** 2. FMAlert **3. Customer** 4. FMBlackList

Registro de los procesos y comportamiento del cliente a la hora de hacer uso de un recurso o servicio brindado. Los Proveedores de Servicios de Comunicaciones (*CSPs*) necesitan una solución para recuperar información tanto general como muy específica, tal como el tipo de servicio que está usando un cliente, la fuente y el destino de las sesiones, las llamadas y otras actividades.

Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
id	Identificador de la central responsable del tráfico de datos	entero	sí	
startDate	Momento inicial de la interacción del cliente con el servicio. Registro de los datos.	date/time	sí	Norma ISO 8601
endDate	Momento final de la interacción del cliente con el servicio propiciado.	date/time	sí	Norma ISO 8601
usageDate	Fecha en que un cliente usa un determinado servicio.	date	sí	Norma ISO 8601
usageStatus	Estado del uso del servicio	entero	sí	

Tabla 8: FMBlackList

Nombre	FMBlackList
Entidades Relacionadas	1. FMSharedInformation 2. FMXDR

	3. FMFraudTeam 4. FMLists

Estas listas contienen nombre e identificaciones de infractores conocidos por lo que deben ser continuamente chequeadas, se debe tener en cuenta las entidades alteradas en gran parte de los casos y cualquier operación a realizar.

Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
description	Descripción de la entidad.	cadena	no	
name	Nombre por el cual será identificada dentro del negocio.	cadena	sí	
creationDate	Fecha de creación, inserción en la base de datos.	date		Norma ISO 8601

Tabla 9: FMFile

Nombre	FMFile
Entidades Relacionadas	1. FMCase 2. FMFraudTeam 3. FMSupportData 4. FMEntity 5. FMOpenReason **6. Employee** 7. FMEntity

Es un fichero que debe ser creado, modificado y gestionado por los actores del negocio con los privilegios establecidos. Este fichero consta de una estructura bien definida, la cual se debe chequear a la hora de la confección y/o modificación del mismo. El mismo surge por la agrupación de casos, según criterios que el analista requiere para realizar una investigación. El mismo incluye gestión documental, modo de operación. En resumen, forma y contenido del fraude en cuestión.

Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
state	Estado en que se encuentra el seguimiento del archivo (caso) en cuestión.	entero	sí	Ej.: 1: Abierto 0: Cerrado
closureDate	Fecha en que se llegó a un	date	sí	Norma ISO 8601

	resultado final y clausura del archivo.			
finalResult	Datos sobre el resultado final que arrojó el seguimiento del archivo o caso.	cadena	sí	

Tabla 10: FMAlarm

Nombre	FMAlarm			
Entidades Relacionadas	1. FMSuplementaryReport 2. FMAlert 3. FMCase			
Es el conjunto de alertas agrupadas por un determinado factor, estas van siendo tratadas y seguidas por equipos de fraude teniendo en cuenta la importancia de su mitigación o eliminación. Las alarmas al igual que las alertas pueden ser desencadenadas por información obtenida mediante personas no involucradas directamente con la empresa, por fuentes ajenas al proceso antifraude o por algún otro factor, que por su inminencia e importancia se considere necesario su investigación inmediata.				
Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
name	Nombre que identifique la alarma de acuerdo sus parámetros de agrupación para las alertas.	cadena	sí	
id	Identificador de la alarma.	entero	sí	
description	Descripción de la alarma, principales características.	cadena	no	
creationDate	Momento de creación de la alarma.	date	sí	Norma ISO 8601
score	Evaluación numérica que sitúa en una cola la urgencia en la atención de la alarma.	flotante	sí	
finalResult	Resultado final del tratamiento de la alarma. Descripción que exponga datos importantes para otros empleados de la	cadena	sí	

	empresa y proveedores de servicios.			

Tabla 11: FMAlert

Nombre	FMAlert			
Entidades Relacionadas	1. FMXDR 2. FMAlarm **3. PolicyRule** 4. FMCase			
Es el cumplimiento de una regla, es decir todos los positivos que la misma dispara, indicios de una actividad sospechosa que debe ser tenida en cuenta como un posible fraude o indicio del mismo. Esta alerta puede surgir por parte de un empleado, agente externo u otra fuente que o necesariamente tiene que estar vinculada con la empresa.				
Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
generationDate	Fecha de generación la alerta	date	sí	
id	Identificador de la alerta generada.	entero	sí	

Tabla 12: FMFraudType

Nombre	FMFraudType			
Entidades Relacionadas	1. FMPatterns 2. FMFraudTeam 3. FMInvestigationProcedure 4. FMCase			
Tipos de fraude identificados hasta el momento por un proveedor de servicio, estos pueden ser identificados u obtenidos mediante interacciones con otros proveedores. Cada tipo de fraude posee la forma de proceder ante su ocurrencia y las principales características que indican su presencia, facilitando la labor del departamento encargado de la detección y eliminación de fraudes.				
Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
id	Identificador del tipo de fraude creado.	entero	sí	

description	Descripción de un determinado tipo de fraude. Características que lo identifiquen.	cadena	sí	
name	Nombre que identifique un tipo de fraude.	cadena	sí	
groupedIn	Grupo al que pertenece un determinado tipo de fraude. Estos grupos se crean por características comunes para varios de ellos y reciben un tratamiento diferenciado.	entero	no	
Operaciones	**Descripción**	**Retorno**	**Notas**	
hasBeenTreated()	Operación que brinda información de cómo se ha comportado un determinado tipo de fraude durante la ejecución del negocio.	boolean		

Tabla 13: FMInvestigationProcedure

Nombre	FMInvestigationProcedure			
Entidades Relacionadas	1. FMFraudTeam 2. FMSupportInformation **3. Intermediary** 4. FMAction 5. FMFraudType 6. FMInvProcStatistics 7. FMHotList			
Procedimiento a seguir ante la ocurrencia de un fraude conocido dentro del negocio del proveedor de servicios. Este fraude es clasificado y agrupado según los criterios de los analistas al analizar sus características, cada grupo posee un tratamiento definido. En caso de no tener precedentes se hace una actualización de todos los mecanismos en la empresa que permitan la aptitud ante la ocurrencia nuevamente de dicha incidencia.				
Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
id	Identificador del procedimiento	entero	sí	

	de investigación.			
name	Nombre del procedimiento a seguir. Nombre sugerente atendiendo a los detalles del procedimiento, del caso tratado y otros aspectos que se consideren importantes.	cadena	sí	
description	Descripción del procedimiento de investigación creado. Fundamentalmente expone datos relacionados con los problemas que soluciona.	cadena	no	

Tabla 14: FMPermissions

Nombre	FMPermissions			
Entidades Relacionadas	**1. Employee** **2. Organization** 3. FMPermissions 4. FMSupportData			
Sistema de permisos para el acceso a la información y al sistema por parte del personal involucrado en la detección y tratamiento de los posibles fraudes. Como parte de este proceso juegan un papel fundamental en la estructura y representación de dicha información las especializaciones creadas, descritas a continuación. • *FMRoleBasedPermissions* Sistema de permisos basados en la asignación de roles a los usuarios del sistema. • *FMLevelsBasedPermissions* Sistema de permisos basados en la asignación de niveles de acceso a la información.				
Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
parent	Jerarquía del permiso.	entero	no	
nombre	Nombre del permiso establecido.	cadena	sí	
id	Identificador de la entidad.	cadena	sí	

Tabla 15: FMAction

Nombre	FMAction
Entidades Relacionadas	1. FMInvestigationProcedure 2. FMAction 3. FMSupportInformation **4. Response**

Acciones a realizar por el equipo de fraude para dar solución al fraude detectado, estas son relacionadas a tipos de fraudes detectados y pueden estar compuestas a su vez por un conjunto de acciones anidadas. Las entidades que a continuación se describen conforman la estructura definida para una *FMAction*.

- *FMActionStatement*

  Estructura correcta en la formulación de una acción a ejecutarse como resultado del proceso de análisis de fraude o como parte del procedimiento necesario.
- *FMActionAtomic*

  Acción en si forma más simple. La entidad recopila una acción a realizar, sencilla y entendible.
- *FMActionComposite*

  Conjunto de acciones anidadas que por sus características son forman parte del mismo proceso a ejecutar. Vista como una sola acción pero contenedora a su vez de un conjunto de acciones atómicas creadas anteriormente.

  Define el los tipos de acciones que pueden coexistir. Garantiza y permite el soporte de todas las acciones su creación, clasificación y agrupación en una estructura común y genérica.
- *FMFraudTeamAction*

  Especialización que describe las acciones ejecutadas por el factor humano, o sea equipos de fraude.
- *FMSystemAction*

  Especialización de la entidad *FMAction* que define la información sobre una acción automatizada. El operador define una actividad a realizar por el sistema bajo ciertas circunstancias en las que no es preciso contar con la aprobación del factor humano.

Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
id	Identificador de la acción	entero	sí	
description	Descripción de la acción a realizar. Se describen detalles importantes para otros usuarios del sistema, trabajadores del servicio antifraude en la	cadena	sí	

	empresa o para otros proveedores de servicios.			
type	Tipo de acción a realizar de acuerdo al grado de implicación directa con los recursos o los individuos involucrados, o a la técnica a seguir por la empresa.	entero	sí	Ej.: 0. No invasiva. 1: Invasiva. 2: Inmediata.
name	Nombre de que identifique la acción.	cadena	sí	

Tabla 16: FMDataCommonStructure

Nombre	FMDataCommonStructure			
Entidades Relacionadas	1. FMLists			
Estructura común para las listas de consulta. Brinda flexibilidad y logra la integración entre varias y distintas fuentes de información dentro del modelo. Es una estructura homologa al grupo de entidades que definen al *PolicyStatement* dentro del *Policy* Domain.				
Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
name	Nombre de la estructura por el que será comúnmente conocido dentro del negocio, en este caso es el *FMHotList*.	cadena	sí	
description	Datos que serán relevantes acerca de su contenido, propósitos, entre otros.	entero	sí	
id	Identificador inequívoco de la lista.	entero	sí	
creationDate	Fecha de creación de la lista.	date	sí	Norma ISO 8601

Tabla 17: FMPenalty

Nombre	FMPenalty

Entidades Relacionadas	**1. Party** 2. FMFraudTeamAction 3. FMFraudTeam
Especialización de una *FMAction*. Son acciones ejecutadas por el equipo de fraude, implementadas a partir de la detección de una actividad fraudulenta o violación de alguna de las políticas establecidas para los empleados dentro del código de ética de la empresa u otro documento que dicte su comportamiento. Las penalizaciones pueden ser aplicadas tanto a personal interno como externo.	

Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
description	Descripción de la penalización aplicada al empleado. Esta recogerá datos de importancia que justifiquen las (s) medidas tomadas.	cadena	no	
type	Tipo de penalización aplicada.	entero	sí	Ej.: 1: Temporal 2: Permanente.
validity	Plazo en que tendrá validez el cumplimiento de la medida aplicada por parte del empleado y su aplicación por parte de la empresa.	TimePeriod	no	

Tabla 18: FMSuplementaryReport

Nombre	FMSuplementaryReport
Entidades Relacionadas	1. FMAlarm 2. FMSharedInformation 3. FMSupportData
Reporte emitido por los analistas o responsables de analizar y gestionar la alarma. Consiste en la recopilación de las características más importantes que ayuden al seguimiento y soporte de las acciones tomadas durante su tratamiento.	

Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**

source	Persona responsable de su creación.	Employee	sí	
summary	Resumen del contenido del reporte.	cadena	no	

Tabla 19: FMLists

Nombre	FMLists
Entidades Relacionadas	1. FMSharedInformation 2. FMDataCommonStructure 3. FMFraudTeam

Lista genérica que contiene las características comunes para todas las listas de control que puedan coexistir dentro del negocio del proveedor de servicios. La flexibilidad y adaptación al cambio son sus principales objetivos dentro del modelo.

Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
description	Descripción de la entidad.	cadena	no	
name	Nombre por el cual será identificada dentro del negocio.	cadena	sí	
creationDate	Fecha de creación, inserción en la base de datos.	date		Norma ISO 8601

Tabla 20: FMPatterns

Nombre	FMPatterns
Entidades Relacionadas	1. FMHotList 2. FMFraudTeam 3. FMFraudType

Es el resultado del análisis exhaustivo de los *FMFile* por el equipo antifraude, definen los comportamientos y datos que describen, además brindan indicios sobre la ejecución de una actividad anómala. La información recogida en esa entidad es incluida en las *FMHotList* como material de consulta para los analistas de fraude.

Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
id	Cadena que define inequívocamente al patrón de	entero	sí	

	fraude creado.			
creationDate	Fecha en que se crea o modifica el patrón.	date	sí	Norma ISO 8601
description	Descripción del patrón creado, aspectos que se consideren importantes y que den una idea clara de la información que maneja el patrón.	cadena	sí	
Operaciones	**Descripción**	**Tipo**		
Modified ()	Método que controla la modificación de patrones recopilando datos de interés para el operador.	boolean		

Tabla 21: FMCase

Nombre	FMCase			
Entidades Relacionadas	1. FMFraudTeam 2. FMAlarm 3. FMAlert **4. CostRate** 5. FMFraudType 6. FMSupportInformation 7. FMEntity 8. FMOpenReason 9. FMFile **10. Employee**			
Un *FMCase* se abre por parte del equipo de fraude a causa de la identificación de un posible fraude, o por la generación de una alerta o una alarma. Contendrán información importante tanto para el equipo de fraude como para el (los) clientes involucrados en la investigación y constituyen el problema a resolver por el equipo antifraude. El resultado final formara parte de los procesos de retroalimentación del proceso de protección contra fraudes.				
Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**

id	Identificador del *FMCase.*	entero	sí	
name	Nombre del caso.	cadena	sí	
description	Descripción del caso. Serán reflejados datos de importancia sobre el mismo.	cadena	no	
creationDate	Fecha de creación del caso.	date	sí	Norma ISO 8601
state	Estado del *FMCase*	entero	sí	1: Abierto. 0: Cerrado.
finalResult	Resultado final del *FMCase*. Será documentado el desenlace final del caso y las medidas que fueron tomadas como consecuencia de la investigación.	cadena	sí	

Tabla 22: FMInvestigationProcedureStatistics

Nombre	FMInvestigationProcedureStatistics
Entidades Relacionadas	1. FMInvestigationProcedure

Entidad que intenta representar las estadísticas del uso de un determinado procedimiento para tratar una posible actividad fraudulenta. Esta permitirá que se evalúe el procedimiento, definiendo su futura transformación, mejora o eliminación.

Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
description	Describe la entidad dentro del negocio. Comprende datos de importancia que describan su función dentro del negocio.	cadena	sí	
dataOfApplyProcedure	Estadísticas de un procedimiento aplicado para la resolución de un posible fraude.	date	sí	Norma ISO 8601

Tabla 23: FMEntity

Nombre	FMEntity			
Entidades Relacionadas	1. FMCase 2. FMFile			
Entidad que define la información sobre las que se centran la creación de los *FMCase* y los *FMFile*. Información en la que se centra la atención en el proceso de investigación de una actividad sospechosa.				
Atributos	**Descripción**	**Tipo**	**Requerido**	**Notas**
id	Identificador del tipo de entidad.	entero	sí	
type	Tipo de entidad	entero	sí	Ej.: • IP • Phone Number • Subscriber
value	Valor que posee la entidad.	cadena		• 10.31.61.2 • 52325674 • dmendibur

3.4. Conclusiones

Ha quedado plasmada la propuesta de solución para la ausencia de la información necesaria en el ABE Gestión de Fraude. A estas alturas de la investigación se está en condiciones de validar la veracidad de los resultados obtenidos, de manera que quedarán reflejados los primeros resultados en la creación de la base de datos del proyecto SIAI, haciendo uso de la solución propuesta en un entorno real, es decir en una empresa de telecomunicaciones específicamente en su área de Gestión de Fraude. En función de ello se han seguido estrictamente las normas establecidas, se trabajó con el objetivo de mantener una genericidad y adaptabilidad eficiente de los datos a cualquier empresa de telecomunicaciones. Con su aplicación en el ámbito nacional, específicamente en los sistemas desarrollados por ETECSA, se da un paso de avance fundamental en el comienzo del perfeccionamiento y uso de la propuesta en el ámbito de las telecomunicaciones y sistemas de Gestión de Fraude desarrollados en todo el mundo.

CAPÍTULO 4: VALIDACIÓN DE LA PROPUESTA

4.1. Introducción

En el presente capítulo se emplearán lo resultados obtenidos durante el desarrollo de la investigación. Todo ello a modo de validación de la propuesta para su inclusión en el SID y su uso por las empresas de telecomunicaciones. Con el aporte a la construcción de la base de datos del proyecto SIAI, específicamente en el flujo de Análisis de Fraude se pretende finalizar por el momento el trabajo desarrollado. A continuación se presenta paso a paso el trabajo con el SID para la obtención de los resultados esperados.

4.2. Escenario de validación.

La propuesta desarrollada fue concebida desde sus inicios para formar parte de Frameworx específicamente del SID en su dominio de Gestión Empresarial, contribuyendo a la construcción de la Gestión de Riesgos. Su enfoque posibilita que sea utilizado por los departamentos de las empresas de telecomunicaciones dedicados a la Gestión de Fraude.

La Oficina Nacional del Grupo de Investigación de la Dirección de Operaciones de Seguridad (DOPS), departamento dedicado a la Gestión de Fraude en ETECSA, en conjunto con un equipo de desarrollo perteneciente a la Universidad de las Ciencias Informáticas une esfuerzos para la informatización de dichos procesos mediante el proyecto SIAI. Como parte de las tareas a realizar, se encuentra la creación de una base de datos que abarque eficientemente toda la información a gestionar por estos procesos. Es en este momento donde los resultados de la investigación serán utilizados, al constituir este proyecto el escenario ideal para la validación del modelo de datos obtenido. Específicamente se pretende construir la parte de la base de datos que se encuentra relacionada con los procesos de **Análisis de Fraude**. Para ello no necesariamente hay que utilizar el modelo SID en su totalidad, el beneficio puede ser obtenido de solo una parte de sus entidades y relaciones, poniéndose de manifiesto la flexibilidad con la que fue concebido, siendo esto una de sus grandes ventajas Las tareas que este trabajo requiere, adquieren su mayor peso en análisis del eTOM, posteriormente de la información proporcionada por el SID y las características de la empresa en cuestión. Estos pasos como parte del proceso van a definir la magnitud del éxito en la solución creada.

4.3. Aplicación de la propuesta.

El diagrama que a continuación es presentado en la figura 25 representa el uso o aplicación del modelo SID en un escenario real, dentro de una empresa de telecomunicaciones. Como se puede observar, son extendidas las entidades existentes tanto en la Gestión de Fraude como las ya presentes en el dominio *Common Business Entities*. En el caso de *Employee* donde además de ser extendida su información son introducidas varias entidades que abarcan el contenido requerido por la aplicación a desarrollar. Todo ello haciendo uso de las pautas expuestas, como la forma de agregar atributos y nuevas entidades, representado en la figura 16. Nótese que no toda la información presente en el flujo original fue utilizada, se considera que hasta el momento la forma seleccionada es la que se adapta a las necesidades de ETECSA para la implementación de los procesos de detección de fraude.

