**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

**FACULTAD DE INGENIERÍA**

# Actividades de monitoreo y análisis en un Security Operation Center

**INFORME DE ACTIVIDADES PROFESIONALES**

Que para obtener el título de

**Ingeniero en Computación**

**P R E S E N T A**

Rogelio Salazar Contreras

**ASESOR DE INFORME**

Ing. Rafael Sandoval Vázquez

**Ciudad Universitaria, Cd. Mx., 2018**

# Contenido

# Introducción

El uso de tecnologías como el Internet y las conexiones remotas es cada vez más común dentro de las grandes organizaciones, las cuales se apoyan de este tipo de alternativas para facilitar sus comunicaciones y contar con una mayor cobertura sin que sus actividades se vean interrumpidas. Por otro lado, esto abre la posibilidad a personas malintencionadas de intervenir dichas conexiones e introducirse en la infraestructura de red para beneficiarse de una u otra forma una vez conseguido el acceso.

A raíz de esta problemática, surgen empresas proveedoras de servicios de seguridad informática, las cuales toman la responsabilidad de asegurar la red, permitiendo a sus clientes enfocarse en asuntos propios de su negocio. Estas empresas proveedoras de servicios de seguridad generalmente ofrecen los servicios de monitoreo y administración de tecnologías de seguridad, los cuales son fundamentales para la contención y mitigación de incidentes.

Las actividades correspondientes a dichos servicios se llevan a cabo en instalaciones especializadas conocidas como *Security Operation Center* (SOC).

El presente trabajo tiene como objetivo principal describir la importancia de un SOC, así como algunas de las actividades que en él se realizan por parte del personal de monitoreo, usando para ello una serie de ejemplos ilustrativos que ayuden a la comprensión de dichas actividades. Así mismo se describirán los procesos de monitoreo de eventos, análisis de actividad sospechosa y escalación.

Por motivos de confidencialidad de la empresa donde laboro actualmente (a la cual haré referencia con el nombre de “Soluciones en Seguridad S.A.”) la información de direcciones IP, segmentos de red, marcas y nombres de herramientas de software serán ficticios, empleando para ello nombres genéricos como IPS1, IPS2, WAF1, SIEM1 en los casos que sea necesario.

# Capítulo 1: Descripción general de Soluciones en seguridad S.A.

En este capítulo se proporciona una reseña sobre la empresa donde laboro, abordando su filosofía y describiendo cada una de las áreas que la conforman así como los servicios que ésta ofrece a sus clientes.

## 1.1 ¿Qué es Soluciones en seguridad S.A.?

Soluciones en seguridad S.A. es una empresa especializada en el diagnóstico y solución de problemas de seguridad informática. Nace como respuesta a una necesidad de las grandes empresas por garantizar la seguridad de su información y retomar la gestión de sus riesgos. Esta necesidad ha crecido en los últimos años debido al desarrollo de ataques y robos de información a empresas e instituciones, de los cuales se escucha cada vez más frecuentemente.

Dichas necesidades se conjuntaron con la pasión de varios expertos en tecnología, dando como resultado su creación hacia finales del 2003.

En este periodo, la empresa ha logrado reunir a diversos especialistas en el área, al tiempo que ha trabajado para clientes del sector financiero, comercial e industrial

tanto nacional como internacionalmente (Soluciones en seguridad S.A., Acerca de nosotros, 2017).

## 1.2 Misión

Ser el socio más confiable para sus clientes en Sistemas de Tecnologías de Información, al brindar innovadoras, ágiles, consistentes y personalizadas soluciones de infraestructuras y servicios de tecnologías de información de misión crítica, manteniendo siempre nuestra flexibilidad operativa (Soluciones en seguridad S.A., Acerca de nosotros, 2017).

## 1.3 Visión

Posicionarse como líderes expertos en el mercado internacional de Tecnologías de Información con Infraestructuras y servicios de TI de misión crítica, en todas las regiones atendidas (Soluciones en seguridad S.A., Acerca de nosotros, 2017).

