FACULTAD DE INGENIERIA

UNIVERSIDAD DE LA REPUBLICA

Análisis

Autor:
Julio Saráchaga

Supervisor:
Dr. Gustavo Betarte

Contraparte del cliente:
Ing. Fernanda Molina

Supervisor alterno:
Ing. Marcelo Rodríguez

1 Introducción

A continuación se presentan los aspectos más importantes que se tuvieron en cuenta para el desarrollo del proyecto. Se presentan características deseadas en un sistema de intercambio de información de seguridad entre organizaciones.

2 Análisis de requerimientos

Existen distintos problemas que obstaculizan el intercambio de información entre las organizaciones. Dichas problemáticas afectan la reputación, seguridad y la capacidad de trabajo de las organizaciones.

Las organizaciones pueden intercambiar grandes volúmenes de datos los cuales pueden provenir de diferentes fuentes, cada una de estas fuentes puede utilizar una representación propia para los datos. Por ello es deseado que las organizaciones utilicen un estándar aceptado por todas. La representación utilizada debería permitir el desarrollo de herramientas que ayuden a la organización y estructuración de los datos de forma de facilitar el trabajo de los analistas.

Otro de los problemas que interfieren en el intercambio de información es el riesgo a la seguridad y reputación de la organización. La información intercambiada debe pasar por procesos que controlen los datos que se intercambien evitando de esta manera la divulgación de información sensible o privada.

Estas son algunas de las problemáticas que se pueden identificar referentes al intercambio de información de seguridad. También existen otros problemas, como por ejemplo establecer un criterio referente a políticas organizacionales que ayuden a identificar organizaciones de confianza. Este problema no será analizado en este documento.

La herramienta que se desea desarrollar busca ayudar a las organizaciones a solucionar algunos de los problemas planteados anteriormente y que afectan el intercambio de información con sus pares. Además es deseado que la herramienta pueda ser extendida en un futuro con nuevas funcionalidades que solucionen otras problemáticas no identificadas o que no se desarrollen en el transcurso de este proyecto.

Se desea desarrollar una herramienta que se integre con alguna de las aplicaciones de gestión de incidentes existentes proveyéndole la capacidad de

intercambiar información de seguridad. Dicha herramienta debería estructurar y organizar la información de forma de facilitar el intercambio. Además se debería dar la posibilidad de correlacionar la información de forma de facilitar el trabajo de los analistas. Una funcionalidad importante en una herramienta de estas características es la sanitiziación de los datos compartidos con el fin de proteger la integridad de la organización durante los intercambios.

Los intercambios podrían proveer información sobre la identificación de nuevas vulnerabilidades o entidades maliciosas, soluciones a problemas, prevención de problemas, etc.

El intercambio de información no es un problema estrictamente técnico, hay procedimientos y consideraciones legales y de confianza que podrían afectar el intercambio de información entre organizaciones. Durante el estado del arte se investigaron distintos protocolos y lenguajes para la representación de la información, se llegó a la conclusión de que ninguno de estos daba soluciones referentes a las políticas organizacionales que solucionaran problemas como la confianza entre las organizaciones o la información que debe ser compartida.

A pesar de lo mencionado anteriormente, es deseable que un sistema que comparta información de seguridad respete y aplique las políticas organizacionales. Por ello es necesario que el sistema aplique políticas definidas por los administradores para sanitizar y anonimizar la información con el fin de remover datos confidenciales o sensibles antes de que sean compartidos. Para resolver este problema se debe evaluar la protección que se le quiere dar a la información y considerar a su vez cuan útil es dicha información luego de ser sanitizada.

Del análisis anterior se desprende la necesidad de contar con un módulo que permita a la aplicación sanitizar la información. Como se mencionó anteriormente, los administradores definen dichas políticas en el sistema. La finalidad del módulo es analizar la información y filtrar datos que pudieran ser sensibles y que pusieran en riesgo los intereses de la organización.

Durante el intercambio de información, se pueden obtener datos provenientes de diversas fuentes que se refieren a distintos tipos de información, pero que guarden una relación entre ellos. Por ello es necesario contar con un módulo que se encargue de relacionar la información por medio de la aplicación de estrategias. El resultado de la aplicación de estrategias es la

agrupación de los datos, dicha agrupación permite a los analistas manejar una menor cantidad de datos y de esta forma simplificar su trabajo. Esto ayuda a bajar el periodo de tiempo entre la detección del problema y su solución.

Con la correlación es posible vincular información generada por distintas fuentes para decidir si se tratan de falsos positivos o hechos reales. A su vez, permite detectar ataques que pudieran pasar desapercibidos en volúmenes muy grandes de información.

Si bien la información correlacionada es de utilidad para los analistas, puede ser necesario contar con toda la información recibida para poder hacer un análisis de los datos originales por parte de los analistas.

Además de recibir información proveniente de otras organizaciones, es deseable que se pueda ingresar nueva información al sistema. Dicho ingreso de información se pretende realizar por medio del sistema de gestión de incidentes, a su vez se desea mantener una representación estructurada de la información ingresada en el incidente. Mantener la información de forma estructurada permite realizar la correlación con datos recibidos de otra organización. Esto permitiría por ejemplo ayudar a solucionar un problema para el cual otra organización tenga una solución.

