# Análisis

## 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.

## Motivación

## En el transcurso del proyecto se identificaron distintos problemas que obstaculizan el intercambio de información entre las organizaciones. Dichas problemáticas afectan la reputación, seguridad y la capacidad de trabajo de la organización.

## Los grandes volúmenes de información intercambiados afectan la capacidad de trabajo de las organizaciones. Además la información puede provenir de diferentes fuentes, cada una de las cuales 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 de la organización así como su reputación. 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. No se mencionan otros problemas, como por ejemplo establecer un criterio referente a políticas organizacionales que ayuden a identificar organizaciones de confianza, sanitización de la información entre otras.

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 este proyecto.

Se desea desarrollar una herramienta que se integre con alguna de las aplicaciones de gestión de incidentes existentes proveyéndole la posibilidad 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. Además los datos deberían ser sanitizados para que no se comprometa 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 (anteriormente la confianza entre organizaciones se menciono como uno de los problemas del intercambio de información). Durante el estado del arte se investigaron distintos protocolos y lenguajes para la representación de la información, se llego a la conclusión de que ninguna 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 el problema planteado 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. 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 busca que sea realizado por medio del sistema de gestión de incidentes y que se mantenga un mapeo entre el incidente ingresado y la información intercambiada. Esto ayuda en el caso de que se reciba información de otra organización la cual este relacionada con el incidente creado en el sistema de gestión.

De lo anterior se pueden identificar los siguientes requerimientos funcionales:

|  |
| --- |
| Requerimientos funcionales |
| * La herramienta de implementar un modelo peer-to-peer de intercambio de información entre CSIRTs. * 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 - 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 - Requerimientos no funcionales del sistema.

## Herramientas

Luego del estudio del estado del arte, se analizó el problema y se decidieron las herramientas que se utilizarían considerando la aceptación que pudieran tener por parte de la comunidad. Se consideró el desarrollo actual de dichas herramientas analizando el trabajo futuro que puedan tener. A su vez se ha buscado que dichas herramientas cumplan con los objetivos establecidos al comienzo del proyecto.

### 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.

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 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.

### 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. Por medio 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, desde 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.

Otra 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.

Además en la especificación de TAXII se dan distintas estructuras con las cuales se realiza el intercambio. Se definen las llamadas “TAXII Data Collections” que son conjuntos de información de seguridad que pueden ser intercambiados utilizando TAXII. Dichas colecciones de datos pueden ser conjuntos ordenados de información en los cuales el criterio de ordenación es un timestamp (“TAXII Data Feeds”) o conjuntos desordenados (“TAXII Data Sets”). Es necesario indicar que en todos los casos la información que se intercambia es estructurada. 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 la comunidad y busca convertirse en un estándar. Por eso es esperable que surjan en un futuro herramientas que utilicen el lenguaje STIX y se realice un intercambio de información por medio de TAXII.

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 representando la información utilizando STIX. Además dicho bloque es el encargado de realizar la sanitización y correlación de información.

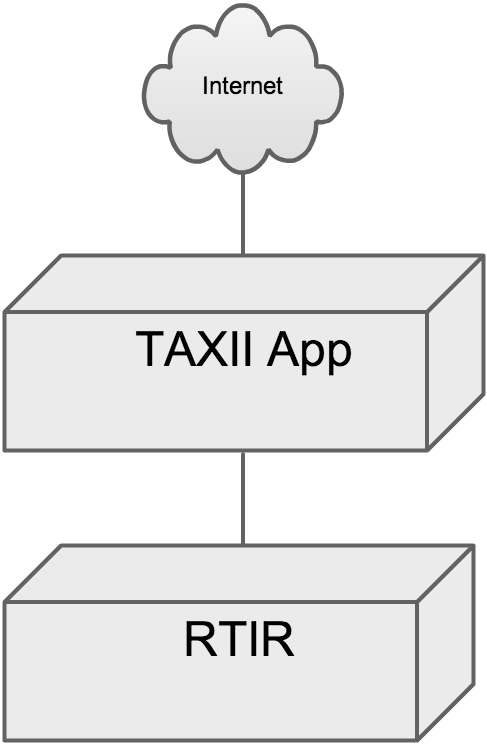


Figura – Esquema de bloques del sistema

## 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 realizar el alta, baja o modificación 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 realizar el alta, baja o modificación de servicio  TAXII de otras organizaciones en el sistema. Estos serán utilizados para lograr el intercambio de información. |

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

|  |  |
| --- | --- |
| Nombre | Selección de 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 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. |

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

También se deben considerar los casos de uso provistos por RTIR para el seguimiento y manejo de los incidentes los cuales no son especificados. Dichos casos de uso permiten el manejo de tickets y queues. Alta y baja de usuarios en RTIR.

