

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**

**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**



**XVIII SIMPOSIO INTERNACIONAL DE INGENIERÍA  
ELÉCTRICA. "SIE 2019"**

**Cleaning Center. Un nuevo servicio de ETECSA**

*Cleaning Center. A new ETECSA service*

**Javier Brooks Miranda<sup>1</sup>**

1-Javier Brooks Miranda. ETECSA, Cuba. [javier.brooks@etecsa.cu](mailto:javier.brooks@etecsa.cu):

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**

**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**



**Resumen:** Con el fin de garantizar la ciberseguridad aparejado con la creciente demanda de servicios de acceso a internet en la que está inmersa la Empresa de Telecomunicaciones de Cuba (ETECSA), el Centro de Operaciones de Seguridad de la Dirección de Operaciones de Seguridad diseña, conforma y pone en práctica una plataforma para el análisis, monitoreo y control de tráfico en los puntos de presencia de los servicios de la red. Los resultados y experiencias obtenidas en este despliegue han sido el precedente del Cleaning Center (Centro de limpieza), un nuevo servicio que ofrece ETECSA que permitirá a los clientes emplear una protección sobre su red sin necesidad de adquirir ni desarrollar en sus instalaciones, costosas soluciones hardware y software.

Cleaning Center está diseñado como parte del servicio de acceso a Internet, de forma que la protección frente amenazas sea una característica esencial del servicio de acceso. Con este servicio, los usuarios obtendrán una protección completa de acceso a internet y un análisis detallado de los eventos de seguridad asociado a sus redes. Completamente diseñado para facilitar el trabajo del analista de seguridad, Cleaning Center proveerá a los usuarios de cuadros de mandos que suministran una panorámica de los principales ataques, programas malignos, fuentes maliciosas, entre otros. Cleaning Center será un servicio integrado a los ya brindados que permitirá el control del tráfico de la red ante las amenazas actuales y futuras como parte importante de la evaluación de las prioridades a tener en cuenta en las crecientes medidas de seguridad.

**Palabras Clave:** Amenazas, Seguridad, Plataforma, Control, Trafico, Servicio

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”

DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.



*Abstract: In order to guarantee cybersecurity coupled with the growing demand for Internet access services in which the Telecommunications Company of Cuba (ETECSA) is immersed, the Security Operations Center of the Security Operations Directorate designs, conforms and It implements a platform for the analysis, monitoring and control of traffic at points of presence of network services. The results and experiences obtained in this deployment have been the precedent of the Cleaning Center, a new service offered by ETECSA, which allows customers to use a protection over their network without having to buy or deploy in their facilities, expensive hardware and software solutions.*

*Cleaning Center is designed as part of the Internet access service, so that protection against threats is an essential feature of the access service. With this service, users will obtain complete protection of Internet access and a detailed analysis of the security events associated with their service networks. Completely designed to facilitate the work of the security analyst, Cleaning Center will provide users with dashboards that provide an overview of the main attacks, malware, malicious sources, among others. Cleaning Center will be an integrated service to those already provided that will allow the control of network traffic in the face of current and future threats as an important part of the evaluation of the priorities to be taken into account in the increasing security measures.*

**Keywords:** *Threats, Security, Platform, Control, Traffic, Service*

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**

**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**



## **1. Introducción**

El monitoreo de seguridad en las redes de servicio de acceso a internet se hace necesario en todo tipo de empresas debido a las demandas en las exigencias de las operaciones y la complejidad en sus redes de cómputo. El análisis, monitoreo y control de tráfico toma mayor importancia y debe tener un carácter proactivo, con el fin de evitar problemas a futuro.

La Plataforma de Monitoreo y Control del Tráfico Malicioso (PMCTM) en las redes de servicio, constituyen el soporte tecnológico fundamental para el cumplimiento de la misión y funciones del Centro de Operaciones de Seguridad (COS) de la Empresa de Telecomunicaciones de Cuba SA (ETECSA): “realizar el monitoreo continuo del estado de la seguridad informática, la detección oportuna de las amenazas, ataques e incidentes de seguridad relacionados con estas y la gestión de la respuesta ante las mismas”.

### **1.1 Antecedentes y problemática**

En marzo de 2014 se realizan ataques de desconfiguración de servicios a usuarios y entidades nacionales con acceso a los servicios de Internet. Como parte de la investigación de estos incidentes de seguridad ocurridos, se evidenció la falta de visibilidad del tráfico malicioso en las redes de servicio y la necesidad de disponer de un sistema para el control de dicho tráfico.

Un mes más tarde, se toma la decisión de realizar un monitoreo del tráfico malicioso que constituyó el primer paso de un programa de trabajo para el desarrollo de un sistema de inteligencia de amenazas, que permitiera identificar indicadores de compromiso. Se desplegó un sensor con el IDS (Sistema de Detección de Intrusos) Suricata, al que se le hizo llegar, a través una red privada de seguridad, el tráfico de puertos espejos de los diferentes Puntos de Presencia de los Servicios(PoP). Simultáneamente se contrataron las bases de datos, con reglas para la detección de amenazas con este IDS que se actualizan sistemáticamente.

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**

**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**



En ese mismo año, la necesidad de prestar el servicio Wi-Fi a la población en espacios públicos y con un carácter extensivo hicieron que se modificarán algunas de las premisas iniciales expandiendo la posición no solo a las salas de navegación sino también a sitios de alta concentración de usuarios en los espacios públicos del país.

