/UCIENCIA/.21
IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: Estandarización del intercambio de Inteligencia de Ciberamenazas

Plataforma de Inteligencia de Amenazas para la Red Nacional Universitaria

Threat Intelligence Platform for the National University Network

Esp. Dennis Barrera Pérez [1*], Ing. Darvis Dorvigny Dorvigny [2], Dr. C. Raydel Montesino Perurena [3]

[1] Universidad de las Ciencias Informáticas, Cuba. dbperez@uci.cu

[2] Universidad de las Ciencias Informáticas, Cuba. ddorvigny@uci.cu

[3] Universidad de las Ciencias Informáticas, Cuba. raydelmp@uci.cu

*Autor para la correspondencia. (dbperez@uci.cu)

Resumen

El aumento vertiginoso del uso de las Tecnologías de la Información y la Comunicación (TIC), ha traído consigo que el mundo esté cada vez más interconectado. Dentro de los principales usos de las TIC se encuentran la prestación de servicios, el comercio electrónico, la educación y el intercambio de información en general. De ahí que las personas y las instituciones se han convertido en el blanco perfecto de los ciberdelincuentes para el robo de información sensible, la propagación de código malicioso y la destrucción de los servicios. Cuba no está exenta de esta tendencia, actualmente en el país existen muchas instituciones que son propensas a ser víctimas de ciberataques, poniéndose en riesgo la integridad, confidencialidad y disponibilidad de la información. Un ejemplo de ello es la Red Nacional Universitaria (RedUniv) donde se desarrollan proyectos de aplicación en diversos sectores del país. Con el objetivo de contribuir en el enfrentamiento a los ciberataques, en el presente trabajo se describe una plataforma de inteligencia de amenazas para análisis e intercambio de información de amenazas en RedUniv. La plataforma permite a los

especialistas recolectar, analizar y compartir información sobre patrones de ataques y amenazas de una manera segura y estandarizada. Los datos que se intercambian pueden ser empleados por sistemas detectores de intrusos y cortafuegos. Debido a su enfoque novedoso, se considera que la plataforma contribuye a mejorar la detección de ciberataques, mitigación de vulnerabilidades y la respuesta a incidentes de seguridad en las instituciones de RedUniv.

Palabras clave: plataforma; amenazas; ciberataques.

ABSTRACT

The vertiginous increase in the use of Information and Communication Technologies (ICT) has made the world increasingly interconnected. Among the main uses of ICT are the provision of services, electronic commerce, education and the exchange of information in general. Hence, individuals and institutions have become the perfect target for cybercriminals to steal sensitive information, spread malicious code and destroy services. Cuba is not exempt from this trend, currently in the country there are many institutions that are prone to being victims of cyberattacks, putting the integrity, confidentiality and availability of information at risk. An example of this is the National University Network (RedUniv) where application projects are developed in various sectors of the country. With the aim of contributing to the confrontation with cyberattacks, this paper describes a threat intelligence platform for analysis and exchange of threat information in RedUniv. The platform allows specialists to collect, analyze and share information on attack patterns and threats in a secure and standardized way. The data that is exchanged can be used by intrusion detection systems and firewalls. Due to its novel approach, the platform is considered to contribute to improving the detection of cyberattacks, mitigation of vulnerabilities and the response to security incidents in RedUniv institutions.

Keywords: platform; threats; cyberattacks.

Introducción

El aumento vertiginoso del uso de las Tecnologías de la Información y la Comunicación (TIC), ha traído consigo que el mundo esté cada vez más interconectado. Según una encuesta de ISACA, el 32 % de los participantes afirmó que en 2019 los ciberataques se incrementaron considerablemente con respecto al año anterior, siendo la ingeniería social el vector de ataque más común, el 15 % de los encuestados afirmó haber sido afectado por este método de ataque. Las Amenazas Persistentes Avanzadas (APT) fueron el segundo método más empleado con un 10% de los encuestados, seguido por el ransomware y los sistemas sin parches de seguridad con un 9% cada uno. Los actores de amenazas más frecuentes fueron los cibercriminales con un 22%, seguidos por los hackers con 19 % (ISACA, 2020).