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 los que se ha realizado para mitigar el incidente.

## 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

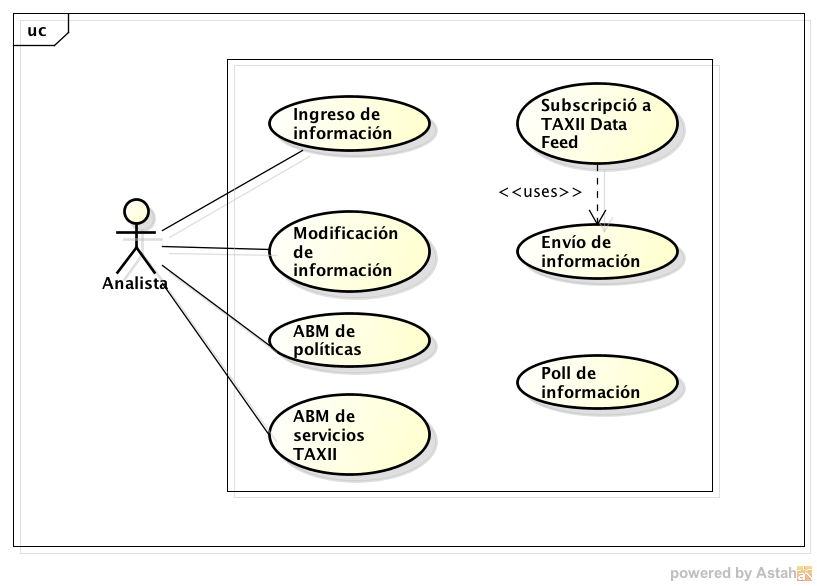


Figura 2 - Diagrama de caso de uso

### 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.

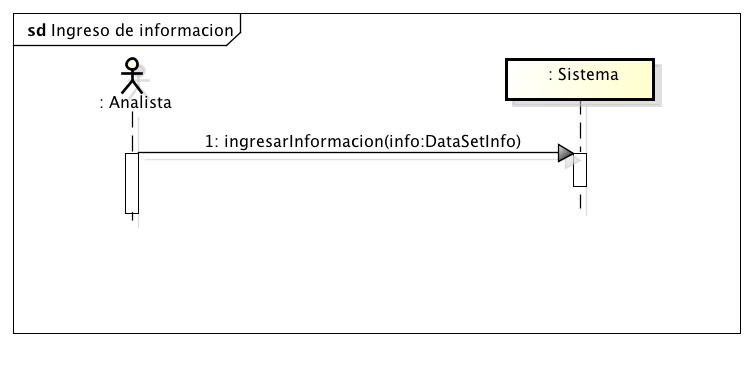


