# Análisis del problema

## Introducción

Este documento presenta los requerimientos que se identificaron junto a los casos de uso necesarios para resolver dichos requerimientos. Además se fundamenta el porqué utilizar las herramientas seleccionadas.

El objetivo de la solución es permitir compartir información con socios de confianza para permitir la identificación precisa de amenazas. Por medio de dicha colaboración se permite tener evidencias específicas que den indicios de una entidad maliciosa afectando la organización. Con la información adecuada se puede mitigar o erradicar el problema.

Esta herramienta permitiría un intercambio mas eficaz del que existe hoy en día dado que agilizaría los tiempos necesarios para el intercambio. Dicha mejora se obtiene por la utilización de métodos automatizados y estandarizados.

## Porque utilizar TAXII y STIX?

El lenguaje STIX nos provee una representación estructurada de información de cyber inteligencia que es más expresiva que las utilizadas en la actualidad, consta de una mayor flexibilidad y extensibilidad. La representación de la información utilizada permite el uso de herramientas de automatización sin perder la posibilidad de que la información sea legible.

STIX facilita el intercambio de información entre organizaciones, comunidades y productos o servicios. Dicho intercambio se realiza por medio de TAXII, protocolo que define un conjunto de servicios y mensajes que permiten el intercambio de información entre organizaciones. El intercambio realizado con TAXII permite la detección, prevención y mitigación de amenazas.

También es importante destacar que STIX facilita la descripción y extensibilidad de evidencia y se integra con otras iniciativas de MITRE como lo son MAEC y CAPEC. MITRE ha logrado integrar en STIX estas especificaciones en lugar de reinventar estos componentes. En STIX también se integran otros lenguajes comúnmente utilizados en la comunidad y que tienen propósitos similares, como lo es OpenIOC.

Como STIX es un lenguaje XML hereda ciertas propiedades de estos, es un lenguaje extensible, simple y fácil de procesar.

Además el lenguaje STIX provee expresividad y flexibilidad para expresar intrusiones, técnicas utilizadas por los adversarios, identificación de éstos entre otras características.

## Porque utilizar RTIR?

RTIR es un sistema de manejo de incidentes diseñado para ser utilizado por CERTs y 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. RTIR cuenta además con una comunidad de usuarios grande cuya característica principal es el nivel técnico de estos.

Distintos CERTs y 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 CERTs y CSIRTs.

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 mas 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 se busca utilizar RTIR por las razones explicadas anteriormente, 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.

## Selección del modelo

Durante el relevamiento de requerimientos se decidió que el modelo a implementar seria el Peer To Peer, esto se debe a que la organización no es gubernamental y tampoco es una organización coordinadora de esfuerzos. El CSIRT-Tilsor presenta la característica de ser una organización de investigación que busca tener un contacto directo con otros CSIRTs.

Otro factor que contribuye a dicha decisión es la capacidad que tiene el CSIRT-Tilsor de generar y consumir información.

## Análisis de requerimientos

La herramienta que se desea desarrollar busca integrarse con RTIR para realizar un seguimiento de incidentes de seguridad. Esta herramienta debe permitir el intercambio de indicadores entre dos organizaciones, dicho intercambio se realiza por medio de TAXII y la información se codifica utilizando STIX.

La herramienta debería dar la posibilidad de interactuar por medio del RTIR con otro CSIRT. En dicha interacción se podría realizar el manejo de incidentes intercambiando información referente a éstos entre los CSIRTs. En dichos intercambios se podría dar información sobre la identificación, solución, atacantes que participaron en el incidente, etc. Dicha información permite expresar de una mejor los incidentes identificados. Cabe recordar que dichos intercambios hoy en día se dan principalmente por medio de foros, mail o comunicaciones telefónicas. Se puede ver que la creación de una herramienta de estas características permitiría un manejo centralizado de la información facilitando el trabajo de los analistas.

Debe existir la posibilidad de que un analista ingrese nueva información sobre un incidente al sistema. Luego dicha información debe ser compartida con otra organización. El ingreso de nueva información sobre incidentes puede ser realizada desde el RTIR y luego se debe realizar el intercambio por medio de TAXII. Particularmente dicha información se representará como un cyber observable en el sistema, este será ingresado por el usuario.