Por otra parte, el 2020 se vio marcado por un nuevo evento de magnitud global, el Coronavirus (Covid-19), el cual fue tomado por los ciberdelincuentes como una oportunidad para el lanzamiento de campañas de spam, phishing y ransomware con temas relacionados con la Covid-19. Según un reporte de Anomali, para el primer trimestre del año, ya se habían observado alrededor de 6000 indicadores maliciosos, al menos 15 campañas de amenazas relacionadas con 11 actores de amenazas o grupos diferentes, distribuyendo 39 familias de malware mediante el empleo de 80 técnicas de ataques diferentes (Anomali, 2020).

En Cuba se realizan grandes esfuerzos por mantener la soberanía tecnológica y avanzar en el proceso de informatización de la sociedad. En la Política Integral para el Perfeccionamiento de la Informatización de la Sociedad (aprobada por el Consejo de Ministros en febrero de 2017), se destacó la necesidad de que las TIC se conviertan en un arma para la defensa de la Revolución y garantice una adecuada seguridad del ciberespacio frente a las amenazas, riesgos y ataques de todo tipo, condición imprescindible para la evolución de este sector (Ministerio de Comunicaciones, 2017).

Actualmente en el país existe la Red Nacional Universitaria del Ministerio de Educación Superior de la República de Cuba (MES) denominada RedUniv, que tiene como objetivo fundamental: promover y coordinar el desarrollo de Redes de Telecomunicaciones y sus servicios; enfocadas al desarrollo científico, educativo y de investigación en los Centros Universitarios y de Investigación, pertenecientes al (MES). La misma permite la interconexión de 22 universidades y 3 centros de ciencia, tecnología e innovación. Un estudio sobre el estado actual de la seguridad informática de las universidades arrojó como resultado que existe poca experiencia por parte de los especialistas en temas de seguridad informática, las soluciones de seguridad existentes son escasas, la información de ataques,

vulnerabilidades y amenazas que se intercambia no se encuentra estandarizada dificultándose el análisis por parte de los especialistas de seguridad y se deben aumentar las acciones de formación especializada en ciberseguridad. Para dar solución a la problemática planteada, se define como objetivo general de la investigación: diseñar e implementar una plataforma de inteligencia de amenazas para la Red Nacional Universitaria que contribuya a elevar los niveles de ciberseguridad de las instituciones.

Métodos o Metodología Computacional

Para el desarrollo de la presente investigación se siguió una estrategia descriptiva, donde se reflejaron los aspectos esenciales y más significativos del objeto de investigación. Se emplearon varios métodos científicos clasificados en teóricos y empíricos, así como técnicas para la recopilación de información. Dentro de los métodos teóricos se encuentra el método **histórico-lógico** y el **dialéctico**, los cuales se emplearon en el análisis de los fundamentos históricos relacionados con la inteligencia de amenazas y el intercambio de información. El método **sistémico** fue empleado en la concepción de la plataforma propuesta. El método **analítico-sintético** se empleó en el estudio del estado del arte sobre las plataformas de inteligencia de amenazas y los estándares para el intercambio de información en el mundo y una síntesis de los elementos analizados.

Para el análisis de los referentes teóricos relacionados con la temática tratada, se realizó un estudio del estado del arte sobre el uso de inteligencia de ciberamenazas (CTI) en las instituciones, así como las principales plataformas de inteligencia de amenazas (TIP) existentes. Para el análisis se tomó como referencia una encuesta realizada por el instituto SANS sobre el uso de CTI en 2020, donde se evidenció que el empleo de esta técnica ha ido creciendo considerablemente. La encuesta permitió comprobar, además, que un número elevado de instituciones han comenzado a establecer y expandir sus programas y productos de ciberinteligencia (Lee, 2020). Como resultado de estos programas se ha hecho muy común el empleo de TIPs. Un TIP es la tecnología emergente que permite a las organizaciones mejorar sus capacidades de inteligencia de amenazas, así como acelerar los procesos de recolectar, analizar, normalizar, enriquecer y compartir información relacionada con amenazas. A continuación, se presenta una tabla resumen de algunos de los TIPs empleados en el mundo organizados por tipo.