## 1.4 Valores

- Responsabilidad social.
- Solidaridad y compromiso con México.
- Transparencia y eficiencia en la aplicación de recursos.

## 1.5 Servicios que brinda

Los servicios proporcionados por Soluciones en Seguridad S.A. hacia sus clientes se basan en el diagnóstico, la gestión de riesgos y la respuesta a incidentes. Mediante estos tres rubros le es posible identificar las brechas de seguridad existentes, así como diseñar una estrategia de seguridad que permita corregirlas. Una vez definida la estrategia, se toman las medidas necesarias para que dicho plan mantenga un nivel aceptable en la protección de la información. Dentro de la estrategia de seguridad se pueden contemplar acciones como la creación de políticas de seguridad, implementación y administración de tecnologías de seguridad, soporte y escalación con fabricantes, etc.

Derivado de los puntos mencionados previamente, se prestan los siguientes servicios por parte de la empresa:

### Diagnóstico y Cumplimiento de la Información

En esta categoría se prestan los servicios orientados a identificar los riesgos que enfrenta cada cliente y definir las acciones de prevención de los mismos.

El proceso comienza con la visita de un grupo de consultores, los cuales aportan ideas, diagnostican problemas y buscan soluciones para los mismos. También se encargan de diseñar una solución a la medida para cada cliente.

Posteriormente se llevan a cabo escaneos con herramientas especializadas y la simulación de ataques informáticos llamados pruebas de penetración en las cuales se logra identificar las vulnerabilidades en la infraestructura del cliente. (Soluciones en seguridad S.A., Capacitación-Servicios, s/f).

### Protección Perimetral

Se incluyen aquellos servicios que protegen los sistemas informáticos de los clientes desde internet. Dentro de esta categoría se encuentran la administración de herramientas como firewall, *Intrusion Prevention System* (IPS), *Web Aplication Firewall* (WAF) y antispam. (Soluciones en seguridad S.A., Capacitación-Servicios, s/f).

### Protección a Servicios de TI

Hace referencia a los servicios que protegen la infraestructura de TI que soporta los procesos/servicios más críticos del cliente. En esta categoría se incluye la administración de *Database Activity Monitoring* (DAM) y *Database Firewall* (DBF), así como herramientas de correlación de eventos *Security Information and Event Management* (SIEM). (Soluciones en seguridad S.A., Capacitación-Servicios, s/f).

### Protección a Usuarios

Categoría enfocada a la detección y prevención de posibles fugas de información, imputables a los usuarios finales.

Entre los servicios que contempla esta categoría podemos encontrar:

- **Protección contra amenazas**: Consiste en proteger a los usuarios finales contra malware mediante la administración de software antivirus de manera remota.
- **Filtrado de contenido web:** Las herramientas de tipo *web filter* proporcionan un control para buscar que los clientes naveguen de forma segura en internet.

- **Protección de dispositivos móviles:** Existe software capaz de monitorear la actividad realizada en dispositivos móviles, además de poder rastrearlos vía satélite en caso de robo. Esta tecnología es conocida como *Movil Device Management* (MDM).
- **Prevención de fuga de información:** Los *Data Loss Prevention* (DLP) son herramientas que monitorean las actividades que realiza el personal en una organización. Los eventos que puede identificar un DLP van desde la quema de CD, almacenamiento en dispositivos extraíbles y correo electrónico hasta impresión de documentos (Soluciones en seguridad S.A., Capacitación-Servicios, s/f).

### Tecnología de Seguridad

Se incluyen los servicios de venta e implementación de tecnología de seguridad proporcionando las tecnologías que requiere el cliente. Posteriormente se realiza la instalación y configuración inicial de los equipos. (Soluciones en seguridad S.A., Capacitación-Servicios, s/f).