A pesar de que exista integración con RTIR, se desea mantener una base de datos separada para el cliente TAXII. Dicha base de datos debe tener la posibilidad de representar objetos STIX y Cybox que sean intercambiados por el cliente TAXII. Esto es deseable para tener la posibilidad de realizar un mejor análisis de la información intercambiada.

Si bien se cuenta con información en bases de datos separadas debe ser posible realizar un mapeo entre incidentes del RTIR e información que esté almacenada en la base de datos del cliente TAXII. Seria de interés poder ver cierta información almacenada en la base de datos de TAXII en el RTIR para poder presentársela a un analista y que éste tenga la información necesaria para realizar un análisis de ésta.

Una base de datos separada le da al cliente TAXII independencia, permitiéndole ser usado con otras herramientas similares a RTIR. Al ser independiente de RTIR u otras herramientas se pueden realizar extensiones al cliente con facilidad sin afectar el sistema. Las nuevas extensiones se busca que sean módulos nuevos e independientes que agreguen funcionalidades al sistema.

Uno de los módulos que es deseado que exista desde la concepción del sistema debe permitir la sanitizacion de la información. Dicha sanitizacion debe alimentarse de políticas definidas por la organización. El módulo debe realizar un análisis de la información previo al intercambio el cual filtre datos sensibles en la información que se intercambia. Luego de dicho análisis la información se puede intercambiar entre las organizaciones.

Otro módulo que se desearía agregar es uno de correlación de cyber observables, este debe poder identificar objetos que representen la misma problemática y agruparlos de forma adecuada.

De lo anterior podemos resumir en los siguientes requerimientos funcionales:

|  |
| --- |
| Requerimientos funcionales |
| * Agregar políticas de sanitizacion de información. * Aplicación de las políticas de sanitizacion para la información intercambiada * Realizar el intercambio de información de seguridad representada con STIX. * Tener la posibilidad de crear información de incidentes de seguridad en el sistema. * Realizar un seguimiento y manejo de incidentes de seguridad. * La herramienta debe implementar un modelo peer-to-peer de intercambio de información. * Se desea poder interactuar con otro CSIRT por medio del RTIR. * Tener un módulo de correlación de cyber observables. |

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. Un ejemplo de esto es un modulo de correlación de cyber observables. * La herramienta debe mantener información en una base de datos independiente a la de RTIR. Dicha base de datos debe poder representar objetos STIX. Estos objetos podrían ser intercambiados o no. |

## Actores y Casos de Uso

### 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. |

### Casos de uso

|  |  |
| --- | --- |
| Nombre | ABM de políticas |
| Actor | Analista |
| Descripción | Este caso de uso comienza cuando el analista desea ingresar nuevas políticas con las cuales desee filtrar la información que se desea intercambiar con otras organizaciones. |

|  |  |
| --- | --- |
| Nombre | ABM de servicios TAXII |
| Actor | Analista |
| Descripción | Este caso de uso comienza cuando el analista desea ingresar servicios TAXII de otras organizaciones en el sistema. Estos serán utilizados para lograr el intercambio de información. |

|  |  |
| --- | --- |
| Nombre | Ingreso información |
| Actor | Analista |
| Descripción | Este caso de uso comienza cuando el analista desea registrar nueva información en el sistema. Para ello debe ingresar la información que desea ingresar al sistema. Entre la información que puede desear ingresar se encuentran IPs, hash de archivos, descripciones de amenazas, etc. El manejo podría realizarse por medio de los incidentes de RTIR. |

|  |  |
| --- | --- |
| 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. |

|  |  |
| --- | --- |
| 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. |

|  |  |
| --- | --- |
| Nombre | Envío de información |
| Actor | Cliente TAXII |
| Descripción | Este caso de uso se da cuando el sistema desea enviar información a otro cliente TAXII. El envió 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. |

|  |  |
| --- | --- |
| Nombre | Poll de información |
| Actor | Cliente TAXII |
| Descripción | Este caso de uso se da cuando un cliente desea recibir información del sistema en un intercambio iniciado por él. Este intercambio se realiza por medio del Polling Service del sistema. |

|  |  |
| --- | --- |
| Nombre | Poll de información a un cliente TAXII |
| Actor | Cliente TAXII |
| Descripción | Este caso de uso se da cuando el sistema desea recibir información de un cliente TAXII en un intercambio iniciado por él. Este intercambio se realiza por medio del Polling Service del sistema. |