Tabla 1. Plataformas de Inteligencia de Amenazas (TIPs). **Fuente:** Elaboración propia.

Nombre	Tipo	Año	Propietario	Sitio Web
Malware Information Sharing Platform (MISP)	Código abierto/ comunidad	2012	CIRCL	http://www.misp-project.org/ https://www.misp-project.org/communities/
Collaborative Research Into Threats (CRITs)	Código abierto	2014	MITRE	https://crits.github.io/ https://github.com/crits
Collective Intelligence Framework (CIF)	Código abierto	2012	CSIRT Gadgets Foundation	https://csirtgadgets.com/collective-intelligence-framework
Malware Attribute Enumeration and Characterization (MAEC v5)	Código abierto	2019	MITRE	http://maecproject.github.io/ https://github.com/MAECProject/
OpenCTI	Código abierto	2019	OpenCTI	https://github.com/OpenCTI-Platform/opencti
Open Threat Exchange (OTX)	Comunitario	2012	Alienvault	https://www.alienvault.com/open-threatexchange
X-Force Exchange	Comunitario	2015	IBM	https://exchange.xforce.ibmcloud.com/
Repositorio Común y Estructurado de Amenazas y Código Dañino (REYES)	Comercial	2017	CCN-CERT	https://www.ccn-cert.cni.es/soluciones-seguridad/reyes.html

Dentro de las plataformas analizadas se identificó REYES como una de las más completas y que cumple con las necesidades de la investigación, sin embargo, el acceso a REYES está restringido solo a aquellas organizaciones que cuentan con un certificado de SAT-INET del CCN-CERT, siendo su uso limitado. Las plataformas CRIST, CIF y MAEC presentan gran utilidad para la recolección y enriquecimiento de indicadores de compromiso, pero carecen de funcionalidades para el intercambio de amenazas, requisito indispensable en la presente investigación. En el caso de OpenCTI y MISP cumplen con los requerimientos de la investigación debido a que ambas permiten gestionar la información de ciberamenazas, pero solo MISP se centra en el intercambio de información de amenazas mediante la creación de comunidades. Sin embargo, su componente para la visualización de amenazas carece de flexibilidad a la hora de realizar análisis complejos y búsquedas avanzadas de IoC.

Resultados y discusión

Con el objetivo de minimizar los esfuerzos en el análisis de amenazas y aumentar la rapidez de las respuestas a incidentes, se propone una Plataforma de Inteligencia de Amenazas para la Red Nacional Universitaria denominada RedUniv-CTI. La plataforma está especialmente ideada para ofrecer un mecanismo estandarizado de intercambio de

información para las distintas instituciones de RedUniv que internamente generan ciberinteligencia. En la plataforma se emplean como elementos principales los eventos, los cuales se encargan de describir las amenazas existentes y están conformadas por un conjunto de características para describir los IoC, a cada una de esas características se les denomina atributos. Los atributos son los encargados de brindar tanta información como sea posible y se dividen en dos clases: categorías y tipos. En la (**Figura 1)**, se muestra una representación de dicho modelo de datos.

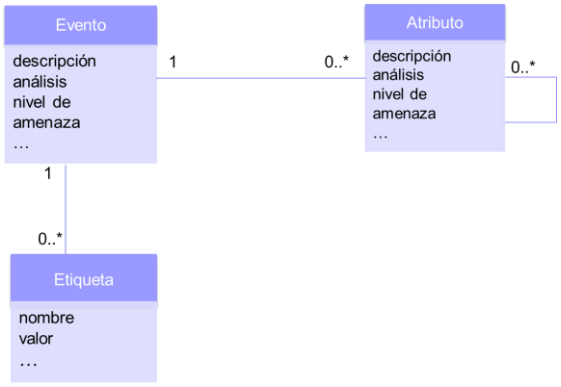

Figura 1. Modelo de datos de la plataforma RedUniv-CTI. **Fuente:** Elaboración propia