La proyección de un sistema de comunicación que posibilite el acceso inalámbrico a Internet en diferentes puntos del país, así como el despliegue de un conjunto de subsistemas que apoyen la operación; obliga a que ETECSA expanda el Proyecto WLAN con tecnología Wi-Fi. El no cumplimiento, en la oferta del proveedor seleccionado, de los requerimientos de seguridad de-mandados y la necesidad de ETECSA de desplegar estos servicios con la mayor rapidez posible, trajo como consecuencia la propuesta de una plataforma de monitoreo y control de tráfico para la detección y mitigación de amenazas e incidentes de seguridad.

En enero del 2015 se le asigna al COS la responsabilidad de conceptualizar una plataforma para los controles de ciberseguridad necesarios para el servicio WLAN y seis meses más tarde este servicio se comienza a brindar con dicha plataforma. Con el transcurso del tiempo, esta primera solución resulto ineficiente teniendo en cuenta el crecimiento del tráfico maliciosos a monitorear y controlar, en correspondencia con la ampliación de dichos servicios, por lo cual se ha ido mejorando y constituye una tarea permanente del COS.

Para el lanzamiento del servicio WLAN, se conceptualizó y ejecutó una solución de control de tráfico no deseado, basado en software libre (pFsense y Suricata), conocida como Mambí1.0. Esta solución a largo plazo se vería afectada por el creciente nivel de tráfico ya que se pudo comprobar que a partir de un tráfico mayor de 1.5 Gbps, presentaba pérdidas de paquetes a procesar.

Para suplir esta deficiencia y seguir ofreciendo el nivel de seguridad requerido, se implementa el Mambí2.0. Esta versión está basada en un IDS Suricata con la funcionalidad de IPS (Sistema de Prevención de Intrusos) lo cual permite continuar con las características propias del firewall pFsense de la solución anterior en cuanto a bloqueo

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**

**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**



de paquetes y posibilita además trabajar con tráfico de hasta 10 Gbps. También se complementa con herramientas como NETDATA y Grafana para la visualización de datos de interés (tráfico, paquetes bloqueados, rendimiento de RAM y CPU, etc.) y está perfectamente integrada con el stack de Elastic (ELK, Elasticsearch-Logstash-Kibana) para la visualización de los eventos y alertas de seguridad.

La PMCTM garantiza un nivel de seguridad en el monitoreo y control del tráfico malicioso actualmente en explotación en redes de servicio Nauta y de acceso Wifi en espacios públicos, así como los servicios ADSL Hogar y el acceso a Internet desde redes móviles (2G, 3G y 4G).

## **2. Contenido**

Cuando hablamos de amenazas, según (Capraru Pons, 2016), nos referimos a aquellos cambios del entorno por parte de un humano, una máquina o simplemente, un suceso que pueda comprometer la seguridad de determinada empresa. Las amenazas pueden ser detectadas antes, después o durante el ataque. Para ello, las intervenciones posibles son:

- **Prevención:** se trata de mecanismos que ayudan a mejorar la seguridad en un funcionamiento rutinario.
- **Detección:** dispositivos encargados de revelar posibles violaciones de las políticas de seguridad.
- **Recuperación:** mecanismos preparados para activarse cuando se produce un ataque y restaurarlo a su estado de funcionamiento normal.

Según las amenazas, podemos clasificarlas según:

- **Origen:**
  - **Amenazas Internas:** pueden ser causadas por un uso incorrecto por parte de la plantilla o por personal técnico, que, por motivos de necesidad en el trabajo, tienen acceso a partes críticas de la red. Los sistemas de prevención contra intrusiones o los cortafuegos, no son eficientes contra amenazas internas, ya que no están guiados al tráfico interno.

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**

**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**



- Amenazas Externas: son aquellas que proceden del exterior. No se tiene información evidente sobre la red y los atacantes deben primero entender cómo funciona para luego buscar una manera para asaltarla. El analista de seguridad, tiene la oportunidad de prevenir de manera correcta este tipo de ataques.
- Efecto:
  - Estafa, Robo de dinero
  - Suplantación de identidad
  - Publicidad de datos personales
  - DDOS de los sistemas
  - Destrucción de información confidencial
- Medio:
  - Virus: malware que intenta alterar la actividad normal del dispositivo, sin el consentimiento del usuario.
  - Phising (Suplantación de identidad).
  - Ingeniería Social.

Las plataformas de seguridad actualmente en una empresa están en constante cambio y desarrollo. ETECSA como principal proveedor de servicios tiene el deber, el compromiso y la misión de brindar servicios de telecomunicaciones que satisfagan las necesidades de los clientes y la población. Por tanto, los sistemas de análisis, monitoreo y control de tráfico, están en constante perfeccionamiento atendiendo a los requerimientos a la hora de ofrecer un determinado servicio. A continuación, se presentan un conjunto de herramientas utilizadas para llevar a cabo el control del tráfico malicioso en los puntos de presencia de los servicios de acceso a internet, las cuales constituyen la base del Cleaning Center.

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”



DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.

## 2.1 Suricata

Suricata es un motor de detección de amenazas gratuita de código abierto, una herramienta madura, rápida y sólida. Está preparado para detección de intrusión en tiempo real (IDS), prevención de intrusiones en línea (IPS), monitoreo de seguridad de red (NSM) y procesamiento de ficheros pcap sin conexión.