De lo anterior se pueden identificar los siguientes requerimientos funcionales:

Requerimientos funcionales
• La herramienta debe implementar un modelo peer-to-peer de intercambio de información entre organizaciones. • Se debe dar la posibilidad de sanitizar la información intercambiada por medio de políticas definidas por el administrador. • Es deseable contar con un módulo para correlacionar la información de los incidentes configurable por el administrador. • Dar la posibilidad de gestionar información de seguridad.

Tabla 1 - Requerimientos funcionales del sistema.

También se pueden ver los siguientes requerimientos no funcionales:

Requerimientos no funcionales
• Extensibilidad: Debe ser posible extender la herramienta con nuevos módulos que implementen nuevas funcionalidades. • Independencia de sistema de gestión de incidentes para que exista la posibilidad de utilizar otra herramienta.

Tabla 2 - Requerimientos no funcionales del sistema.

3 Herramientas

En esta sección se muestran las herramientas utilizadas. STIX fue elegida porque provee una representación estructurada y estándar de la información. Junto con STIX se eligió TAXII el cual ha sido diseñado para intercambiar información de seguridad representada por medio del lenguaje STIX y que

tiene consideraciones para realizar el intercambio. Posteriormente se menciona a que se debió la utilización de RTIR y se detalla en mayor profundidad la selección de STIX y TAXII.

Además se consideraron en menor medida la posibilidad de desarrollar trabajo futuro con dichas herramientas y su aceptación por parte de la comunidad.

3.1 RTIR

RTIR es un sistema de manejo de incidentes diseñado para ser utilizado por CSIRTs para manejar el creciente número de incidentes reportados. Si bien existen otras herramientas similares, RTIR presenta la ventaja de ser *opensource* y contar con una API que permite extender la herramienta de forma sencilla. También es posible desarrollar *plugins* para extender las funcionalidades de la herramienta. RTIR cuenta además con una comunidad de usuarios grande cuya característica principal es el nivel técnico de estos.

Distintos CSIRTs han contribuido en el desarrollo de la herramienta, el resultado ha sido una herramienta que posee un *workflow* para el manejo de incidentes de seguridad. Dicho *workflow* facilita el trabajo de los CSIRTs.

Como se mencionó en el estado del arte, RTIR no cuenta con una representación estructurada de la información ni tampoco con un método automático para compartir información de seguridad. Una integración con TAXII y STIX le permitiría cubrir estas dos falencias.

El interés de usar RTIR proviene de que el CSIRT-Tilsor tiene la herramienta instalada y la utiliza para sus operaciones. Además hay miembros del equipo que tienen experiencia en su uso.

Además al ser una herramienta con una profunda inserción en la comunidad, es esperable que sea más fácil la aceptación de una extensión basada en TAXII y STIX que la creación de una nueva herramienta a la que los usuarios deberán adaptarse.

Si bien RTIR fue una premisa dentro de los objetivos del proyecto se evaluaron durante el estudio del arte otras herramientas que pudieran tomar su lugar. De todas formas, del análisis realizado, se eligió RTIR por las razones dadas anteriormente. A pesar de utilizarse RTIR, es deseable que la herramienta desarrollada no sea dependiente de RTIR, esto quiere decir que se pueda utilizar una herramienta con funcionalidades similares en el futuro.

3.2 STIX y TAXII

Se decidió utilizar STIX para representar la información por la facilidad con la que permite representar información de seguridad de forma estructurada y estándar. Por medio de CybOX se permite describir evidencia en la forma de observables, artefactos y/o comportamientos presentes en un sistema. La representación de forma precisa se debe a la gran gama de objetos distintos que permite describir, entre ellos, el nombre de procesos ejecutándose, hash de archivos o mensajes ICMP. Como se vio en el estado del arte, STIX también permite representar incidentes, tácticas, técnicas y procedimientos de los adversarios, actores maliciosos entre otros conceptos que permiten representar adecuadamente información de seguridad.

Otras de las características que posee STIX son la extensibilidad, la simpleza y la facilidad de procesamiento. Dichas características son propias de un lenguaje XML.

TAXII define un conjunto de servicios e intercambios de mensajes que permiten el intercambio de información de seguridad. En la especificación de TAXII se establece que la información de seguridad es representada por medio de STIX. Además TAXII posee consideraciones de seguridad para realizar el intercambio como lo son encriptación y autenticación.

TAXII realiza el intercambio de conjuntos de información de seguridad llamados "TAXII Data Collections". Dichas colecciones de datos pueden ser conjuntos ordenados de información ("TAXII Data Feeds") en los cuales el criterio de ordenación es un *timestamp* o conjuntos desordenados ("TAXII Data Sets"). La información en dichos conjuntos es representada de forma estructurada utilizando el lenguaje STIX. Durante los intercambios de información es necesario que el cliente pida información de una de las colecciones de las que dispone el productor. Por ello es necesario que se de en el sistema la posibilidad de gestionar las colecciones a las que un cliente se suscribe.

STIX también integra con otras iniciativas de MITRE e incluso se integra con lenguajes de otras organizaciones como IODEF de IEEE y OpenIOC de Mandiant.

Es importante mencionar que STIX ha tenido un fuerte apoyo de comunidad y busca convertirse en un estándar. Actualmente existen esfuerzos para crear herramientas que utilicen el lenguaje STIX y se realice un intercambio de información por medio de TAXII.