Con la meta planteada de aplicar en su totalidad los flujos desarrollados, fueron insertadas entidades que aparentemente no juegan un papel activo en la base de datos como es el caso de *PartyRole*. Este constituye una puerta abierta hacia la inclusión de nuevas entidades e información, propiciando la vinculación e interoperabilidad entre la base de datos de SIAI con sistemas ya desarrollados. Por su parte la entidad *CostRate* dio pie a una implementación de prioridad para la asignación de casos que hasta el momento era realizada con la asistencia de un analista, sin recibir una propuesta previamente elaborada por una solución informatizada, por consiguiente factores adversos como tiempo empleado y errores eran frecuentes en la ejecución del proceso. Por su parte la entidad *PolicyRule* da lugar al inicio del flujo tratado, generando las alertas (*FMAlert*) que serán tratadas por el personal encargado del proceso de análisis e investigación modelado a su vez por las entidades *Organization, Employee y FMFraudTeam*.

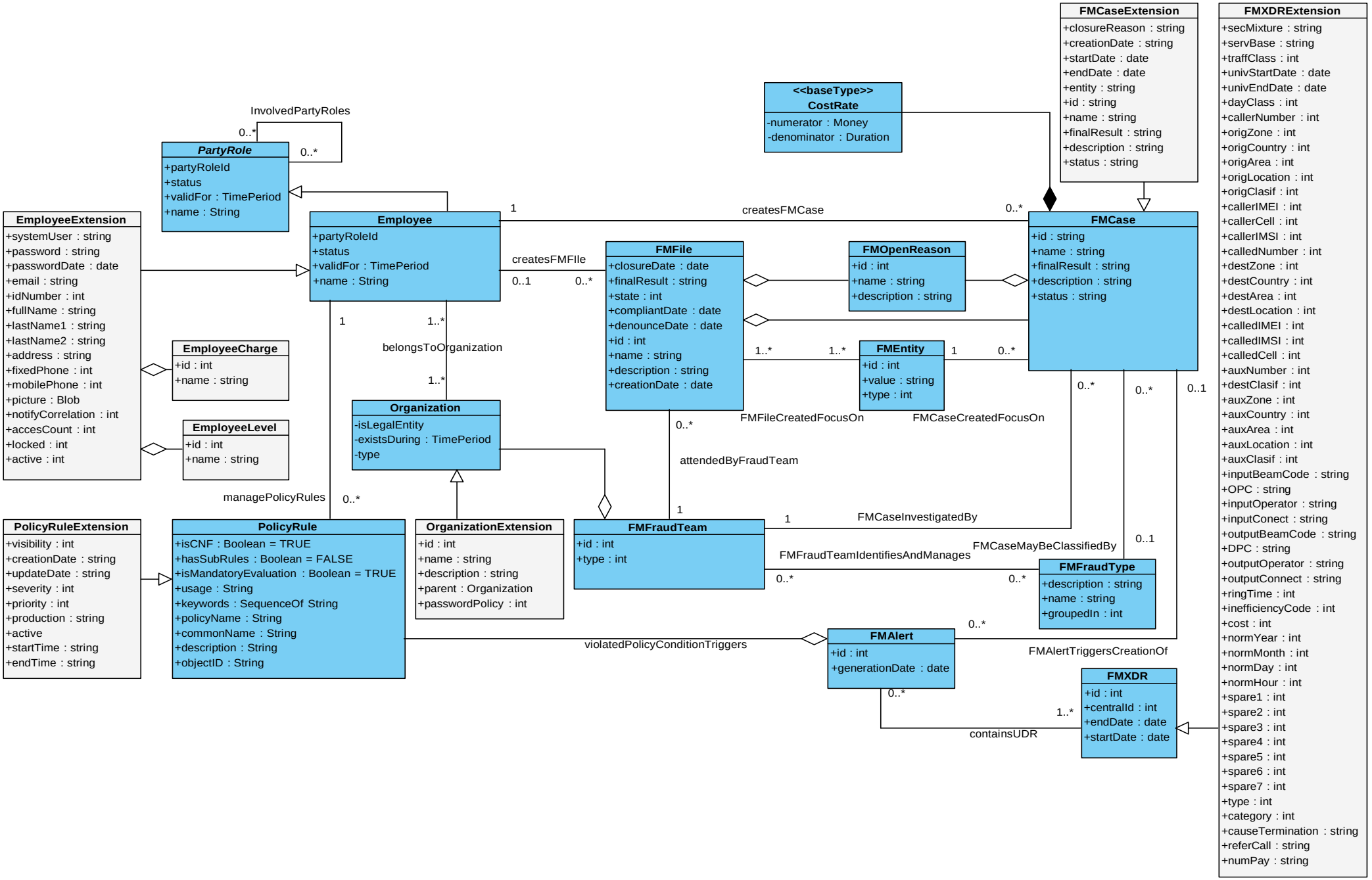


Fig. 25: Validación de la propuesta. Extendiendo el modelo.

4.4. Modelo Físico Lógico de la Base de Datos.

Finalmente, a partir del diagrama de clases fue obtenido el diagrama de clases persistentes, que formará parte de la base de datos del proyecto SIAI para la Gestión de Fraude. Para ello, el mismo ha estado sujeto a algunas modificaciones, sin alterar su contenido fundamental. Como se puede observar surgen nuevas tablas a causa del uso de nomencladores, en lugar de atributos o columnas en la base de datos, ganando en cuanto a ahorro de memoria, homogeneidad de la información y flexibilidad. La utilización de algunos de los atributos que forman parte del SID, con la propiedad de aceptar valores nulos permite que el sistema asimile poco a poco los cambios realizados, manejando los datos que hasta el momento requieren los servicios que brinda.

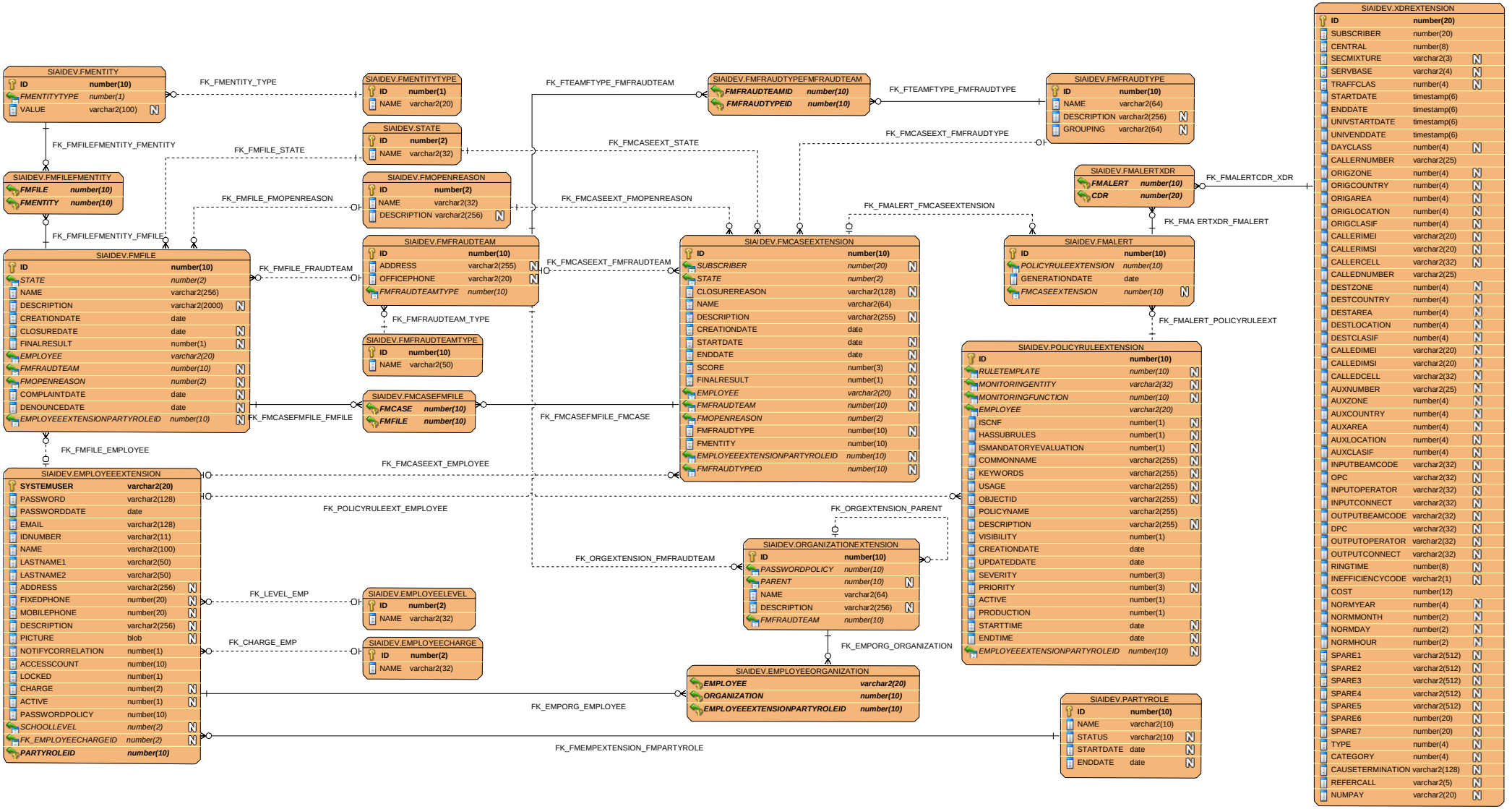


Fig. 26: Validación de la propuesta. Modelo Físico.