## 1.6 Organigrama general

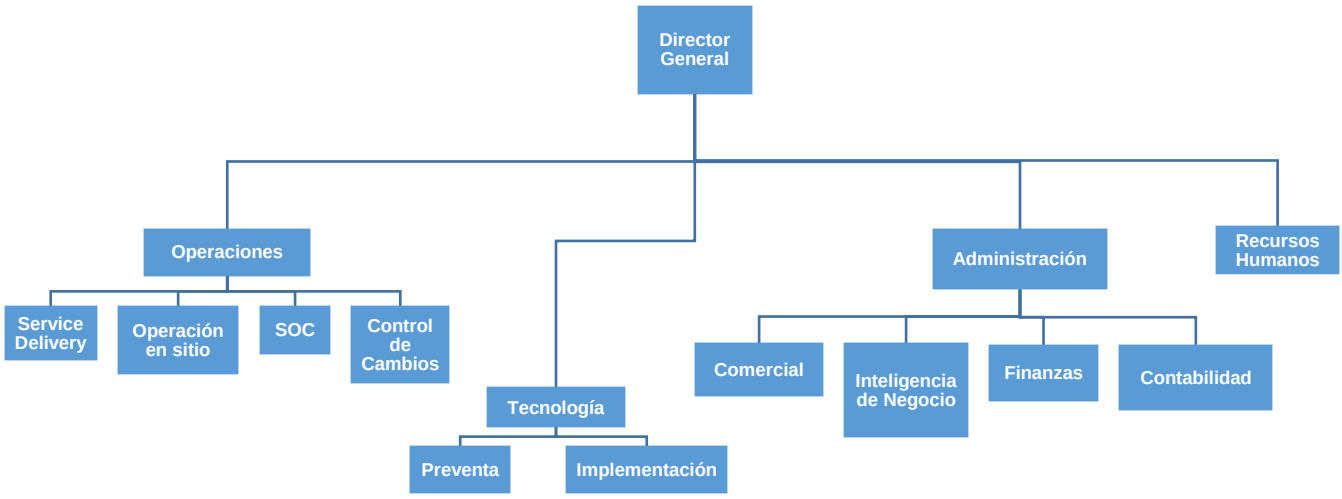



*Diagrama 1.1. Organigrama general de Soluciones en seguridad S.A. Adaptado de (SuccessFactors, 2017)*

### 1.6.1 Recursos humanos

Es el área que se encarga de llevar a cabo la gestión y dirección del personal de la empresa y entre sus funciones principales se encuentran el reclutamiento de nuevos candidatos, llevar todo lo relacionado con los sueldos y pagos de los colaboradores, así como proporcionarles diversos tipos de cursos y capacitación para un mejor desempeño en sus respectivas funciones.

### 1.6.2 Administración

Se refiere al área que contempla todos aquellos asuntos relacionados con la gestión de la empresa en general y que a su vez conllevan el desarrollo y crecimiento de la misma. En el área de administración se revisan aspectos publicitarios, financieros y de inteligencia de negocio, dentro de los cuales se encuentran la administración de los servicios proporcionados y verificar el cumplimiento de los *Service Level Agreement* (SLA) con cada uno de los clientes.

### 1.6.3 Tecnología

En esta área se conjuntan las actividades referentes a las tecnologías empleadas por parte de la empresa para poder prestar sus servicios. En este punto se contemplan el trato con proveedores y licitaciones, así como el dimensionamiento y cotización de tecnologías de seguridad por parte del equipo de preventa. Una vez adquiridas estas tecnologías, toca el turno al equipo de implementación llevar a cabo un plan de trabajo para integrar la tecnología adquirida por el cliente a su infraestructura, al mismo tiempo que da un seguimiento hasta que esta quede liberada por completo.

### 1.6.4 Operaciones

Contempla todas las áreas que se encargan de la parte operativa de los servicios brindados, es decir los servicios ya en un ambiente de producción. En el área de operaciones se encuentra el personal encargado de entregar los servicios liberados al cliente y mantener una comunicación con él para que pueda mantener a la empresa al tanto de cualquier inquietud que el cliente pueda presentar respecto a sus servicios.

Finalmente en esta categoría también se encuentran el personal de control de cambios que es el responsable de la administración de cambios en la infraestructura del cliente así como el personal de SOC al que pertenezco, el cual proporciona monitoreo 24/7 y atención a incidentes.