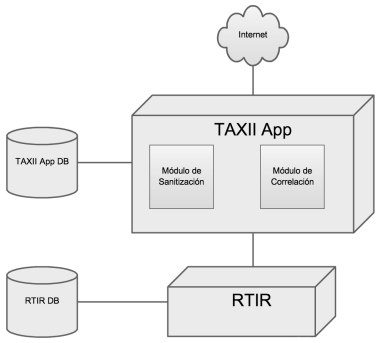

Figura 1 - Diagrama de bloques del sistema

Con las herramientas mencionadas anteriormente podemos ver un diagrama de bloques como el de la figura 1. En la figura se puede ver que se cuenta con una instalación de la herramienta RTIR que será la encargada de la gestión de incidentes y por medio de la cual se dará de alta la información en el sistema. Además en el bloque "TAXII App" realiza el intercambio de información con otras organizaciones por medio de TAXII y representa la información utilizando STIX. Además dicho bloque es el encargado de realizar la sanitización y correlación de información.

4 Actores y Casos de Uso

4.1 Actores

Actor	Analista
Descripción	Este actor tiene la posibilidad de ingresar nueva información en el sistema. Dicha información puede ser intercambiada con otro sistema. Con la información que se ha intercambiado el actor puede realizar un análisis de ella y hacer un manejo de los casos creados en el RTIR.

Actor	Cliente TAXII
Descripción	Este actor es el que interactúa con el sistema para intercambiar datos por medio del protocolo TAXII. El sistema tiene que dar soporte para dicho protocolo para que el intercambio sea exitoso.

4.2 Casos de uso y diagramas de secuencia

4.2.1 ABM de políticas de sanitización

Nombre	ABM de políticas de sanitización
Actor	Analista
Descripción	Estos casos de uso comienzan cuando el analista desea realizar el alta, baja o modificación de las políticas de sanitización. Por medio de estas se filtra la información que se desea intercambiar con otras organizaciones.

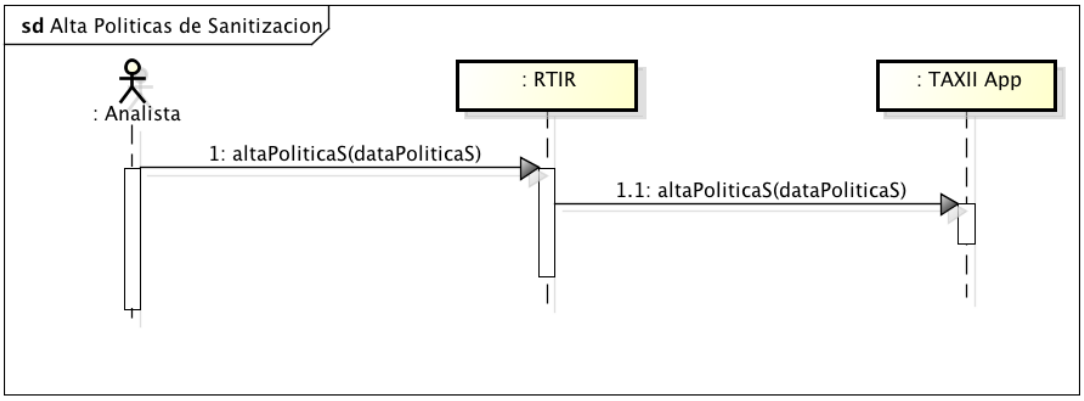

Figura 2 - Caso de uso alta políticas de sanitización

En la figura 2 se especifica el caso de uso, en este un analista ingresa a RTIR y da de alta en el sistema una política de sanitización. Dicha política es utilizada para realizar la sanitización de la información intercambiada por la organización. Las políticas son registradas en TAXII App.

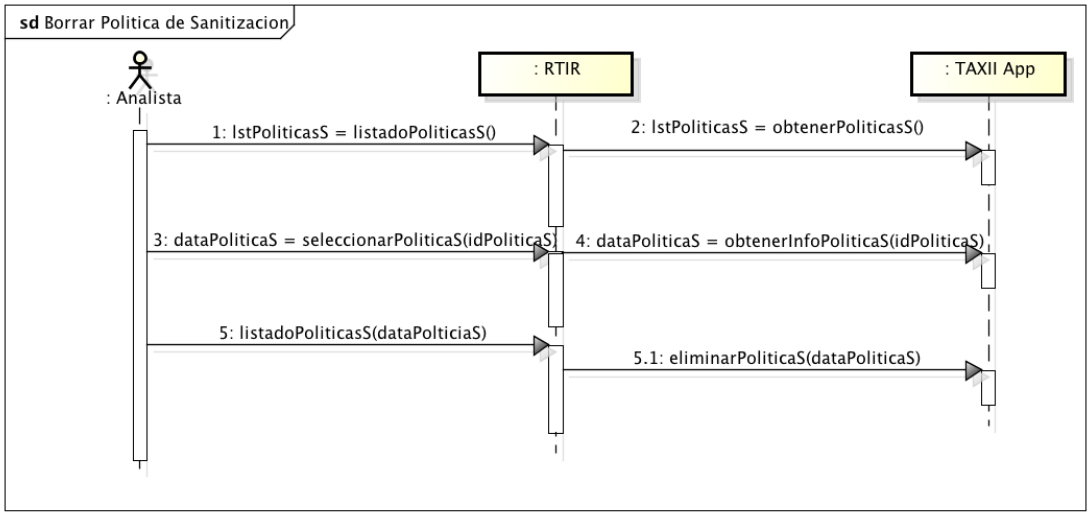

Figura 3 - Caso de uso borrado políticas de sanitización

En la figura 3 se especifica el caso de uso de borrado de políticas de sanitización, en este un analista ingresa a RTIR y lista todas las políticas disponibles en el sistema. Luego selecciona la política que desea dar de baja para luego borrarla.