Suricata inspecciona el tráfico de la red utilizando potentes y extensas reglas y lenguaje de firmas y se integra perfectamente con herramientas existentes como los SIEM, Logstash/Elasticsearch/Kibana y otras bases de datos.(Foundation)

### 2.1.1 Características

Suricata implementa un completo lenguaje de firmas para la correlación con amenazas conocidas, violación de políticas y comportamiento malicioso. Detecta muchas anomalías en el tráfico que inspecciona y utiliza el conjunto de reglas especializadas Emerging Threats y el conjunto de reglas VRT<sup>1</sup>.

**Alto rendimiento:** Una sola instancia de Suricata es capaz de inspeccionar el tráfico de varios gigabits. El motor está construido alrededor de una base de código multihilo, moderna y altamente escalable. Existe compatibilidad nativa para la aceleración de hardware de varios proveedores a través de PF\_RING y AF\_PACKET.

**Detección automática de protocolos:** Suricata detectará automáticamente protocolos como HTTP en cualquier puerto y aplicará la lógica adecuada de detección y registro, ayudando enormemente a la localización de malwares y dominios C&C<sup>2</sup>.

---

<sup>1</sup> Conjunto de reglas oficiales elaboradas y actualizadas por Vulnerability Research Team (Equipo de Investigación de Vulnerabilidades)

<sup>2</sup> Command & Control es una forma de referirse a los servidores con la función de dar instrucciones a determinado malware.

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**

**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**



**NSM (más que un IDS):** También puede inspeccionar solicitudes HTTP, registrar y almacenar certificados TLS, extraer archivos de flujos y almacenar-los en el disco. Soporta de capturas completas de pcap que permite un análisis sencillo. Todo esto hace que Suricata sea un poderoso motor para su ecosistema de Monitoreo de Seguridad de Red (NSM).

- Registro y análisis TLS / SSL: no solo puede coincidir con los aspectos de un intercambio SSL/TLS dentro del conjunto de reglas gracias al TLS Parser de Suricata, sino que, también puede registrar todos los intercambios de claves para su posterior análisis. Una excelente manera de asegurarse de que su red no sea víctima de una autoridad certificadora no confiable.
- Registro HTTP: ¿Por qué agregar más hardware a su red solo para registrar la actividad http cuando su IDS ya la ve? Suricata registrará to-das las conexiones HTTP en cualquier puerto para su posterior análisis. (Foundation)

La arquitectura de múltiples hilos de Suricata es única, ya que puede soportar sistemas multinúcleo y multiprocesador de alto rendimiento, ofreciendo mayor velocidad y eficiencia en el análisis de tráfico de red. Esto también ayuda a dividir la carga de trabajo de IDS/IPS en función de las necesidades de procesamiento. Además de la aceleración de hardware (con limitaciones de hardware y de tarjeta de red), el motor está diseñado para utilizar la mayor potencia de procesamiento ofrecida por los últimos chips de CPU multinúcleo. (Agra Monte, 2017)

## **2.2. ELK**

Al combinar las herramientas masivamente populares Elasticsearch, Logstash y Kibana (lo que se conoce como Elastic Stack o ELK), Elastic ha creado una plataforma extremo a extremo que ofrece información procesable en tiempo real de casi cualquier tipo de fuente de datos estructurados y no estructurados. Construido y respaldado por ingenieros detrás de cada uno de estos productos de código abierto, Elastic Stack hace que las

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**

**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**



búsquedas y el análisis de datos sea más fácil que nunca. Miles de organizaciones en todo el mundo usan estos productos para una variedad infinita de funciones críticas para determinadas empresas. (Shay Banon)

### **2.2.1 Elasticsearch**

Elasticsearch es un motor de búsqueda y análisis de texto completo altamente escalable y de código abierto. Permite almacenar, buscar y analizar grandes volúmenes de datos de forma rápida y casi en tiempo real. Lo que esto significa es que hay una ligera latencia (normalmente un segundo) desde el momento en que indexa un documento(dato) hasta el momento en que se convierte en un dato a buscar. (Shay Banon)

Elasticsearch (Roldán Mínguez, 2016), es una base de datos NoSQL orientada a documentos en formato JSON y basada en Apache Lucene. Es una herramienta ampliamente utilizada en motores de búsquedas de texto en documentos de datos, proporcionando funcionalidades con muy baja latencia, dado que los datos están indexados. Elasticsearch permite configurar un clúster con distintos nodos a través del cual se distribuirán los datos, para después realizar búsquedas sobre ellos. En todo clúster debe haber un nodo de datos y un nodo maestro. El primero, se encargará de almacenar los datos y ejecutar las consultas y el nodo maestro será el encargado de dirigir el clúster, ordenando la ejecución de consultas, recuperando índices corruptos, etc. Los datos se introducen en Elasticsearch en índices y las búsquedas se restringen a un único índice.

El almacenamiento de los datos en los nodos es gestionado directamente por el clúster, por medio de dos parámetros configurables por el usuario. El primero se denomina Shard y hace referencia al número de partes en que se dividirá un conjunto de datos para repartirlo por los nodos de datos del clúster. El segundo parámetro se denomina Factor de Replicación, con el que se especifica cuantas réplicas en otros nodos se hará de cada uno de los shards, para no perder datos en caso de fallo en alguno de los nodos de datos. Por ejemplo, en la siguiente figura se muestra el esquema de un clúster Elasticsearch con tres

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.

nodos de datos a través de los cuales se almacena un índice, el cual se ha subdividido en 3 shards. Cada uno de estos shards se ha distribuido por los 3 nodos, y, por cada shard principal se ha generado una réplica. Las réplicas de estos shards también se han distribuido, pero por nodos distintos al nodo con el shard principal.