# Capítulo 2: Centro de Operaciones de Seguridad

En este capítulo se brinda una explicación sobre qué es un SOC, así como sus objetivos y los procesos de operación empleados por el personal de monitoreo dentro del mismo. De igual manera se abordan los conceptos de bitácoras, falsos positivos e incidentes de seguridad debido a su importancia dentro de los procesos mencionados.

## 2.1 ¿Qué es un SOC?

Existen diferentes tipos de centros de operación, los cuales involucran personal con diferentes clases de conocimientos y habilidades que interactúan entre sí para lograr los objetivos correspondientes al centro de operación en cuestión. Por ejemplo, un *Network Operation Center* (NOC) es un centro de operaciones enfocado en las comunicaciones y también es el encargado de mantener la red funcionando, es decir, que el acceso a internet y la conectividad entre equipos sea adecuada. Podemos mencionar también otros tipos de centros de operación como los *Threat Operation Center* (TOC) y los *Emergency Operation Center* (EOC) los cuales

cuentan con personal calificado para la investigación de nuevas amenazas y vulnerabilidades, y para responder de manera rápida y efectiva frente a una crisis respectivamente (Nathans, 2015, pág. 1).

Un *Security Operation Center* (SOC) es justamente otro de los centros de operación existentes y por obvias razones se enfoca en eventos relacionados con cuestiones de seguridad informática, usando para ello distintos mecanismos y/o herramientas de seguridad manipuladas por especialistas en el área. De igual manera es necesario establecer un conjunto de procesos, políticas y buenas prácticas que deben respetarse al pie de la letra para de este modo garantizar resultados óptimos y con un nivel aceptable de efectividad.

Cabe mencionar que la ubicación del SOC puede estar tanto dentro de la institución que asume el papel de cliente (SOC Interno) como fuera de ésta, en instalaciones especializadas y equipadas con infraestructura de alto nivel, con el fin de monitorear, identificar y dar solución a incidentes de seguridad remotamente, que pudieran causar afectaciones al cliente.

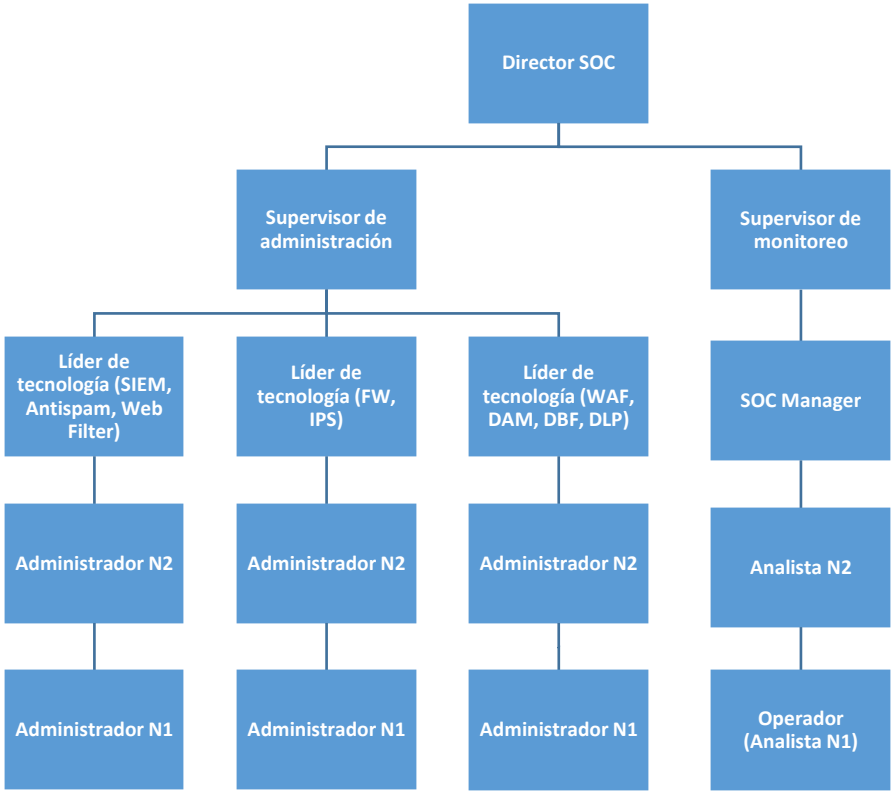



*Diagrama 2.1. Organigrama del SOC de Soluciones en Seguridad S.A. Adaptado de (SuccessFactors, 2017)*