4.5. Conclusiones.

Al concluir este capítulo han sido insertados los cambios requeridos en la base de datos de forma satisfactoria, viendo materializados por primera vez las ventajas en el uso de la iniciativa Frameworx en ETECSA. Durante el proceso fueron cambiados los nombres de las tablas implicadas en el flujo, actualizada la información y relaciones a aquellas que así lo requerían, migrando de forma gradual hacia la estandarización que propone TM Forum. Los resultados inmediatos de la solución no pasaron desapercibidos, de forma inmediata fueron detectadas redundancia de la información, existencia de tablas innecesarias dentro del modelo e información importante, que hasta el momento no era tenida en cuenta o carecía de un eficaz tratamiento.

CONCLUSIONES GENERALES

En este momento se puede afirmar que el trabajo de investigación desarrollado, sobre los componentes de Frameworx, en función de las necesidades identificadas concluye con los resultados esperados. Basado en los siguientes resultados.

- El estudio de los procesos llevados a cabo actualmente en ETECSA, el contenido y razón de ser de la comunidad TM Forum, así como las herramientas necesarias para el análisis de los recursos brindados por la comunidad han permitido la creación de un marco teórico idóneo para el soporte de la investigación.
- Se ha realizado un minucioso estudio de los componentes de Frameworx, eTOM y SID así como el contenido asociado a la realización de los procesos de Gestión de Fraude en las telecomunicaciones.
- Como resultado fundamental se ha obtenido un modelo de datos con su respectiva documentación, acorde a las pautas seguidas por la comunidad TM Forum para el desarrollo de la iniciativa Frameworx, cumpliendo con las necesidades en el área de Gestión de Fraude dentro del SID.
- Los resultados alcanzados han sido aplicados parcialmente en la empresa nacional ETECSA, mediante el despliegue de la base de datos del proyecto SIAI arrojando resultados satisfactorios y alentadores para futuros cambios dentro de la estructura actual tanto de la información como de los procesos que actualmente se llevan a cabo para la prestación de servicios. De esta manera han quedado validados los resultados alcanzados obteniendo la aprobación por parte del cliente.

Ha quedado demostrado que el éxito asociado al uso de los componentes de Frameworx está garantizado, dependiendo en gran medida del nivel de análisis e identificación de puntos débiles dentro de la empresa y un estudio profundo de los estándares propuestos para su total aprovechamiento. Actualmente formar parte de la comunidad y beneficiarse de su capital intelectual, así como contribuir al desarrollo del mismo es una acertada opción para todas las empresas pertenecientes al sector.

RECOMENDACIONES

- Proponer los resultados de la investigación a los miembros de la comunidad TM Forum para su inserción oficialmente dentro del SID, siendo esto una vía para que ETECSA comience a gestionar lo antes posible su inclusión como miembro de dicha comunidad.
- Continuar con el desarrollo de la base de datos del proyecto SIAI haciendo uso de la propuesta obtenida, realizando una continua retroalimentación de los resultados alcanzados hasta el momento.
- Hacer uso del eTOM para la restructuración de los procesos que actualmente son llevados a cabo, no solo en el área de Gestión de Fraude sino en toda la empresa.

BIBLIOGRAFÍA

1. **Ing. Rolando Rodríguez Andrés, Dra. Lourdes García Ávila.** Ilustrados. [En línea] [Citado el: 17 de Enero de 2013.] http://www.ilustrados.com/documentos/ngoss-herraminetas-automatizacion-negocio-130508.pdf.

2. **TM Forum.** *tmforum.* [En línea] [Citado el: 5 de Abril de 2012.] http://www.tmforum.org/TMForumFrameworx/1911/home.html.

3. —. *GB947 Fraud Operation Management Guide v1.1.* TM Forum. Morristown, NJ 07960 USA : s.n., 2011. Guía.

4. —. *Better billing saves more than $60 millon in a year and reduces churn.* Comunidad TM Forum. s.l. : TM Forum Cases Study Handbook, 2012.

5. —. *Next-generation service assurance improves operational efficiency.* Comunidad TM Forum. s.l. : TM Forum Cases Study Handbook, 2012.

6. —. *Consistent processes deliver more than 50 percent greater efficiencies in launching new services.* s.l. : TM Forum Cases Study Handbook, 2012.

7. —. tmforum. [En línea] [Citado el: 1 de Abril de 2012.] http://www.tmforum.org/Adoption/11940/home.html.

8. **IBM.** IBM. [En línea] 14 de Junio de 2004. [Citado el: 12 de 12 de 2012.] http://www.ibm.com/developerworks/rational/library/content/04August/3153/3153_Rumbaugh_ch01.pdf.

9. **EcuRed.** EcuRed. [En línea] [Citado el: 10 de Febrero de 2013.] http://www.ecured.cu/index.php/SQL.

10. **La Flecha.** Oracle 11g, la nueva base de datos de Oracle. *LaFlecha Tu diario de ciencia y tecnología.* [En línea] [Citado el: 25 de February de 2012.] http://www.laflecha.net/canales/empresas/noticias/oracle-11g-la-nueva-base-de-datos-de-oracle.

11. **Oracle.** Oracle. [En línea] [Citado el: 14 de Enero de 2013.] http://www.oracle.com/technetwork/database/database-11g-standard-edition-one-d-132019.pdf?ssSourceSiteId=ocomen.

12. **TM Forum.** *GB922 SID Addenda Files R9.0.* 2004.

13. **Ashley Hanna, Stuart Rance.** ITIL. [En línea] Mayo de 2007. www.itil-officialsite.com/nmsruntime/saveasdialog.aspx?lID=1183&sID=242.

14. **UIT.** UIT. *UIT.* [En línea] [Citado el: 14 de Febrero de 2013.] https://www.itu.int/ITU-T/recommendations/index.aspx?ser=M.

15. BusinessDictionary. *BusinessDictionary.com.* [En línea] WebFinance Inc, 2012. [Citado el: 12 de 05 de 2012.] http://www.businessdictionary.com.
16. Eclipse. *Eclipse Documentation.* [En línea] [Citado el: 25 de 11 de 2012.] http://help.eclipse.org/indigo/index.jsp.
17. **Grupo Soluciones Innova.** GSInnova. *GSInnova.* [En línea] Grupo Soluciones Innova, 2007. [Citado el: 01 de 10 de 2012.] http://www.rational.com.ar/herramientas/rup.html.
18. **Knowledge Based System, Inc.** IDEF Integrated DEFinition Methods. *IDEF Web Site.* [En línea] 2010. [Citado el: 25 de 11 de 2012.] http://www.idef.com/IDEF0.htm.
19. ITESCAM. [En línea] http://www.itescam.edu.mx/principal/sylabus/fpdb/recursos/r25380.PDF.
20. **JBoss Community.** JBoss Community. [En línea] [Citado el: 10 de Enero de 2013.] http://www.jboss.org/developer/about.html.
21. LaFlecha. [En línea] [Citado el: 24 de Febrero de 2013.] http://www.laflecha.net/canales/empresas/noticias/oracle-11g-la-nueva-base-de-datos-de-oracle.
22. **TM Forum.** tmforum. [En línea] [Citado el: 5 de 4 de 2012.] tmforum.org/TMForumFrameworx/1911/home.html.
23. Un poco de Java. [En línea] [Citado el: 16 de Enero de 2013.] http://unpocodejava.wordpress.com/2012/09/18/un-poco-de-plataforma-wso2-carbon/.
24. Visual Paradigm. *Visual Paradigm Web Site.* [En línea] Visual Paradigm. [Citado el: 25 de 11 de 2012.] http://www.visual-paradigm.com/product/vpuml/provides/.
25. **Visual Paradigm Community.** Visual Paradigm. *Visual Paradigm Web Site.* [En línea] [Citado el: 25 de 11 de 2012.] http://s1.linkvp.com/quickstart/quickstart_vpuml.pdf.
26. Visual Paradigm. *Visual Paradigm Web Site.* [En línea] Visual Paradigm. [Citado el: 25 de Noviembre de 2012.] http://www.visual-paradigm.com/product/vpuml/.
27. w3schools.com. [En línea] [Citado el: 20 de Febrero de 2013.] http://www.w3schools.com/sql/sql_intro.asp.
28. **WSO2 Enterprise.** WSO2. [En línea] [Citado el: 5 de Enero de 2013.] http://wso2.com/products/carbon/.
29. **TM Forum.** tmforum. [En línea] http://www.tmforum.org/DownloadRelease115/8371/home.html.
30. —. tmforum. [En línea] http://www.tmforum.org/DownloadRelease115/8175/home.html.
31. —. *GB921 Concepts and Priciples v9.2.* Morristown, NJ 07960 USA : s.n., 2011.
32. —. *GB921 Addendum P v4.10.* Morristown, NJ 07960 USA : s.n., 2011.
33. —. *GB921 Addendum U v1.5.* Morristown, NJ 07960 USA : s.n.

34. —. *GB921 Getting Started Pack R9.0.* Morristown, NJ 07960 USA : s.n., 2011.
35. —. *GB921 eTOM Core Standards Files R9.0.* Morristown, NJ 07960 USA : s.n., 2011.
36. —. *GB922 Getting Started with SID R9.0.* 2010.
37. —. *GB921 eTOM Applying the Framework Files R9.0.* Morristown, NJ 07960 USA : s.n.

ANEXOS

En esta sección serán expuestos fundamentalmente los diagramas que contienen la información asociada a la mayoría de las entidades creadas como parte de la propuesta de solución. El análisis de la información expuesta toma mayor relevancia y se considera fundamental a la hora de entrar en los detalles de cada flujo.