## Comportamiento de casos de uso

### Diagrama de casos de uso

En el siguiente diagrama se ve en resumen los actores y casos de uso del sistema

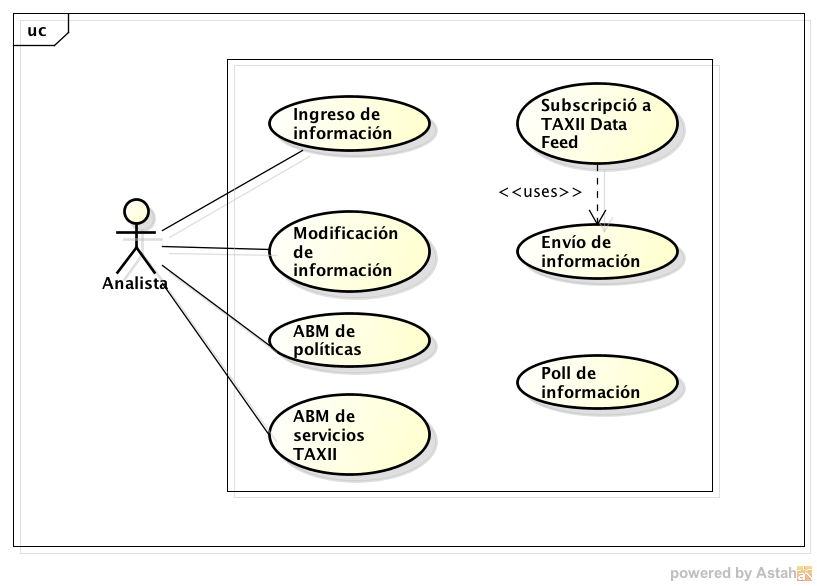


Figura 1 - Diagrama de caso de uso

### Diagramas de Secuencia del Sistema

A continuación se presentan los diagramas de secuencia del sistema para los casos de uso. En los casos de uso que son similares no se presentan los diagramas.