## 2.2 Propósitos y objetivos de un SOC

Cada tipo de centro de operación tiene objetivos muy concretos dependiendo el enfoque al que estos estén referidos, en este caso, podemos decir que el objetivo principal de un Centro de Operación de Seguridad (SOC) es como su nombre lo indica, brindar “seguridad”, pero ¿a qué nos referimos exactamente cuando hablamos de seguridad en el campo de las TI?

La respuesta a esta pregunta la podemos establecer de la siguiente manera: preservar los tres principios básicos de la seguridad informática, los cuales son integridad, confidencialidad y disponibilidad, aplicados sobre la información y/o los servicios del cliente.

Dicho lo anterior, debemos establecer también las tareas necesarias para lograr estos objetivos, y estas incluyen un correcto monitoreo de eventos, análisis de la información y el tráfico detectado, toma de decisiones, proponer soluciones y dar recomendaciones de prevención o contención según sea el caso. Es importante mencionar que entre las metas del SOC se encuentra la atención a incidentes en un corto lapso de tiempo y esta actividad es posible en gran parte gracias al servicio de monitoreo en tiempo real proporcionado por el área de operación y monitoreo del SOC de la cual yo formo parte y en la que se analiza la actividad recibida o detectada por las herramientas de software, para determinar si ésta es sospechosa o no.

Parte importante del éxito del SOC para lograr sus objetivos se encuentra en la cohesión de su equipo de trabajo en sus diferentes niveles, es decir, todo el personal debe estar en la misma sintonía y mantener una comunicación efectiva y eficiente, así mismo debe existir una relación a nivel profesional entre los equipos tanto de monitoreo y detección, como los de contención y mitigación de incidentes.

## 2.3 Procesos de operación de un SOC

Como se mencionó anteriormente, una parte fundamental para que los resultados obtenidos por el SOC sean los deseados está constituida por los procesos que éste adopte para llevar a cabo las tareas pertinentes tanto a la recepción de la información como a la manipulación de la misma. Es decir, se debe respetar en medida de lo posible cada proceso tal cual se encuentre en la documentación proporcionada. De este modo, siguiendo cada etapa de los procesos planteados por el SOC prácticamente se están garantizando resultados que si bien no serán exactamente los mismos cada vez (pueden variar ligeramente debido a que las circunstancias no siempre son las mismas), si serán muy parecidos entre sí ya que provienen de una metodología comprobada previamente, dicha metodología es el desarrollo del proceso en sí. Si se siguen los pasos establecidos por los procesos

cada vez que se realicen labores de monitoreo y análisis de la información, se obtendrán resultados más precisos y sobre todo satisfactorios.

Es importante señalar también que en ciertas ocasiones la salida o resultado de un proceso se puede convertir en la entrada de otro, por lo que es de suma importancia realizar las diferentes actividades correspondientes a cada proceso de una manera clara y cuidadosa, de este modo no se arrastraran errores que puedan perjudicar el resultado final, lo cual representaría pérdida de tiempo y esfuerzo.

A continuación se describen algunos de los procesos utilizados dentro del SOC. Naturalmente existen varios procesos dedicados a cada una de las diferentes actividades y roles, sin embrago, me enfocaré a los correspondientes al área de operación y monitoreo, que es en la que yo participo.

### 2.3.1 Proceso de monitoreo de eventos

El proceso de monitoreo de eventos es el que se toma como referencia debido a que es la actividad principal por parte del área de operación y monitoreo, y de la cual partirá el análisis de la actividad sospechosa, posteriormente se procederá a clasificarla y determinar el nivel de escalación si es necesario, sin embargo cada etapa se desarrollará en los capítulos posteriores en su respectivo proceso.