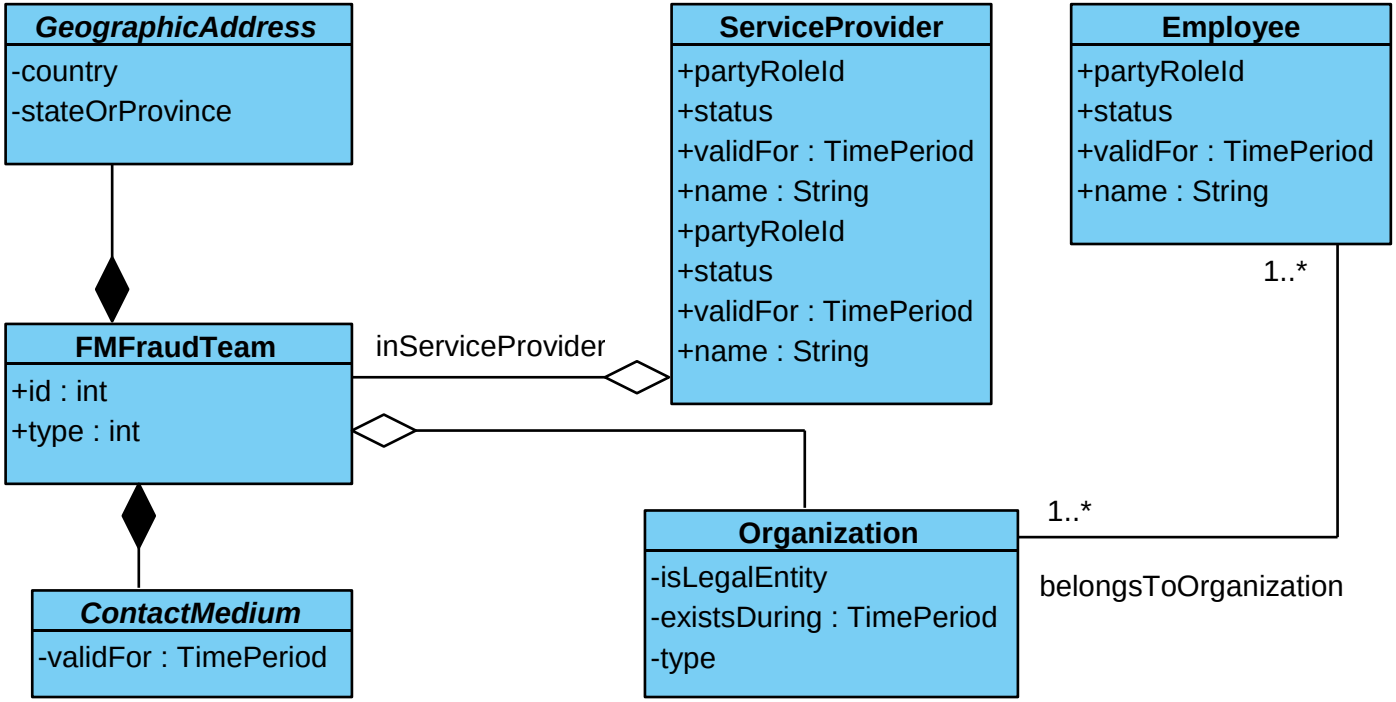


Fig. 27: Modelado de la entidad FMFraudTeam.

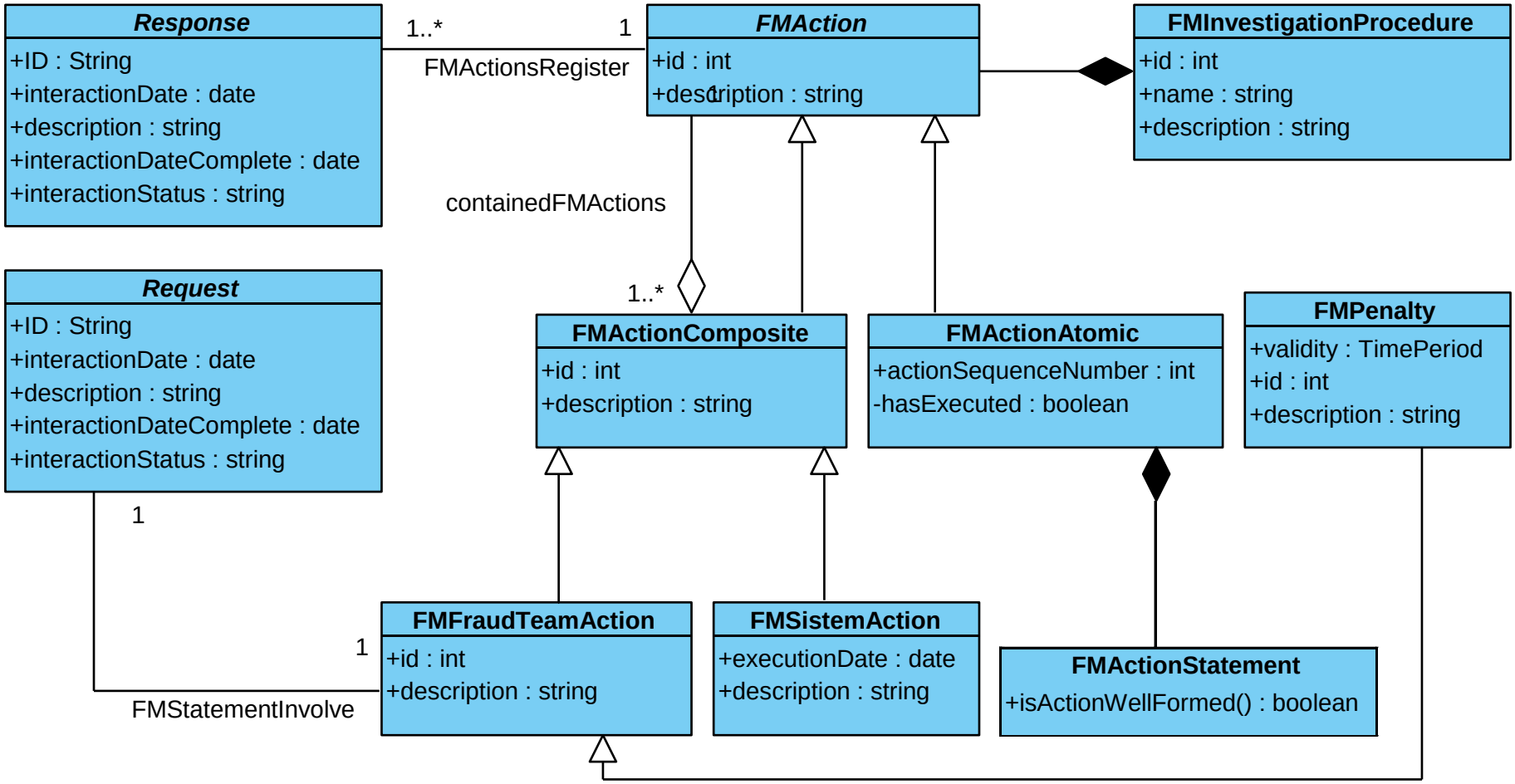


Fig. 28: Modelado de la entidad FMAction.

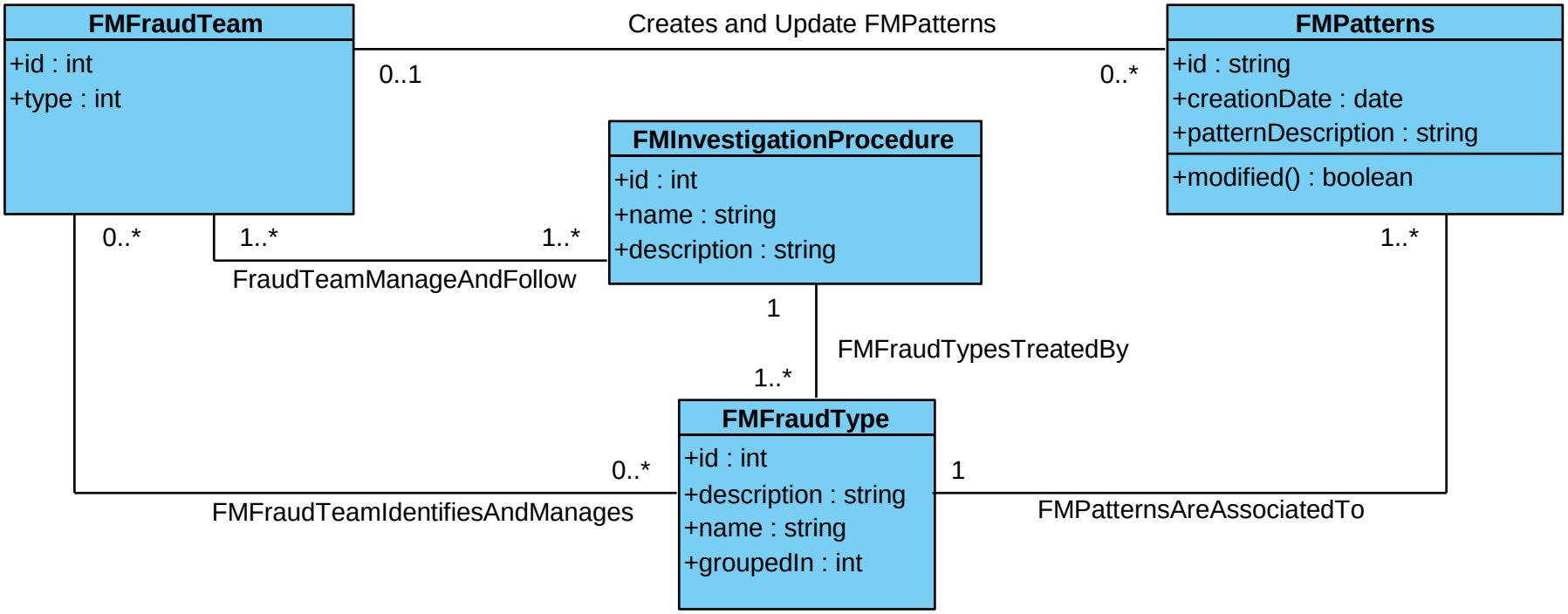


Fig. 29: Modelado de la entidad FMFraudType.