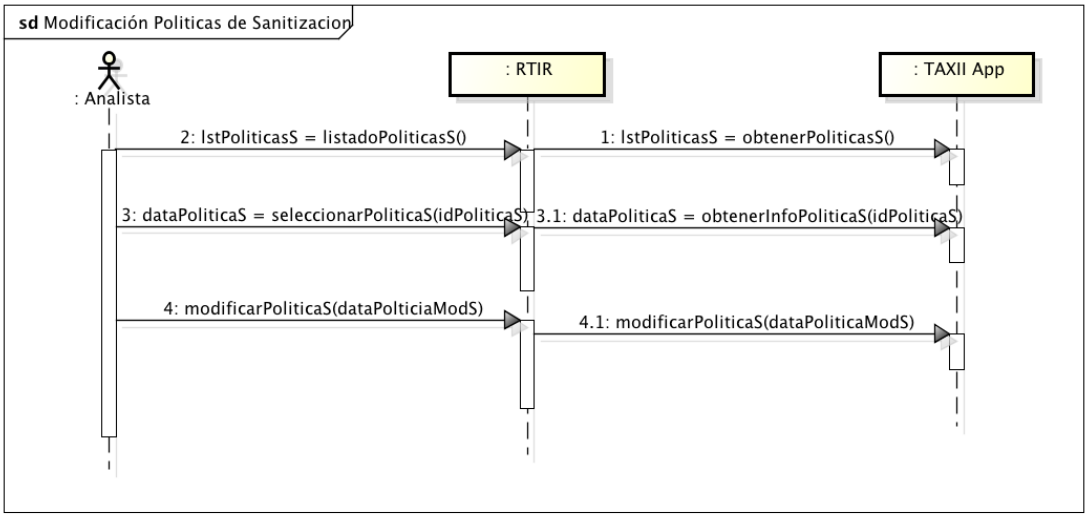

Figura 4 - Caso de uso modificación de políticas de sanitización

En la figura 4 se especifica el caso de uso de modificación de políticas de sanitización, en este un analista ingresa a RTIR y lista todas las políticas disponibles en el sistema. Luego selecciona la política que desea modificar.

4.2.2 ABM de Políticas de Correlación

Nombre	ABM de políticas de correlación
Actor	Analista
Descripción	Estos casos de uso comienzan cuando el analista desea realizar el alta, baja o modificación de las políticas de correlación. Por medio de estas se agrupa la información según los datos existentes en el sistema.

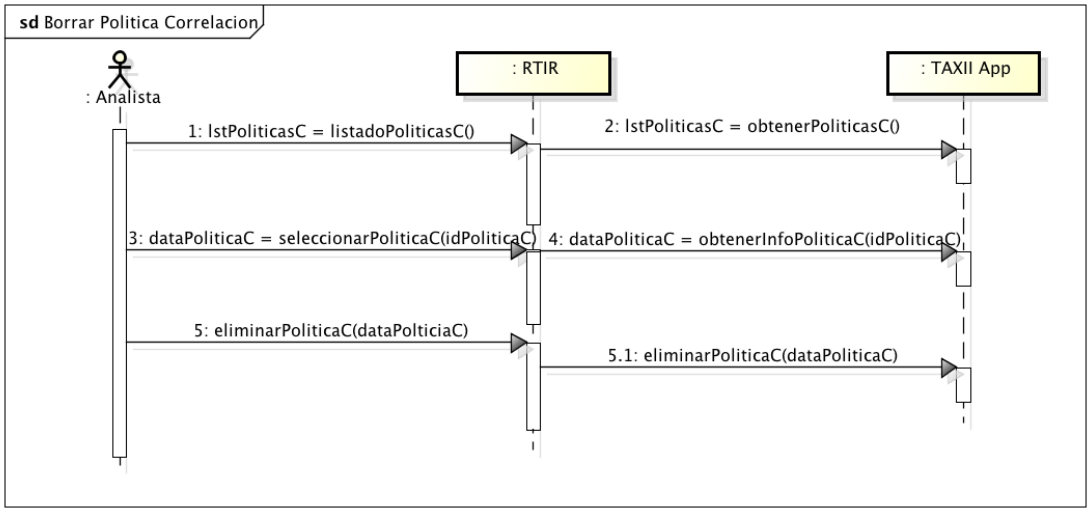

Figura 5 - Caso de uso borrado políticas de correlación

En la figura 5 se especifica el caso de uso de borrado de políticas de correlación, en este un analista ingresa a RTIR y lista todas las políticas disponibles en el sistema. Luego selecciona la política que desea dar de baja para luego borrarla.