El monitoreo a grandes rasgos consiste en recolectar, observar y utilizar información con el objetivo de dar un seguimiento a un hecho particular (en nuestro caso un incidente de seguridad) hasta que éste quede solucionado. Cabe señalar que los incidentes monitoreados no solo se enfocan a un nivel lógico, es decir, no sólo se refieren a amenazas potenciales, ataques informáticos o vulnerabilidades en los sistemas, sino que también se realiza un monitoreo a nivel físico como el estado y disponibilidad de los equipos físicos (también llamados *appliances*) correspondientes a cada herramienta, comprobando el correcto funcionamiento de las mismas.

La importancia de este proceso radica en observar los eventos detectados por las herramientas en tiempo real y así poder dar un diagnóstico y recomendaciones apropiadas para cada caso. Existen factores que pueden hacer que el tiempo de respuesta al incidente varíe, como pueden ser la severidad de los eventos (dependiendo la criticidad del evento se determina la prioridad del mismo), el tiempo de análisis del evento, la observación de comportamiento, etc. Sin embargo la esencia del proceso es la de atender y/o mitigar el incidente en el tiempo más corto posible.

A continuación se presenta el proceso de monitoreo de eventos de un SOC, en el cual se describen cada una de las actividades que lo componen. Podemos describir el proceso en la siguiente secuencia de pasos a seguir:

1. El operador revisa las notificaciones en los correos electrónicos configurados por las diferentes herramientas o hace una revisión parcial de cada herramienta como parte de las actividades programadas en el turno en curso ya sea análisis de firmas, listas de chequeo (*checklist*) de herramientas, registro de rendimiento, etc.
2. Se extrae la información arrojada por la herramienta (a esta información obtenida le llamamos *logs* o bitácoras) para su posterior análisis, de este modo se puede hacer un rastreo de lo que sucedió en el periodo de tiempo reportado, comparar con eventos anteriores y así determinar cuál es el comportamiento de dicha actividad detectada. En este punto también se verifica si existe algún problema con la herramienta, por ejemplo que no arroje eventos en tiempo real, no se tenga acceso a la misma, se encuentre en niveles óptimos de almacenamiento, etc. Si se presenta alguna problemática, se procede a canalizarla con el equipo de atención a fallas.
3. Una vez extraídas las bitácoras correspondientes, el proceso continúa con la consulta de una base de conocimiento, la cual puede estar constituida por diferentes tipos de documentación como pueden ser las listas negras (*blacklist*) y listas blancas (*whitelist*) definidas por el mismo personal del SOC o por el cliente, los correos de alerta enviados con anterioridad por parte de los operadores, o incluso es posible consultar el registro de tickets relacionados a cierto incidente o problemática. De este modo se corroborara si existen precedentes de cierto comportamiento (¿el evento ya ha sido alertado?, ¿el evento es recurrente?, ¿el incidente fue resuelto?), lo cual nos permitirá pasar al siguiente paso, la clasificación de severidad.
4. El operador procede a clasificar la severidad del evento basándose en la información recopilada en la consulta de bases de conocimiento así como en la matriz de severidad proporcionada por el área de administración de cada herramienta y determina si el evento debe alertarse o no con base en los siguientes criterios:

    - Si la severidad se determina baja se descarta como actividad sospechosa y se continua con el monitoreo, sin embargo esto no implica que no se le dé el apropiado seguimiento a la actividad determinado que pudo haberla generado.
    - Si la severidad se determina media o alta es considerada como actividad sospechosa y en ambos casos se pasa al proceso de análisis de actividad sospechosa el cual desarrollaré en el siguiente capítulo.

5. Por último, dependiendo los resultados obtenidos en el punto anterior se determina si la actividad es considerada como legítima o realmente representa un incidente de seguridad. Si se determina que la actividad

representa un incidente se procede a realizar la escalación correspondiente con el fin de mitigar dicho problema, por lo que la labor a nivel de operación es canalizar la problemática con el equipo de administración adecuado para cada herramienta. (Soluciones en seguridad S.A., Descripción del modelo de operación del Security Operation Center, s/f).