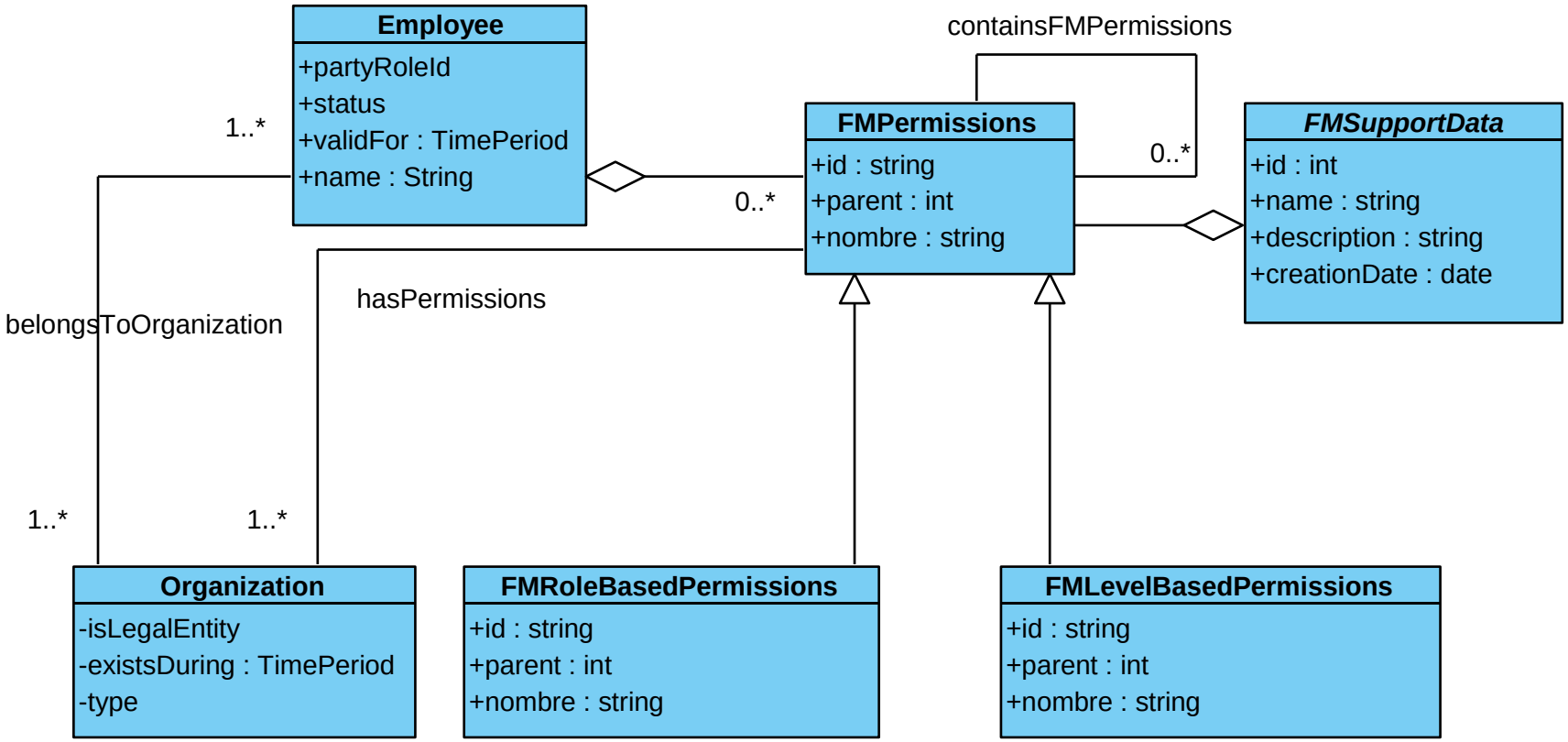


Fig. 30: Modelado de la entidad FMPermissions. Control de acceso.

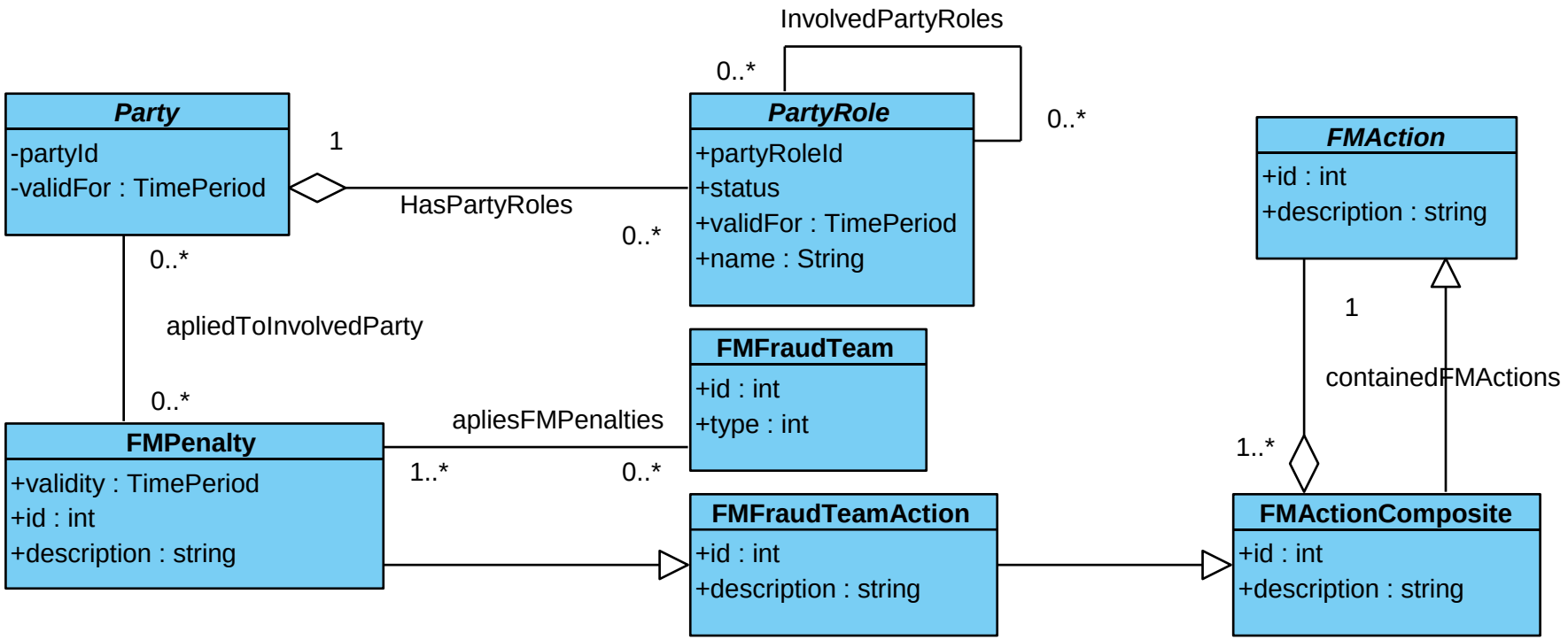


Fig. 31: Modelado de la entidad FMPenalty

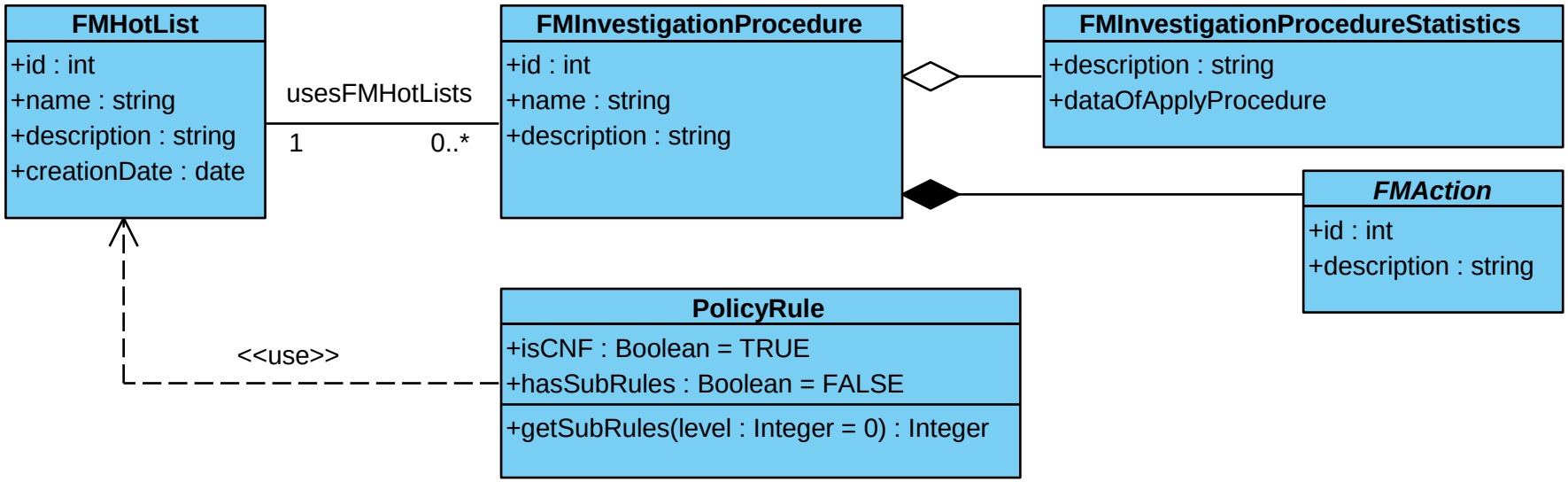


Fig. 32: Modelado de la entidad FMInvestigationProcedure.