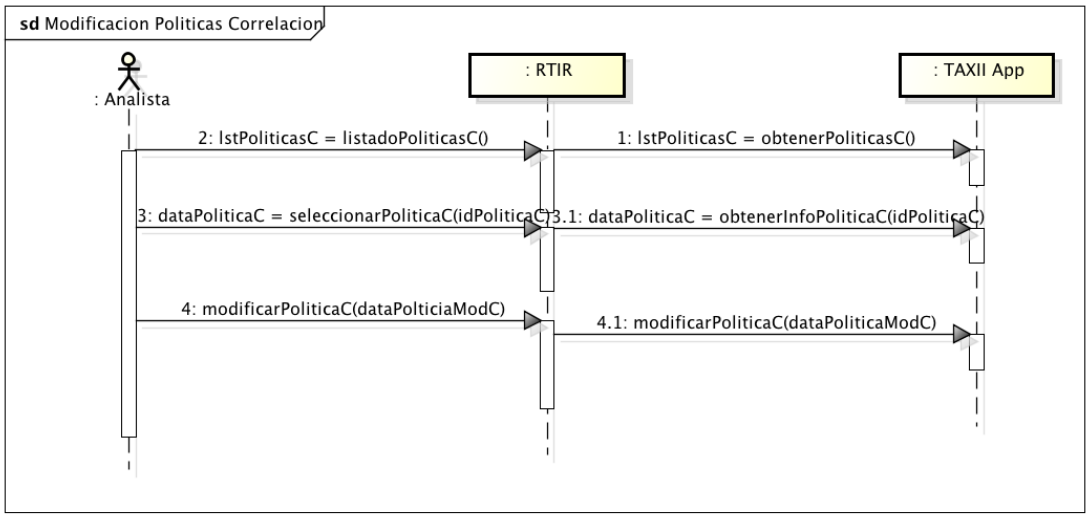

Figura 6 - Caso de uso modificación políticas de correlación

En la figura 6 se especifica el caso de uso de modificación de políticas de correlación, en este un analista ingresa a RTIR y lista todas las políticas disponibles en el sistema. Luego selecciona la política que desea modificar.

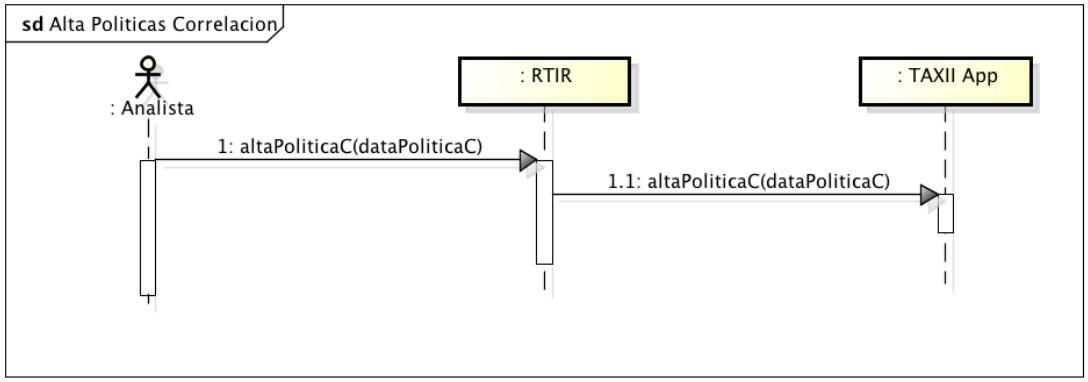

Figura 7 - Caso de uso alta políticas de correlación

En la figura 7 se especifica el caso de uso de alta de políticas de correlación, en este un analista ingresa a RTIR y da de alta en el sistema una política de correlación. Dicha política es utilizada para realizar la correlación de la

información presente en el sistema. Las políticas son registradas en TAXII App.

4.2.3 ABM de Servicios TAXII

Nombre	ABM de servicios TAXII
Actor	Analista
Descripción	Estos casos de uso comienzan cuando el analista desea realizar el alta, baja o modificación de servicio TAXII de otras organizaciones en el sistema. Estos serán utilizados para lograr el intercambio de información.

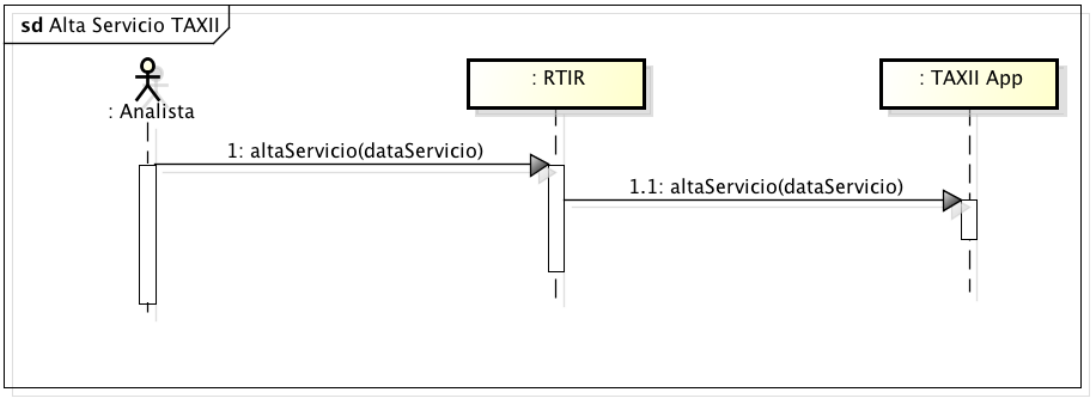

Figura 8 – Caso de uso alta servicio TAXII

En la figura 8 se especifica el caso de uso de alta de servicios TAXII, en este un analista ingresa a RTIR y da de alta en el sistema un servicio TAXII. Por medio de dicho servicio TAXII se realizara el intercambio con otra organización.