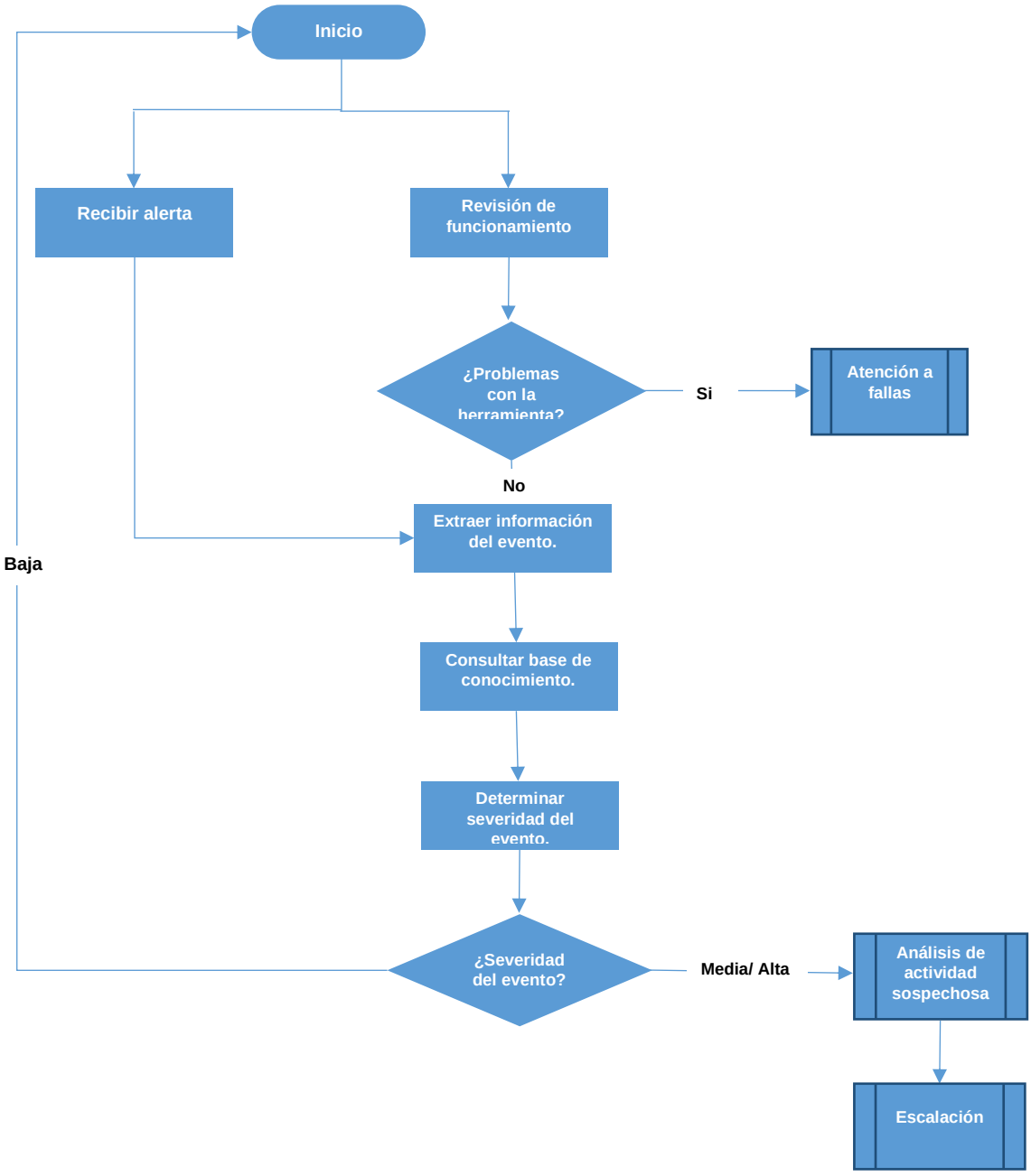



*Diagrama 2.2. Proceso de monitoreo de eventos. Adaptado de (Soluciones en seguridad S.A., Descripción del modelo de operación del Security Operation Center, s/f)*

Así concluye este primer proceso cuyo principal objetivo es, como pudimos observar, el identificar y determinar la severidad de la actividad y el tráfico que fluye por la red mediante las distintas herramientas y actividades programadas.