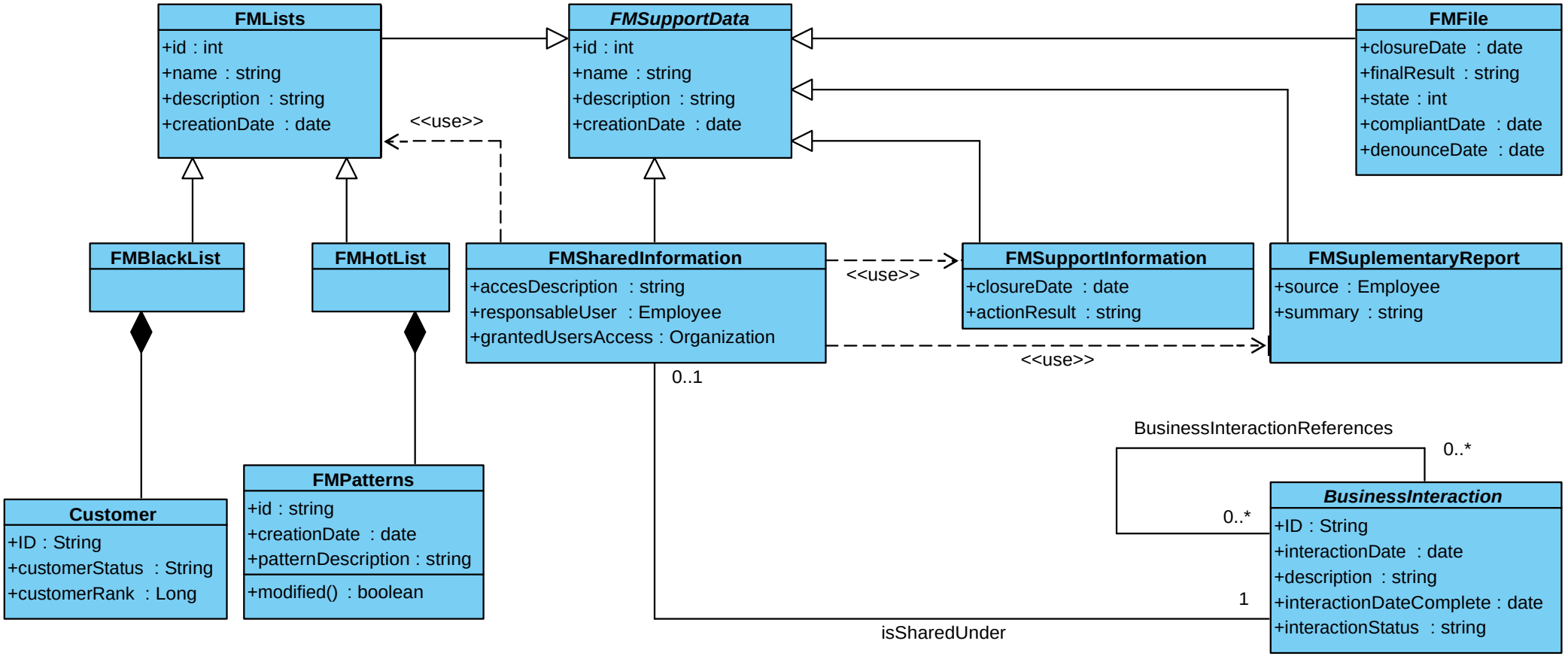


Fig. 33: Modelado de la entidad FMSupportData.

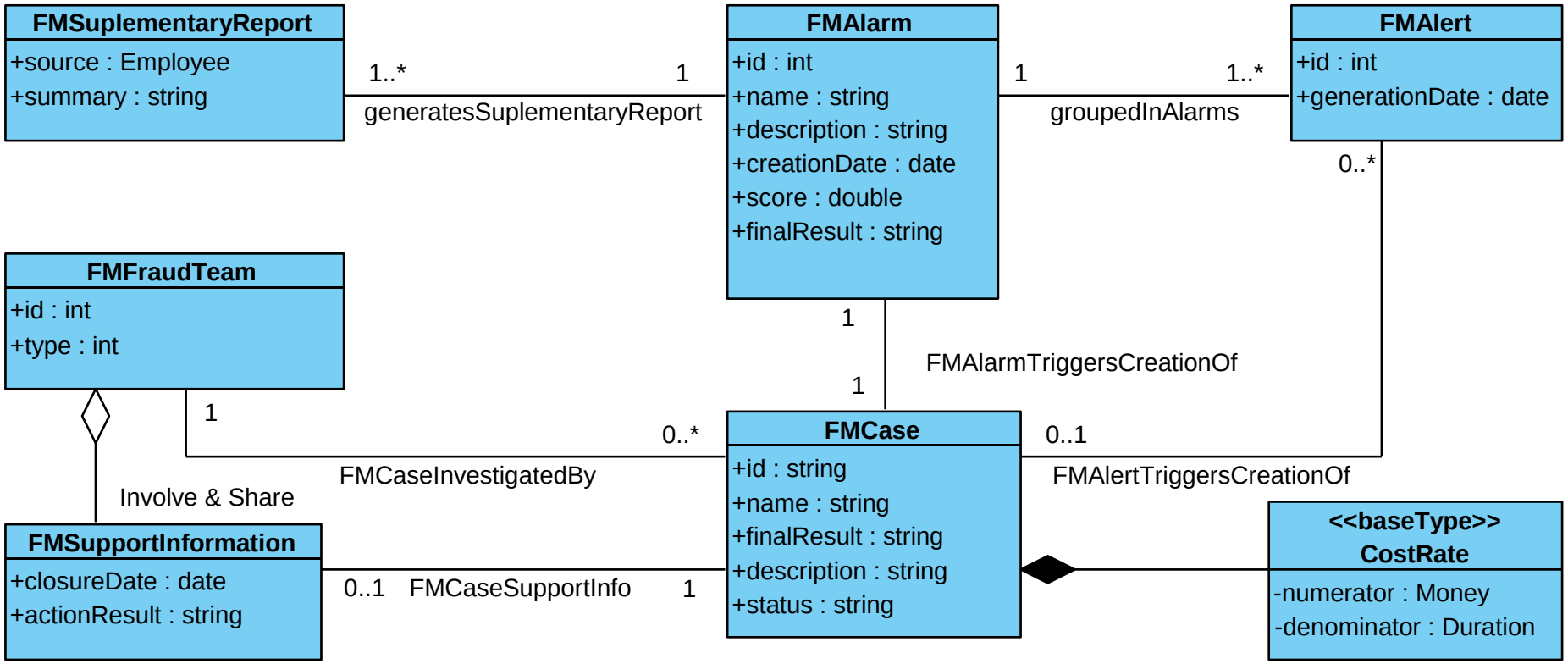


Fig. 34: Modelado de la entidad FMCase.

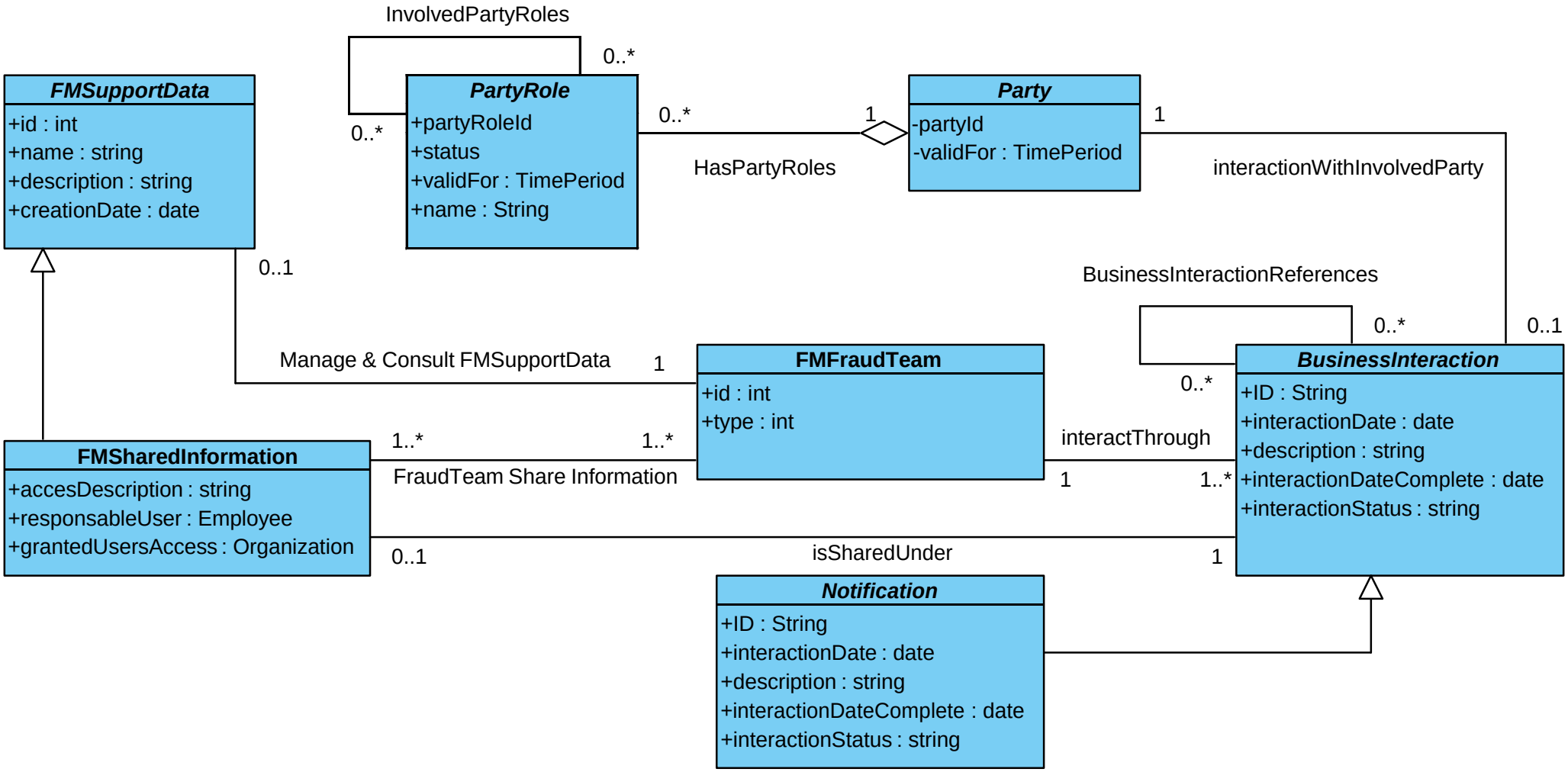


Fig. 35: Modelado de la entidad BusinessInteractions para la Gestión de Fraude.