Arquitectura de la plataforma RedUniv-CTI

Con el objetivo de incorporar en la propuesta la mayor cantidad de funcionalidades presentes en un TIP ideal, el sistema MISP se integró con varias herramientas de software libre para la recolección de datos y el análisis e intercambio de información de amenazas. En la **(Figura 2)** se presenta la arquitectura definida para la plataforma:

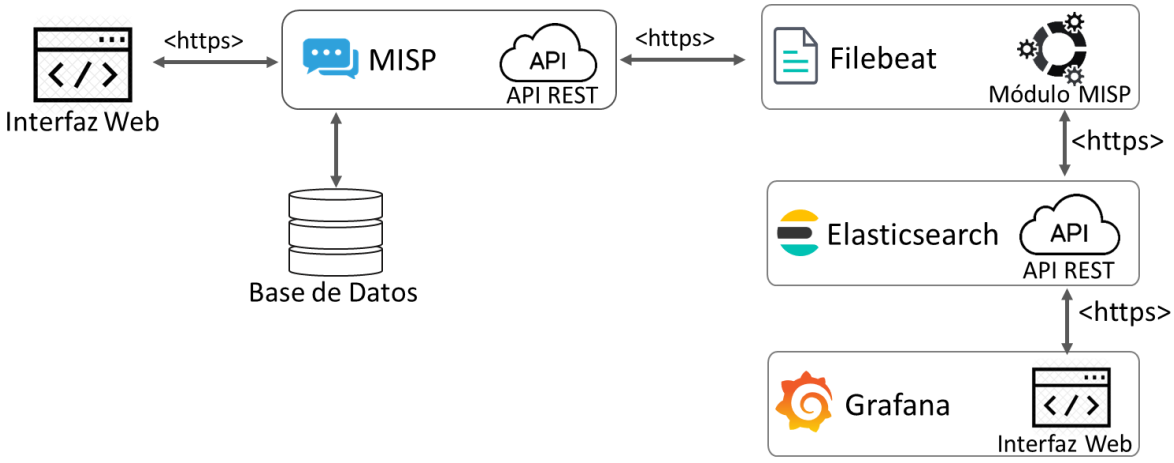

Figura 2. Arquitectura de la plataforma RedUniv-CTI. **Fuente:** Elaboración propia.

A continuación, se presenta una descripción detallada de cada uno de sus componentes:

MISP: Es el componente principal de la plataforma, permite la creación de organizaciones y comunidades de confianzas para el intercambio de amenazas. Brinda la posibilidad a los especialistas de recolectar IoC de fuentes abiertas de internet para la detección y análisis de ciberataques (Wagner et al., 2016).

Base de Datos: La base de datos permite almacenar indicadores maliciosos, así como información técnica y no técnica sobre malware, incidentes, atacantes e inteligencia.

Interfaz Web de MISP: Es la interfaz principal de la plataforma, en ella se muestran las diferentes opciones para que los especialistas puedan gestionar las amenazas. En la siguiente figura se muestra un ejemplo de las opciones disponibles para la gestión de un evento correspondiente a varios ciberataques realizados en 2020 empleando temáticas sobre la covid-19:

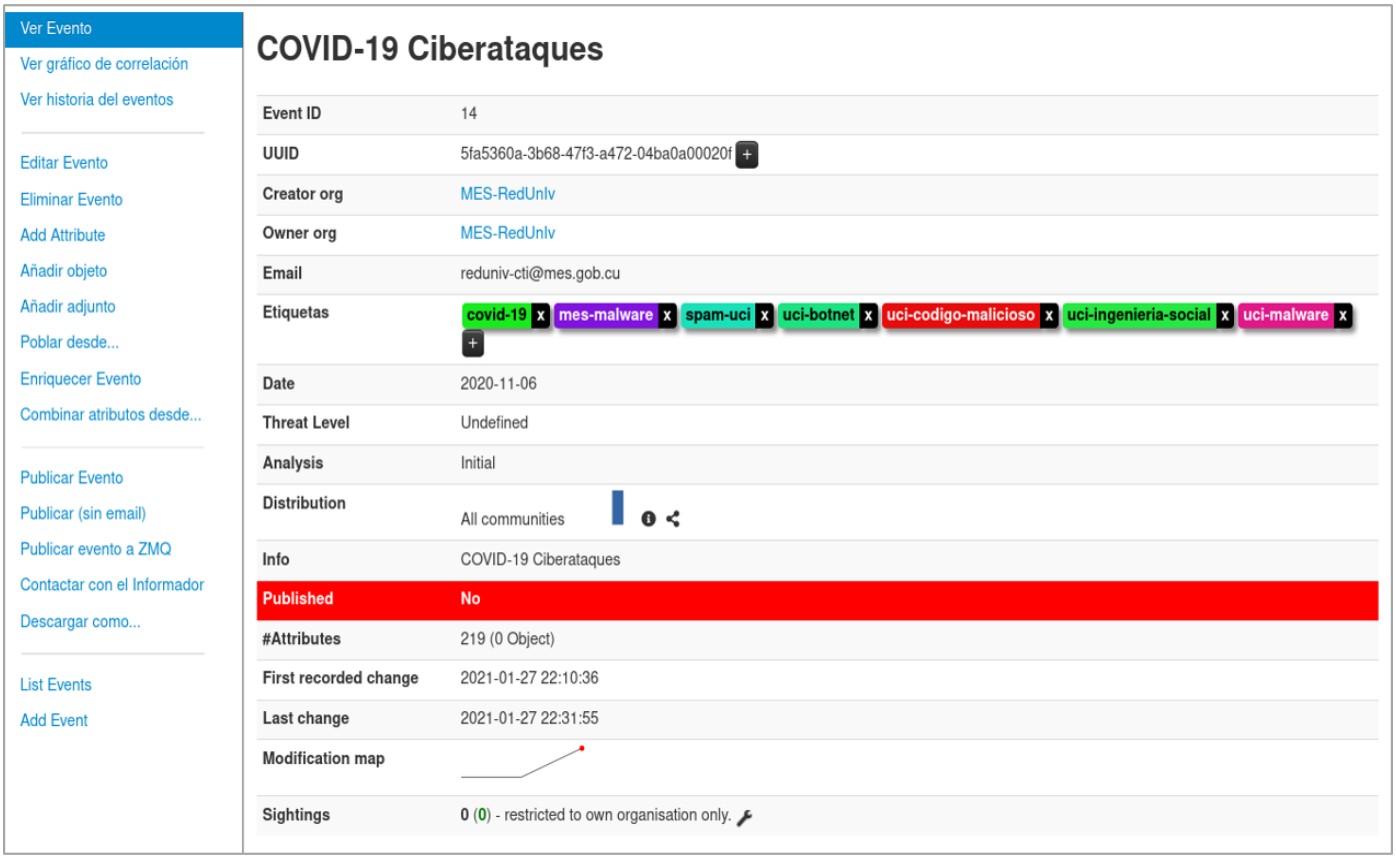

Figura 3. Interfaz web para la gestión de amenazas. **Fuente:** Elaboración propia.

API REST de MISP: La API de MISP permite la interacción con los demás sistemas mediante el protocolo HTTPS, para la conexión con MISP será necesario un código de autorización de Identificador Único Universal (UUID, por sus siglas en inglés) el cual se puede obtener desde la interfaz principal de MISP.

Filebeat: Filebeat es la herramienta (también desarrollada por Elastic) que se utiliza en los servidores clientes para constantemente enviar sus archivos de logs al servidor de Elasticsearch (Elastic, 2020). Su empleo en la plataforma se evidencia en la recolección de IoC desde MISP mediante la API REST para ser enviados a Elasticsearch.

Elasticsearch: Es un motor de analítica de código abierto para todos los tipos de datos, incluidos textos, numéricos, geoespaciales, estructurados y no estructurados (Elastic, 2020). Elasticsearch permite la recolección de gran cantidad de datos obtenidos de MISP como son: direcciones IP, hash de ficheros, URL, dominios. Estos datos son obtenidos desde Filebeat e indexados posteriormente en Elastic a través de su API.