Figura 3 - caso de uso de ingreso de información

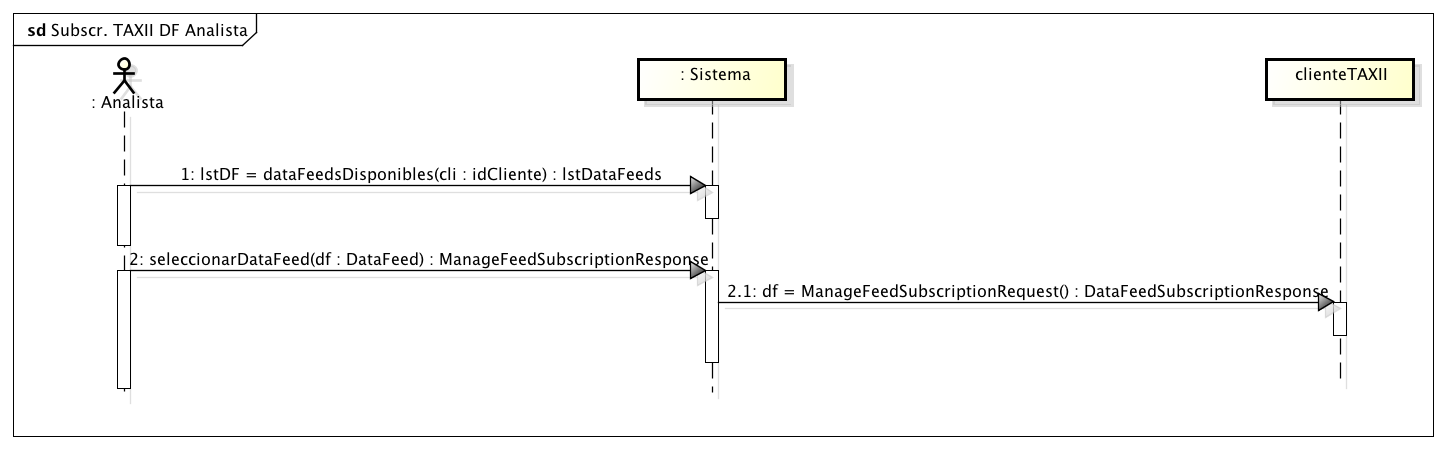


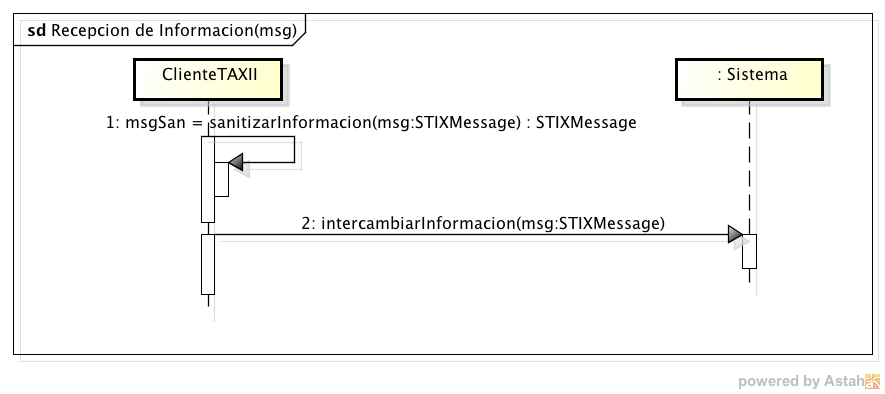
Figura 4 - Caso de uso subscribirse a un Data Feed

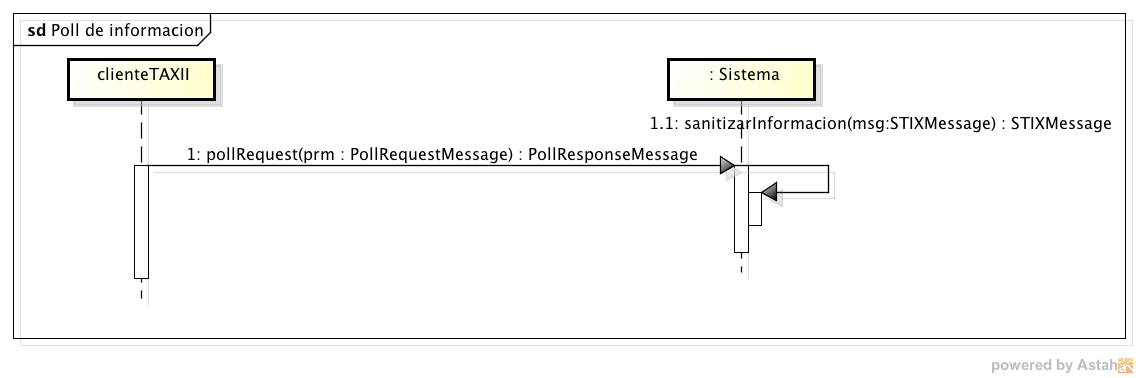
Figura 5 - Caso de uso de recepción de información

Figura 6 - 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. |