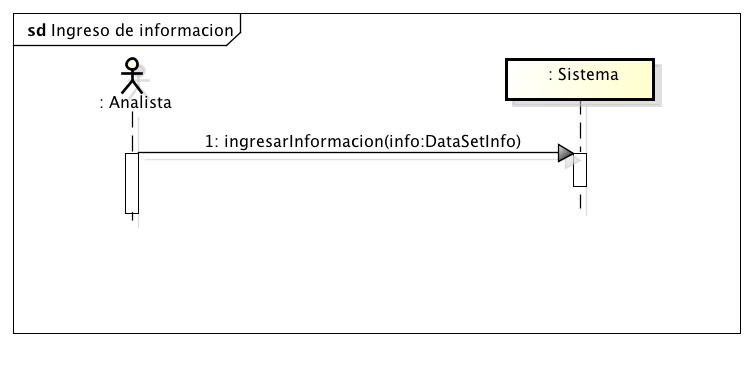


Figura 2 - caso de uso de ingreso de información

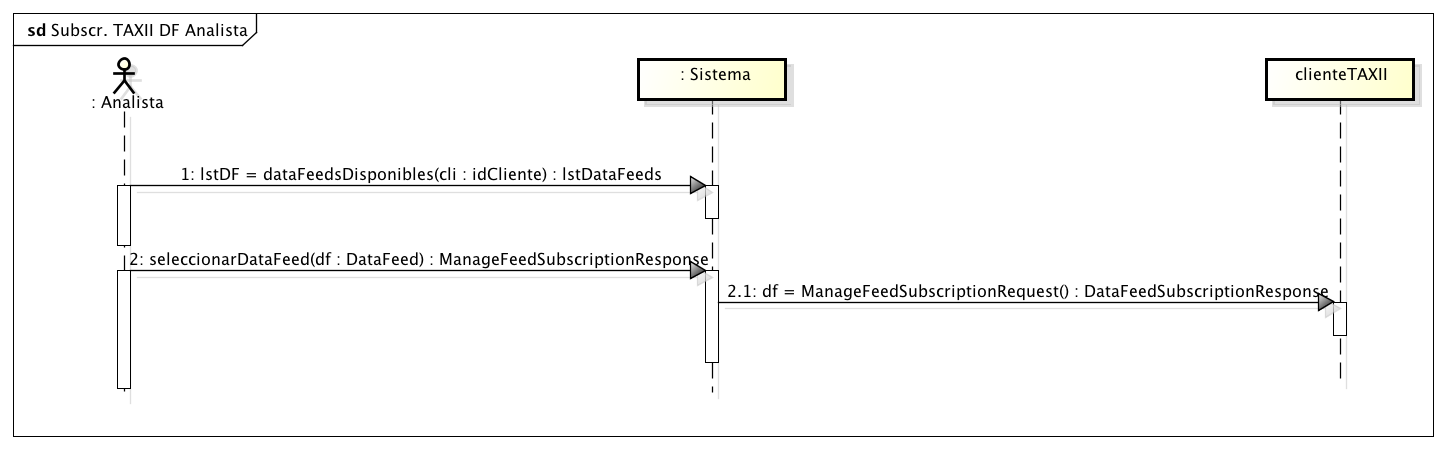


Figura 3 - Caso de uso subscribirse a un Data Feed

### 

Figura 4 - Caso de uso de recepción de información

### 

Figura 5 - Caso de uso poll de información

### Contratos

|  |  |
| --- | --- |
| Nombre | ingresarInformacion |
| Operación | ingresarInformacion(info:DataSetInfo) |
| Entrada | Info representa los datos de la información que se desea ingresar al sistema. |
| Salida | No aplica |
| Descripción | Ingresa al sistema la información que el analista desee agregar. |

|  |  |
| --- | --- |
| Nombre | dataFeedsDisponibles |
| Operación | lstDF := dataFeedsDisponibles(cli : idCliente) : lstDataFeed |
| Entrada | Se pasa como parámetro el id del cliente en el sistema. |
| Salida | Se retorna una lista de los DataFeeds en dicho sistema. |
| Descripción | La operación retorna una lista con los DataFeeds existentes en el cliente pasado como parámetro. |

|  |  |
| --- | --- |
| Nombre | seleccionarDataFeed |
| Operación | seleccionarDataFeed(df : DataFeed) : msg |
| Entrada | El parámetro df representa un DataFeed en un cliente TAXII. |
| Salida | Se retorna un mensaje de éxito o error. |
| Descripción | La operación trata de suscribir el sistema a un nuevo TAXII Data Feed en un cliente TAXII. |

|  |  |
| --- | --- |
| Nombre | ManageFeedSubscriptionRequest |
| Operación | Df := ManageFeedSubscriptionRequest() : DataFeedSubscriptionResponse |
| Entrada |  |
| Salida | Se retorna un mensaje Feed Subscription Response Message con el resultado de la operación. |
| Descripción | La operación se lleva a acabo entre un cliente TAXII y el otro. El cliente trata de subscribirse en el otro para así poder intercambiar información. |

|  |  |
| --- | --- |
| Nombre | intercambiarInformacion |
| Operación | intercambiarInformacion(msg:STIXMessage) |
| Entrada | Se recibe como parámetro un mensaje STIX. |
| Salida |  |
| Descripción | La operación envía al Inbox Service de otro cliente un mensaje STIX. Este incluye la información de seguridad a intercambiar. |

|  |  |
| --- | --- |
| Nombre | pollRequest |
| Operación | pollRequest(prm:PollRequestMessage) : pollResponseMessage |
| Entrada | Prm representa la información que se desea recibir del servidor. |
| Salida | Se retorna la información que se pidió por medio de prm. |
| Descripción | La operación retorna la información deseada, el prm es el que identifica la información en el servidor. |