Grafana: Permite visualizar datos de series temporales y obtener un panorama gráfico de situación de una empresa, a partir de datos recolectados (Grafana Labs, 2020). En la plataforma se empleó para recolectar los datos indexados en Elastic mediante la creación de consultas basadas en expresiones regulares. Una vez recolectada la información Grafana permite la creación de paneles personalizados para la visualización de datos, el análisis de tendencia, el filtrado avanzado de IoC mediante el empleo de consultas de agregación como se muestra en la siguiente figura.

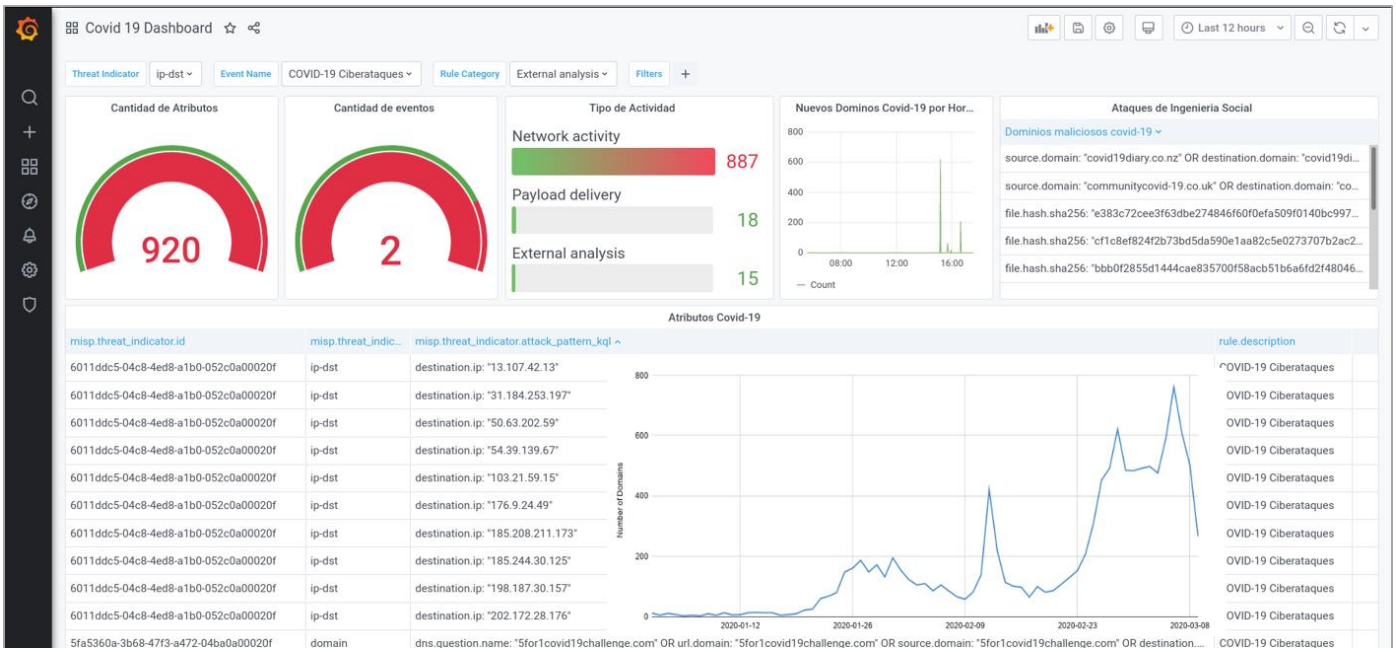

Figura 4. Interfaz web de la herramienta Grafana para la visualización de datos. **Fuente:** Elaboración propia.

Comunidad RedUniv

En la presente investigación se denomina instancia de RedUniv-CTI a cada instalación de la plataforma en una institución. El ambiente colaborativo conformado por todas las instancias se denomina Comunidad de RedUniv-CTI. Los eventos de cada institución pueden ser intercambiados entre varias instancias mediante un mecanismo de sincronización automático. En una instancia de la plataforma, una organización colaboradora puede disponer de múltiples usuarios con distintos niveles de privilegios de visibilidad de la información y con registro de sus actividades. Igualmente, a nivel de organizaciones también se pueden implementar distintos niveles de visibilidad. Aunque en una instancia no se genere información de ciberinteligencia, la misma tendrá el derecho de consumir información compartida en la comunidad. A continuación, se presenta un modelo para el intercambio de información de ciberamenazas en RedUniv-CTI basado en el modelo presentado en (Barrera Pérez et al., 2019).