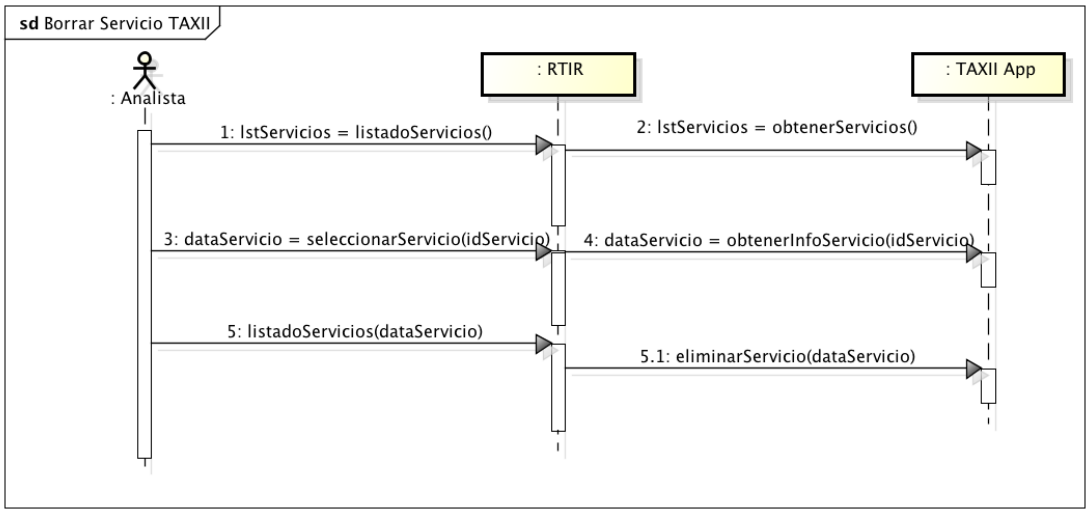

Figura 9 - Caso de uso borrar servicio TAXII

En la figura 9 se especifica el caso de uso de borrado de servicios TAXII, en este un analista ingresa a RTIR y lista todas las servicios disponibles en el sistema. Luego selecciona el que desea dar de baja.

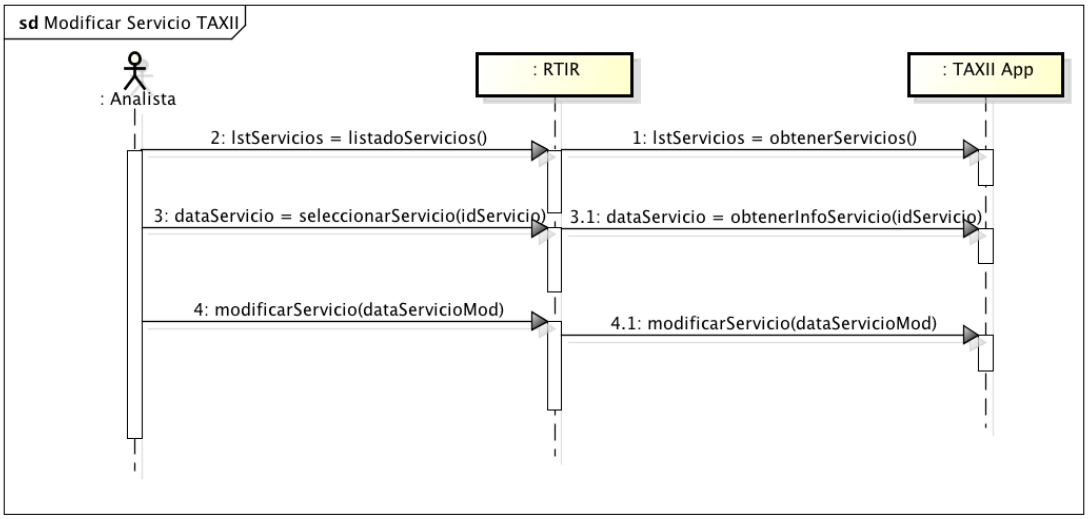

Figura 10 - Caso de uso modificar servicio TAXII

En la figura 10 se especifica el caso de uso de modificación de servicios TAXII, en este un analista ingresa a RTIR y lista todos los servicios disponibles. Luego selecciona el que será dado de baja.

4.2.4 Alta de información RTIR

Nombre	Alta de información RTIR
Actor	Analista
Descripción	Este caso de uso comienza cuando el analista desea registrar nueva información en el sistema. Para ello debe ingresar la información deseada al sistema. Es deseado que se pueda dar de alta información referente a cyber observables como por ejemplo IPs, hash de archivos, descripciones de amenazas, etc. El manejo podría realizarse por medio de los incidentes de RTIR.