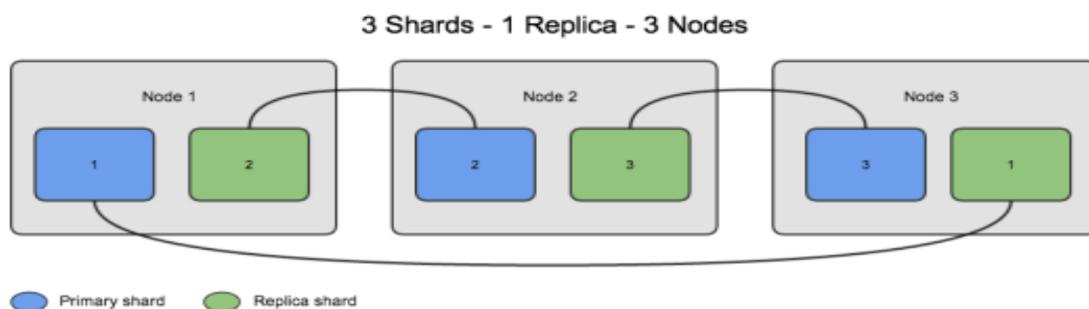


Figura 1 Almacenamiento de datos en shards y réplicas en Elasticsearch (Roldán Mínguez, 2016)

## 2.2.2 Logstash

Logstash es una aplicación java de código abierto con el objetivo de transportar, recolectar, filtrar e indexar logs. La arquitectura de Logstash está compuesta por tres componentes principales en forma de plugins: Entrada, Filtro y Salida.

Los plugins de Entrada habilitan el soporte de Logstash para diversas fuentes generadoras de logs. Los plugins de Filtro permiten el procesamiento, incluidos filtrado y normalización, de los logs recolectados en las fuentes. Por último, los de Salida, posibilitan el envío de los logs recolectados y procesados a su destino final. (Carrión Ramírez 2015)

Otra ventaja de Logstash respecto a sistemas basados en syslog es que ha sido creada por el mismo desarrollador que la base de datos. Esto asegura que no habrá incompatibilidad entre las diferentes piezas de la implementación. (Agra Monte, 2017)

# PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS II CONVENCION CIENTÍFICA INTERNACIONAL “II CCI UCLV 2019”

DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.

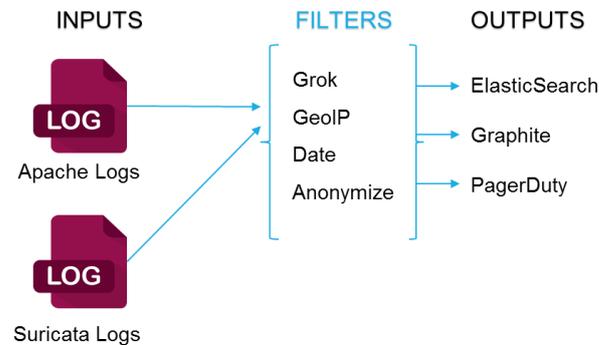


Figura 2 Arquitectura de Logstash.

### 2.2.3 Kibana

Kibana es una herramienta de visualización y exploración de datos. Entre las principales características que presenta se encuentran: integración completa con Elasticsearch, vistas personalizadas, análisis incorporado y soporte multorigen. (Carrión Ramírez 2015)

Kibana se puede usar para buscar, ver e interactuar con los datos almacenados en los índices Elasticsearch, de tal forma que se puede realizar fácil-mente análisis avanzados de datos y visualizar estos datos en gran variedad de gráficos, tablas y mapas, todo ello por medio de una interfaz web. (Roldán Mínguez, 2016)

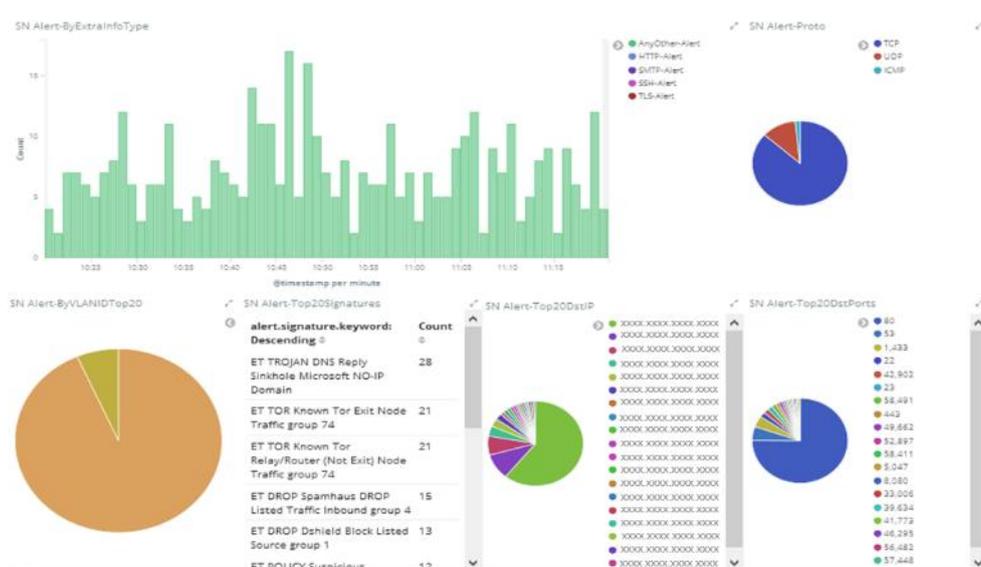


Figura 3 Visualización con Kibana. (elaboración propia)