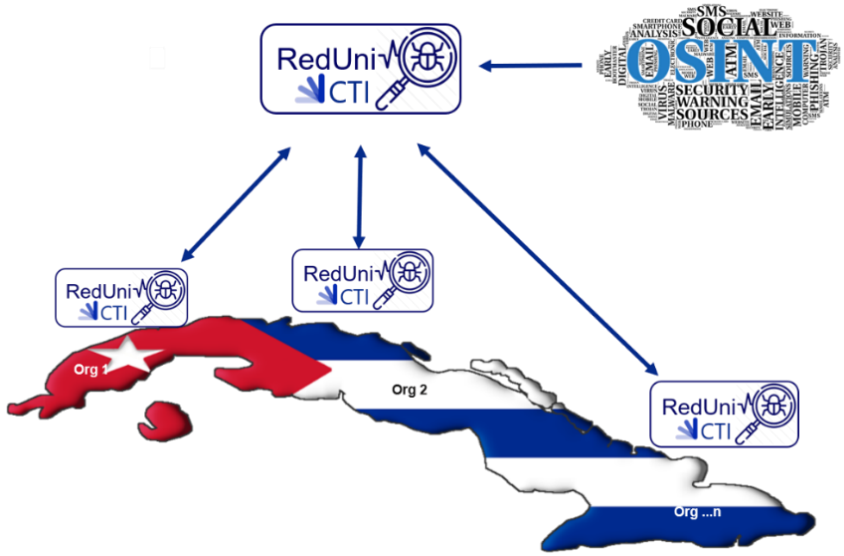

Figura 5. Modelo de intercambio de amenazas definido para la Plataforma de Inteligencia de Amenazas RedUniv-CTI.
Fuente: Elaboración propia.

Conclusiones

- El análisis de los referentes teóricos relacionados con el objeto de estudio, permitió identificar que no existen plataformas adaptables al entorno universitario cubano, por lo que la plataforma propuesta se considera un aporte práctico en la presente investigación.

- El diseño e implementación de una plataforma de inteligencia de amenazas basada en referencias internacionales posibilitó la obtención de una solución acorde a las características del entorno universitario cubano.
- El despliegue de la plataforma en la Universidad de las Ciencias Informáticas y los indicadores obtenidos permitieron validar la factibilidad de la propuesta.

Referencias

- Anomali. (2020). ¿Qué es una plataforma de inteligencia contra amenazas (TIP)? https://www.anomali.com/es/what-is-a-tip
- Barrera Pérez, D., González Brito, H. R., & Sánchez Borrell, Y. (2019). Modelo para la detección de ataques a las aplicaciones WEB e intercambio de ciberamenazas. Revista Telemática, 17(2), 71–80. https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/306
- Elastic. (2020). ¿Qué es Elasticsearch? | Elastic. https://www.elastic.co/es/what-is/elasticsearch
- Grafana Labs. (2020). Grafana Features | Grafana Labs. https://grafana.com/grafana/
- ISACA. (2020). State of Cyber 2019, Part 2: Current Trends in Attacks. https://www.isaca.org/bookstore/state-of-cybersecurity-2019/whpsc192
- Lee, R. M. (2020). The Evolution of Cyber Threat Intelligence (CTI): SANS CTI Survey. https://go.eclecticiq.com/resources/sans-cyber-threat-intelligence-survey-2020
- Ministerio de Comunicaciones. (2017). POLÍTICA INTEGRAL PARA EL PERFECCIONAMIENTO DE LA INFORMATIZACIÓN DE LA SOCIEDAD EN CUBA. 91, 399–404.
- Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016). MISP - The design and implementation of a collaborative threat intelligence sharing platform. WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, Co-Located with CCS 2016, 49–56. https://doi.org/10.1145/2994539.2994542