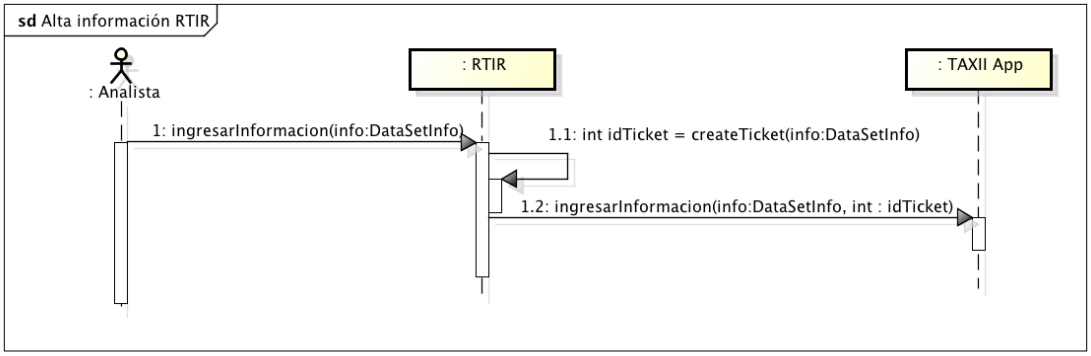

Figura 11 - Caso de uso alta de información RTIR

En la figura 11 se ve el caso de uso de alta de información en RTIR. En este un analista ingresa al sistema e ingresa nueva información en RTIR. En RTIR se crea un nuevo ticket y en TAXII App se da de alta la información representando y almacenándola de forma estructurada.

4.2.5 Subscripción a TAXII Data Feed

Nombre	Subscripción a Taxii Data Feed
Actor	Analista
Descripción	Con este caso de uso un analista selecciona un data feed en otro sistema al que quiere subscribirse. Esto se realiza por medio del Feed Managment Service de los sistemas.

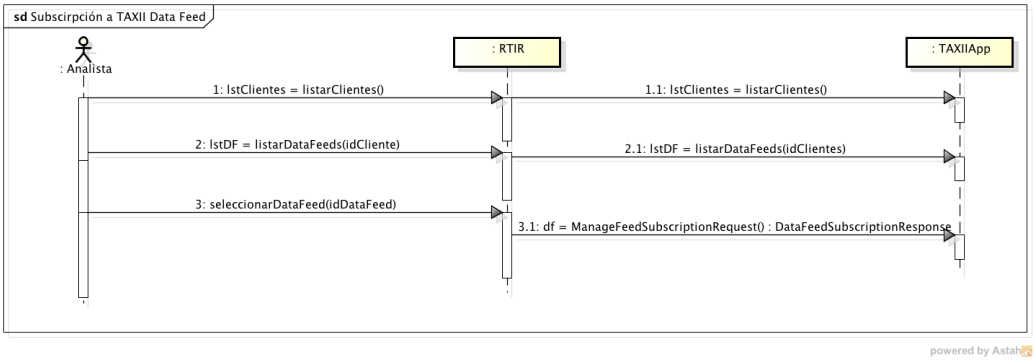

Figura 12 **- Caso de uso subscripción a TAXII Data Feed**

En este caso de uso el analista desea subscribirse a uno de los TAXII data feed provistos por otra organización. Para ello obtiene un listado de los clientes TAXII con los que se relaciona para luego obtener un listado de los Data Feeds disponibles en ese cliente. Finalmente selecciona el TAXII data feed deseado.

4.2.6 Recepción de información

Nombre	Recepción de información
Actor	Cliente TAXII
Descripción	Este caso de uso se da cuando un cliente TAXII desea enviarle información a nuestro sistema. El envío de información se realiza porque un analista se subscribió a un data feed en el cliente. La recepción de información se realiza por medio del Inbox Service de nuestro sistema.

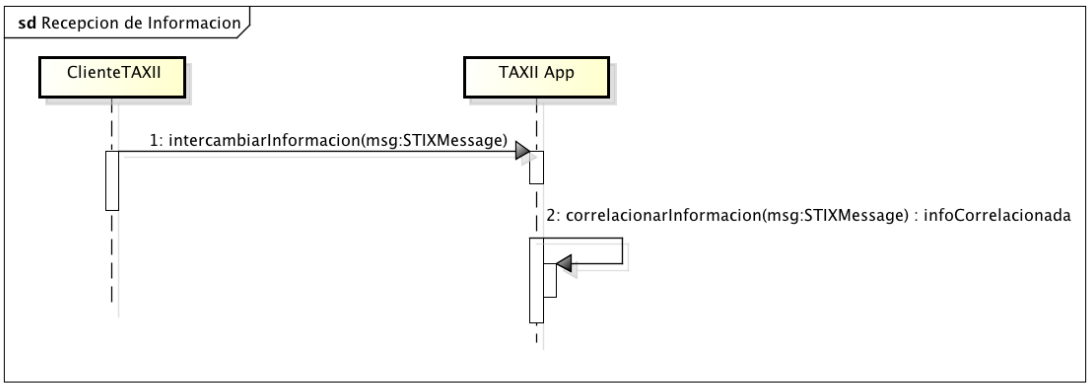

Figura 13 - Caso de uso de recepción de información

En este caso de uso un cliente TAXII en otra organización envía información a TAXII App. Luego la aplicación correlaciona la nueva información con la ya existente en el sistema.