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCIÓN CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**

**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**



### **2.3 Firewall**

Este dispositivo, que es la primera capa de seguridad, nos permite filtrar las conexiones entrantes a nuestra plataforma de modo que seamos capaces de definir políticas con respecto a qué tipo de protocolos pueden utilizarse para consultar nuestras aplicaciones publicadas.

Habitualmente en una plataforma dedicada a las publicaciones Web, estarán activadas las comunicaciones contra el puerto en el que esté publicado el servicio HTTP y, si además tenemos conexiones seguras, el puerto HTTPS.

De esta manera, somos capaces de restringir el acceso a nuestros equipos protegidos para que únicamente se redireccionen peticiones hacia nuestros equipos frontales cuando dichas comunicaciones sean, supuestamente, legítimas.

El firewall realmente nos define un filtro que únicamente dejará pasar las comunicaciones que cumplan ciertos criterios (por ejemplo, comunicaciones contra una dirección IP en concreto que vengan por los puertos permitidos), es decir define una pequeña ventana entre todos los servicios disponibles en Internet. (Huerta Molina, 2015)

Entre las funciones más habituales de los firewalls tenemos (Pérez González, 2016):

- Autorización o denegación de tráfico.
- Registro de las comunicaciones entre redes.
- Encaminamiento (“routing”) de paquetes entre redes.
- Segmentación y securización de las grandes redes.

Esta labor se realiza a través de un motor de inferencia basado en reglas. Estas reglas son configuradas por los administradores con el fin de autorizar o denegar comunicaciones.

### **2.4 Filtrado antispam**

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**

**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**



El filtrado antispam permite evitar que la empresa se vea inundada por infinidad de fastidiosos mensajes de correo electrónico no deseados, que consumen tiempo y muchas veces resultan peligrosos.

El filtrado antispam es un componente imprescindible en todo kit de herramientas de seguridad de red. Evita que los mensajes de correo electrónico no deseados inunden las bandejas de entrada de los empleados. Además, las soluciones antispam protegen contra los virus más recientes, los ataques de phishing y otras amenazas que llegan por correo electrónico.

En condiciones ideales, conviene adquirir un dispositivo antispam que:

- Detenga los mensajes de correo no deseados, los virus y otro tipo de software malicioso antes de que lleguen a los servidores de correo electrónico.
- Ofrezca una instalación sencilla, basada en un navegador web, para poder instalarlo con rapidez y facilidad, y comenzar a trabajar de inmediato.
- Brinde una defensa que se actualice de forma constante y automática, por lo que protege a la empresa contra amenazas emergentes de rápida propagación.
- Se adapte a las necesidades y al presupuesto de su empresa.(Cisco, 2016)

### **3. Resultados y discusión**

Como parte de las tareas de supervisión de la seguridad informática durante la realización de eventos y visitas de primer nivel en el país, el COS estableció un grupo para la respuesta a incidentes de seguridad, dedicado al monitoreo del tráfico malicioso en los puntos de agregación de los servicios. Como resultado del mismo, se ha logrado tener una visibilidad de las amenazas, incidentes y hechos de fraude asociados a estos servicios.

#### **3.1 Cleaning Center. Un nuevo servicio**

Los resultados y experiencia adquirida en el proceso de conceptualización e implementación para el control de tráfico malicioso en los PoP, ha arrojado la propuesta de ofrecer un nuevo servicio destinado a las empresas. Dicho servicio, denominado

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCIÓN CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**

**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**



Cleaning Center, tiene la funcionalidad de detectar y mitigar cualquier tipo de amenaza, programas maliciosos, entre otros, y dar respuesta ante este tráfico no deseado.

Cleaning Center proveerá a los clientes de un acceso a internet con una capa de seguridad adicional para protegerlos de un entorno de amenazas en constante evolución detrás del acceso. Con esta solución, todo el tráfico de internet del cliente, entrante y saliente se redirige a través de la red troncal MPLS a la plataforma Cleaning Center, donde se filtra y se bloquea cualquier malware y tráfico no deseado.



Figura 4 Proceso de Cleaning Center. (elaboración propia)

Cleaning Center se basa en el conjunto de herramientas anteriormente expuestas trabajando como un todo y perfectamente integradas, a fin de, ofrecer una mayor seguridad los usuarios que dispongan la contratación de dicho servicio. Entre sus principales características se encuentran las siguientes:

- Firewall (IPS/IDS): Mecanismos basados en firmas que monitorean la red, detectan y detienen actividades maliciosas permitiendo o denegando el flujo de entradas y salidas, basándose en protocolo, puerto y dirección IP.
- Filtrado web: Mecanismos de clasificación de URL junto con un potente motor de reglas que permite la creación de políticas de acceso de internet. Limita la exposición a contenidos maliciosos e implanta políticas de uso de Internet corporativas.

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCIÓN CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”



DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.