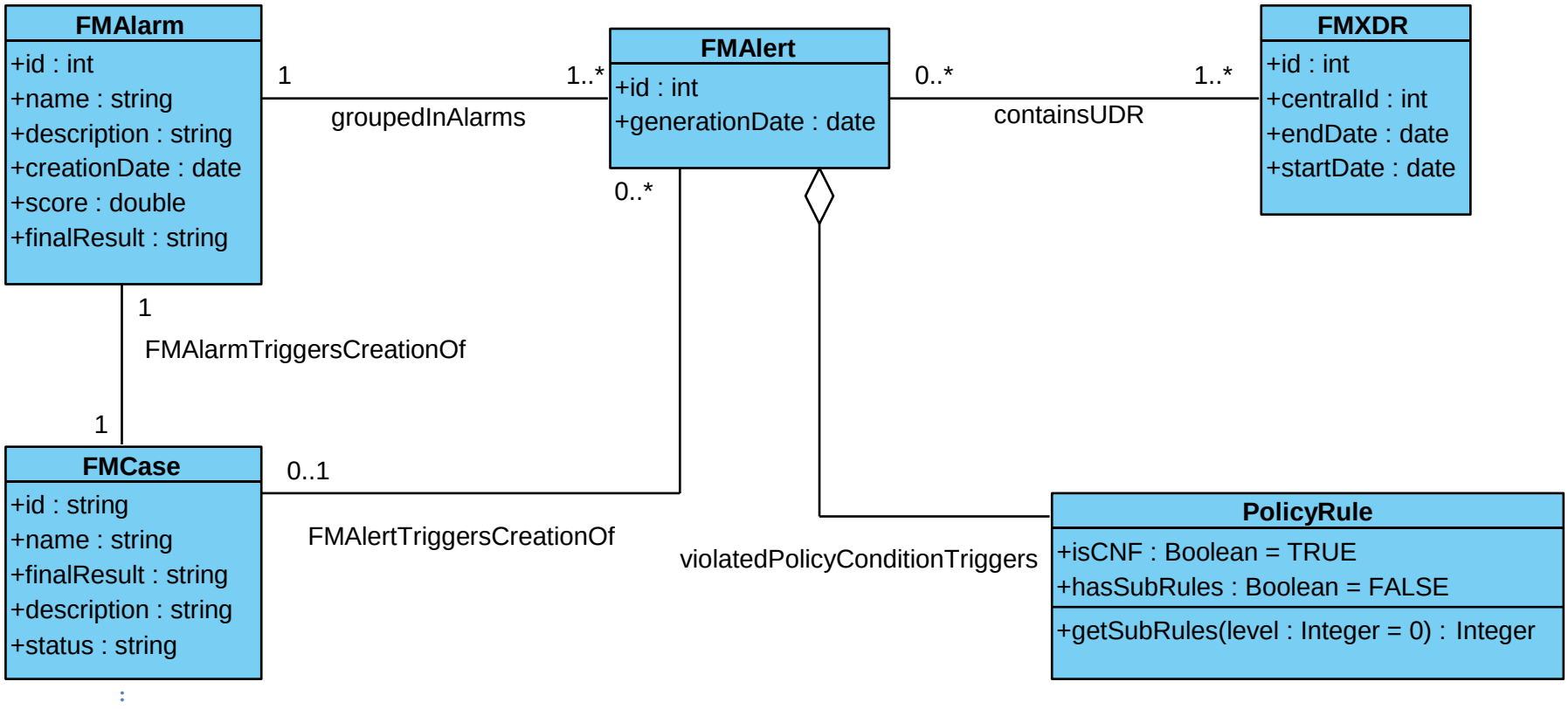


Fig. 36: Modelado de la entidad FMAlert.

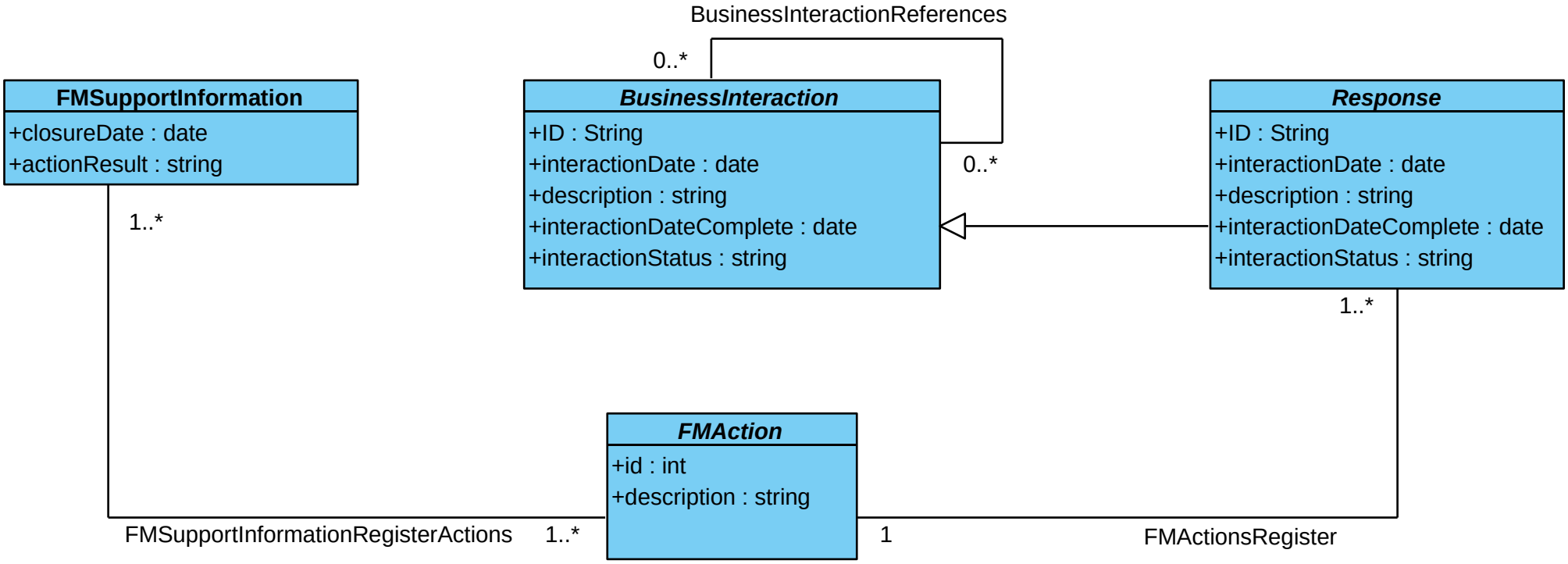


Fig. 37: Modelado de la entidad FMSupportInformation.

GLOSARIO

Proveedor de servicios:

Es una organización que proporciona servicios a uno o más clientes, internos o externos. A menudo se utiliza el término proveedor de servicio para abreviar proveedor de servicios de TI[13]*.* **(Hanna, 2007)** Es una entidad que cuenta con los medios e infraestructura necesarios para establecer un servicio de telecomunicaciones determinado, puede ser con fines comerciales o solamente colaborativos. Generalmente estos servicios incluyen el acceso a internet, consumo de datos mediante servicios webs implementados, suscripciones a servicios de telefonía entre otros.

Área

Sección del eTOM donde se enmarca un determinado grupo de procesos, condicionados por su ubicación y su razón de ser dentro de la empresa.

ABE: *del inglés (Agregate Bussines Entities)*

Cumulo de información y operaciones que caracterizan un grupo de entidades de negocio altamente cohesivo y débilmente acoplado.

Proceso

Secuencia de actividades que describe el correcto funcionamiento de una actividad dentro del negocio.

Estándar

Es un requerimiento obligatorio. El término también se utiliza para referirse a un código de prácticas o las especificaciones publicadas por una organización de estándares como ISO. **(Hanna, 2007)**

Especificación

Es una definición formal de los requerimientos. Una especificación puede utilizarse para definir los requerimientos técnicos u operacionales, y puede ser interna o externa. Muchas normas públicas consisten de un código de prácticas y una especificación. La especificación define el estándar contra el cual puede auditarse a una organización. **(Hanna, 2007)**

Dominio

Hace consistente el modelo de información con el modelo de negocio en el nivel 0, son un conjunto de ABEs asociadas a un área de administración especifica.

[13] Tecnologías de Información.

NGOSS

Proyecto desarrollado por la comunidad TM Forum para la creación de una nueva generación de sistemas de soporte para las operaciones y negocios B/OSS (*del inglés: Business / Operations Support Systems*) a través de la creación de una marco de trabajo, un repositorio de documentación, modelos y líneas de desarrollo como soporte para el trabajo en el sector de las telecomunicaciones.