4.2.7 Envío de información

Nombre	Envío de información
Actor	TAXII App
Descripción	Este caso de uso se da cuando el sistema desea enviar información a otro cliente TAXII. El envío de información se realiza porque el cliente se subscribió al TAXII Data Feed del sistema. Esto se realiza por medio del Inbox Service del cliente. El intercambio es iniciado por el sistema.

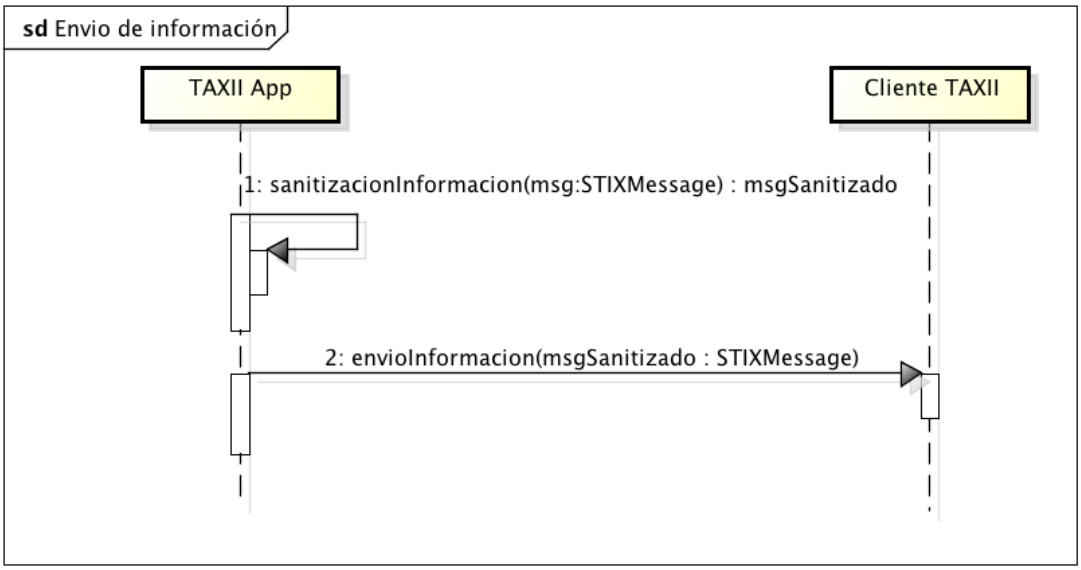

Figura 14 - Caso de uso de envío de información

En este caso de uso TAXII App se comporta como el Actor y desea enviar nueva información a un cliente TAXII. Para ello lo primero que debe hacer es sanitizar la información. Luego envía la información representada en la forma de un mensaje STIX. Esto se ve en la figura 14.

4.2.8 Poll de información

Nombre	Poll de información
Actor	TAXII App
Descripción	Este caso de uso se da cuando un cliente desea recibir información de un productor TAXII, en este los intercambios son iniciados por el cliente que contacta al Poll Service del productor.

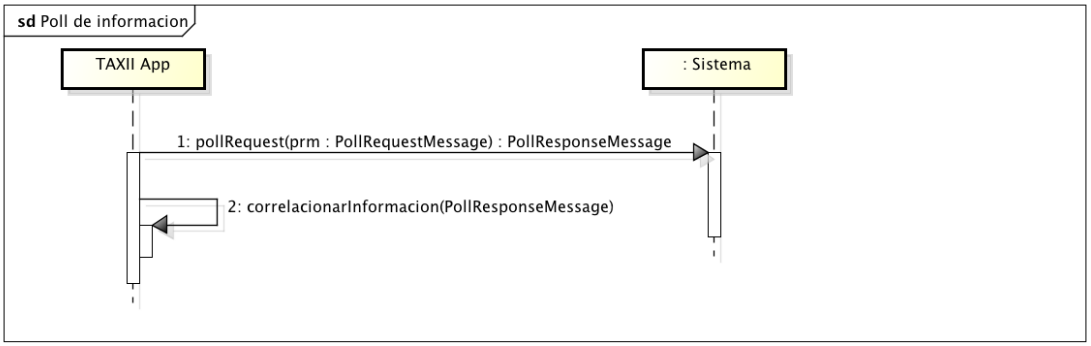

Figura 15 - Caso de uso de poll de información

En la figura 15 se ve el caso de uso de poll de información. En este TAXII App realiza el pedido de información a otro cliente TAXII por medio de mensajes Poll Request. Cuando obtiene la información esta se correlaciona con los datos existentes en el sistema.

También se deben considerar los casos de uso provistos por RTIR para el seguimiento y manejo de los incidentes los cuales no serán especificados en este documento ya que se pueden encontrar en [RTIR]. Dichos casos de uso permiten el manejo de *tickets*, *queues* y gestión de usuarios.

Con RTIR se especifica un *workflow* para el trabajo con los *tickets* en organizaciones de seguridad. Dicho *workflow* comienza cuando se reporta un incidente, dicho reporte de incidente se asocia a un incidente o se crea uno nuevo. Los incidentes tratan de registrar toda la información necesaria para resolver el problema. De los incidentes se pueden iniciar investigaciones para trabajar con otras organizaciones. También se pueden crear *blocks* para mantener un registro de las acciones realizadas para mitigar el incidente.

References

[1] D. Rolsky D. Chamberlain J. Vincent, R. Spier and R. Foley. *RT Essentials*. A. Randal and T. Apandy, 2005.