- Protección frente a amenazas: prevención de intrusiones y bloqueo de software malicioso. Incluye funcionalidad de prevención de fuga de información basada en tipos de archivo y patrones.
- Protección Antispam: se basa en filtros de spam en lista negras de direcciones IP y URL, también sumas de verificación de correos.
- Portal de servicio: integrado a la plataforma de seguridad, con acceso a cuadros de mando en tiempo real, informe y visualizaciones de políticas de seguridad.

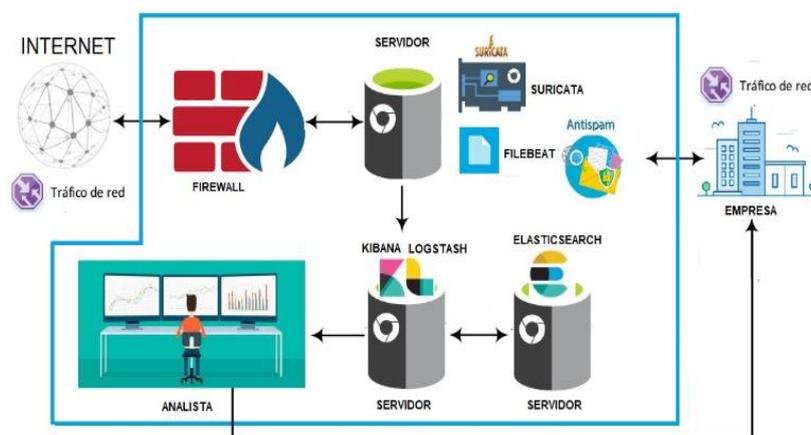


Figura 5 Estructura interna de Cleaning Center. (elaboración propia)

Cleaning Center es un servicio geográficamente redundante que elimina puntos únicos de falla y se ofrece únicamente desde la nube de seguridad de ETECSA. Con este modelo el cliente evita tener que adquirir y mantener soluciones de seguridad.

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCIÓN CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”

DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.

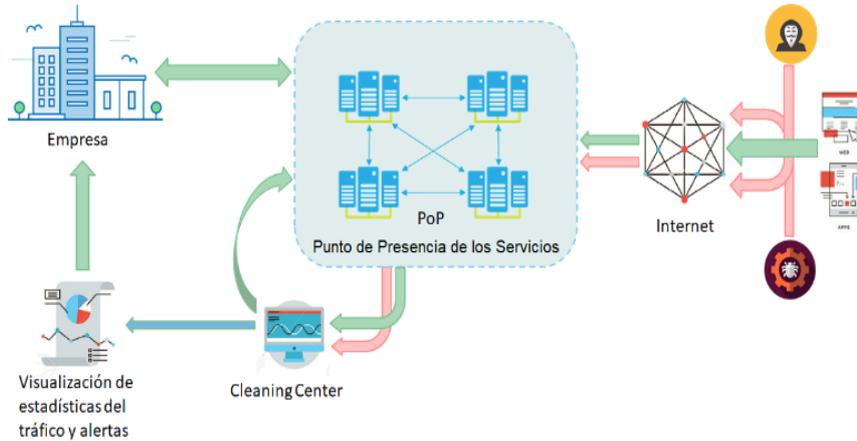


Figura 6 Funcionamiento del Cleaning Center. (elaboración propia)

Además de las funcionalidades de protección, nuestros clientes cuentan con un portal de servicios donde pueden visualizar la actividad del servicio a través de cuadros de mando y reportes en tiempo real. Además de tener acceso para ver sus políticas de seguridad asociadas con los diferentes módulos del servicio.

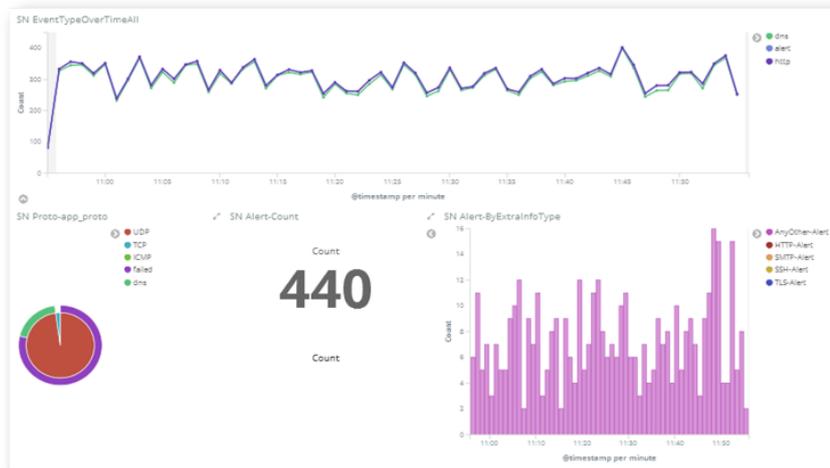


Figura 7 Cuadros de mandos Cleaning Center. (elaboración propia)

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCIÓN CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**



**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**

### 3.2 ¿Porque Cleaning Center?

Cleaning Center, gracias a su poderosos IDS, detecta la existencia de computadoras vinculadas a redes botnet y programas malignos (incluidos ransomware y otros principalmente asociados a sistemas operativos de dispositivos móviles).

Tabla 1 Ejemplos de programas malignos detectados. (elaboración propia)

<b>MUESTRA DE PROGRAMAS MALIGNOS DETECTADOS</b>	
Linux/XorDDoS	Win32/Sality
W32/Bayrob	Win32/Small
W32/Lethic	W32/Joiner.A
W32/Njw0rm	W32/Tempedreve
W32/Ramnit	Win32/Kido
W32/Rukap	Win32/Kido EJT
W32/Sality	Win32/Blaknight.A
Win/32 Dapato	Win32/Conficker
Win/32 Ramnit	Win32/Ursnif
Win32 / Floxif	Win32/Dreambot
Win32 / Glupteba	Win32/Qadars
Win32 / Injector.BRLE	Win32/Sohanad.AL
Win32 / InstallCore	TrojanDownloader W32/Carberp.A
Win32.Pushdo	Win32 / Recslurp.D
Backdoor.Win32.Rbot.adqd	Win32 / Xtrat.B
Backdoor.Win32.Rbot.bni	Win32/Blaknight.A
Botnet Lethic	Win32.Addrop
Win32/TrojanDownloader.Banload	Win32.Ammyy
Win32.Protux.B	Win32.Dapato

Como elemento común en las redes del país está la existencia de vulnerabilidades, la mayoría de estas conocidas desde hace varios años. Estas brechas de seguridad se encuentran en aplicaciones, sitios web, configuraciones de equipos entre otros elementos que interactúan en la red. El Cleaning Center permite identificar cuando una red está siendo objeto de escaneos en búsqueda de vulnerabilidades, previendo que sean explotadas posteriormente.

Los correos spam es otro de los comportamientos comunes en las redes empresariales cubanas ya sea como emisoras o receptoras del mismo, existiendo deficiencias en las configuraciones de los servidores de correo. El filtrado antispam realizado por Cleaning

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”



DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.

Center permite filtrar los mensajes entrantes ahorrando tiempo en no leer correos no deseados o spam y filtra toda la basura antes de que comience a consumir el ancho de banda ni utilizar el espacio en su servidor.

El siguiente gráfico muestra la cantidad de incidentes que han sido detectados y sus categorías estos datos sirven de ejemplo de lo que se podrá lograr con una implementación de Cleaning Center.

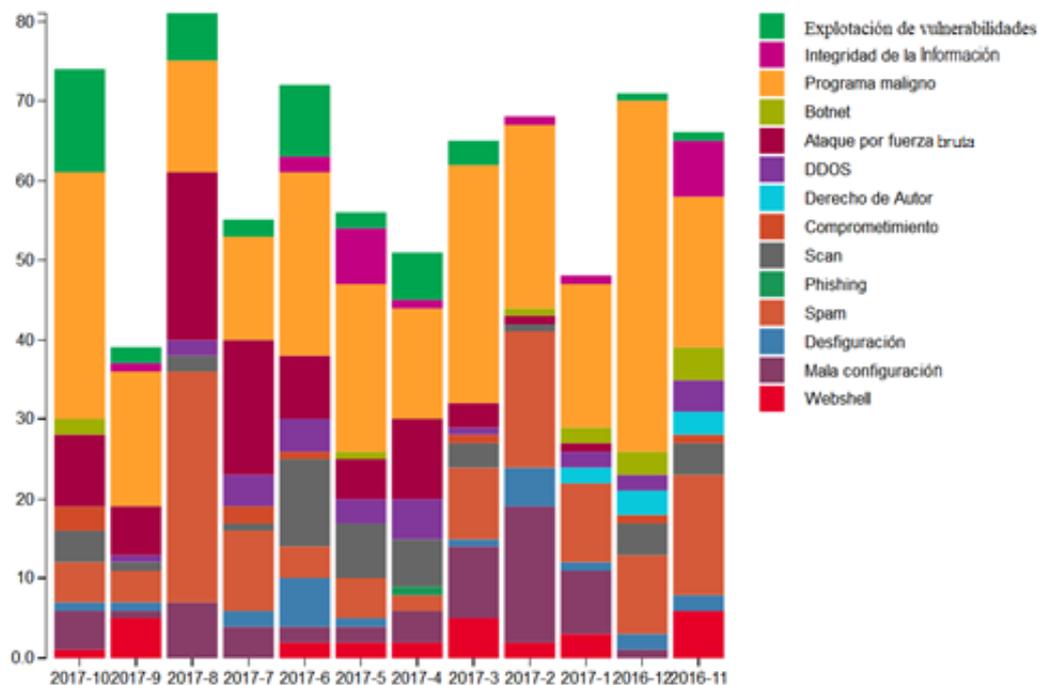


Figura 8 Ejemplo de incidentes detectados. (elaboración propia)

#### 4. Conclusiones

El panorama de amenazas se encuentra en constante cambio, los atacantes emplean diversas técnicas avanzadas para sortear las herramientas de seguridad. Las amenazas basadas en malware, tales como ransomware, siguen siendo sumamente populares entre los atacantes. Además, las amenazas que no contienen malware, como phishing de credenciales, correos spam y vulneración de correo electrónico de empresas, afectan cada vez a más entidades. El uso del servicio de Cleaning Center permitirá disminuir, e incluso

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**



**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**

erradicar este tipo de amenazas mediante el filtrado del tráfico malicioso gracias a Suricata y a su función de IPS en el bloqueo de dicho tráfico.

Cleaning Center está diseñado como parte del servicio de acceso a Internet, de forma que la protección frente amenazas sea una característica esencial del servicio de acceso.

Con la contratación de dicho servicio, Cleaning Center proveerá a los usuarios de los siguientes beneficios:

- Proporcionar un plan completamente transparente de “pago por uso” sin costo adicional. Permite una drástica reducción de costo, el cliente no necesita invertir en hardware o software por lo tanto puede evitar los costos de mantenimiento, renovación y desarrollos tecnológicos.
- Garantizar el desarrollo continuo de actualizaciones para proteger la empresa en cuestión de las últimas amenazas, con esto poder garantizar la mejor tecnología de seguridad en un entorno de constante evolución de las amenazas de internet.
- Proporcionar protección completa de acceso a internet.
- Garantizar la disponibilidad de servicio cercana al 100% gracias a la arquitectura de alta disponibilidad y geográficamente redundante.
- Brindar al cliente un portal con informes y cuadros de mando en tiempo real.
- Tiene facilidad en la implementación, la gestión y el mantenimiento.
- Los administradores de redes de las empresas podrán completar con rapidez y facilidad las tareas de gestión, para que se centren en labores más estratégicas.
- El soporte técnico por parte de los especialistas de ETECSA les proporcionará a las empresas que contraten el servicio la seguridad de saber que siempre recibirán ayuda especializada cuando la necesiten.
- Los administrativos podrán definir políticas de acceso a internet para su empresa, como sitios o contenidos no relacionados a su trabajo y que no desean que sean accedidos durante el horario laboral.

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCIÓN CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”



DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.

## 5. Referencias Bibliográficas

- Agra Monte, A. (2017). *Diseño e implementación de infraestructura NIDS (Network Intrusion Detection System) para PIMES*. (Trabajo Fin de Grado), Universidad Politécnica de Valencia. Retrieved from <https://riunet.upv.es/bitstream/handle/10251/88856/AGRA%20-%20Dise%C3%B1o%20e%20implementaci%C3%B3n%20de%20infraestructura%20NIDS%20%28Network%20%20Intrusion%20Detection%20System%29%20par....pdf?sequence=1&isAllowed=y>
- Banon, S. Elasticsearch Getting Started. Retrieved from <https://www.elastic.co/guide/en/elasticsearch/reference/current/getting-started.html#getting-started>
- Banon, S. An Introduction to the ELK Stack. Retrieved from <https://www.elastic.co/webinars/introduction-elk-stack>
- Capraru Pons, C. A. (2016). *Detección de anomalías HTTP trazando la sesión web de un usuario*. Universidad Obrera de Catalunya. Retrieved from <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/52890/4/ccapraruTFM0716mem%20ria.pdf>
- Carrión Ramírez, B. A. (2015). *Diseño e Implementación de una solución de gestión centralizada de logs de aplicaciones, sistemas y dispositivos basada en Logstash que permita la creación de cuadros de mando para explorar, analizar y monitorear eventos de seguridad*. Retrieved from <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/42250/3/bycaTFM0615memoria.pdf>
- Cisco. (2016). *Filtrado antispam: El fin del correo electrónico no deseado* Retrieved from [https://www.cisco.com/c/dam/global/es\\_mx/solutions/small-business/centro\\_recursos/pdf/antispam\\_filtering\\_the\\_end\\_of\\_junk\\_email\\_spa.pdf](https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/centro_recursos/pdf/antispam_filtering_the_end_of_junk_email_spa.pdf)
- Foundation, O. I. S. Características de Suricata. Retrieved from <https://suricata-ids.org/features/>
- Foundation, O. I. S. Suricata. Retrieved from <https://suricata-ids.org/>
- Huerta Molina, A. (2015). *Diseño, implementación y análisis de un sistema de detección y respuesta activa*. (Proyecto fin de carrera), Universidad Autónoma de Madrid. Retrieved from [https://repositorio.uam.es/bitstream/handle/10486/665070/Huerta\\_Molina\\_Alejandro\\_pfc.pdf?sequence=1#%5B%7B%22num%22%3A87%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C82%2C646%2C0%5D](https://repositorio.uam.es/bitstream/handle/10486/665070/Huerta_Molina_Alejandro_pfc.pdf?sequence=1#%5B%7B%22num%22%3A87%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C82%2C646%2C0%5D)
- Pérez González, R. C. (2016). *Los sistemas de seguridad perimetral y principales vectores de ataque web*. Universidad Obrera de Catalunya. Retrieved from <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/52986/6/rperezgonTFG0716mem%20ria.pdf#%5B%7B%22num%22%3A168%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C85.099998%2C596.299995%2C0%5D>

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)

**PLANTILLA OFICIAL PARA LA PRESENTACIÓN DE TRABAJOS  
II CONVENCION CIENTÍFICA INTERNACIONAL  
“II CCI UCLV 2019”**

**DEL 23 AL 30 DE JUNIO DEL 2019.  
CAYOS DE VILLA CLARA. CUBA.**



Roldán Mínguez, A. (2016). *Mecanismos de análisis BigData para la caracterización de la actividad docente en un Campus Virtual Moodle*. UNIVERSIDAD DE VALLADOLID. Retrieved from [http://uvadoc.uva.es/bitstream/10324/17475/1/TFM-G\\_547.pdf](http://uvadoc.uva.es/bitstream/10324/17475/1/TFM-G_547.pdf)

Información de contacto  
[convencionuclv@uclv.cu](mailto:convencionuclv@uclv.cu)  
[www.uclv.edu.cu](http://www.uclv.edu.cu)