### 2.3.2 Proceso de análisis

El proceso de análisis servirá como un punto en el que se ligan tanto el proceso de monitoreo como el de escalación, mediante el análisis e investigación de la información recolectada con las diferentes herramientas empleadas en el proceso de monitoreo y posteriormente determinando a través de dicho análisis si es pertinente escalar o no la actividad detectada. Es importante procesar la información de tal modo que al final se conserven sólo los datos que indiquen si la actividad detectada realmente pudiera representar un incidente de seguridad, para esto es importante depurar la información obtenida en la extracción de bitácoras que proveen las herramientas, descartando aquellos eventos que pudieran representar un falso positivo.

Para continuar con el desarrollo de este capítulo es importante tener en cuenta los conceptos descritos a continuación para saber de qué estamos hablando durante el proceso de análisis.

**Bitácoras**

Las bitácoras (*logs*) son el tipo más básico de información que un sistema puede generar y en ellos se almacenan los detalles respecto a cualquier cosa que ocurra en dicho sistema. Mediante las bitácoras se obtienen indicadores con los que se puede saber si algo anda mal con la actividad del sistema y pudiera representar un problema.

El registro de estas bitácoras lo realizan las herramientas de seguridad, mediante un proceso de monitoreo y un censo de la información que pasa a través de la red. Es gracias al almacenamiento de bitácoras que es posible, de ser necesario, realizar una correlación de eventos en las diferentes herramientas y hacer un diagnóstico o hipótesis respecto a lo que pudiera estar sucediendo con un caso particular.

Es de suma importancia que las bitácoras extraídas se presenten de manera ordenada y que presenten ciertos datos relevantes que proporcionan valor al proceso de análisis, un claro ejemplo de estos datos que siempre deben acompañar a un *log* es la fecha y la hora en que se registró. Afortunadamente para nosotros las herramientas se encargan de almacenar las bitácoras, así como dar una clasificación predeterminada con cierta información por cada registro obtenido, sin

embargo, es posible configurar la herramienta para que nos arroje exactamente la información que consideramos necesaria para realizar el análisis.

Entre estos elementos se encuentran los siguientes:

- Fecha
- Hora
- Direcciones IP de origen y de destino
- Descripción del evento
- Severidad del evento
- Protocolo utilizado
- Puertos de origen y destino
- Usuario

Todos los elementos de la lista anterior ayudan a identificar si la actividad pudiera representar un riesgo para el cliente, sin embargo, existen más datos que se pueden proporcionar dependiendo la herramienta y siempre con miras a la posibilidad de responder a las siguientes preguntas: ¿Quién? ¿Dónde? ¿Cuándo? Y ¿Por qué? (Nathans, 2015, págs. 13-16)

En el caso del SOC se cuenta tanto con bitácoras del sistema en sí (las bitácoras propias de la herramienta como intentos de acceso a la misma, si hubo alguna interrupción en el servicio, qué usuarios han accedido y en qué momento, etc.) como las que la herramienta recolecta acerca de los activos de los clientes y son estas últimas los que realmente tienen más peso para los operadores ya que la información recolectada sobre los activos del cliente es la que servirá para realizar investigación y análisis. Por otro lado, las bitácoras de los *appliances* le son más provechosas al área de administración de cada herramienta debido a que ellos se encargan de resolver problemáticas relacionadas con configuraciones e interrupciones de los servicios.

### Falsos Positivos

Este es un concepto muy recurrente dentro de un SOC y se debe en gran parte a la configuración con la que cuenta cada una de las herramientas que se monitorean, entre mejor y más refinada sea la configuración de alertas en una herramienta, menor será la cantidad de falsos positivos generados. Sin embargo un falso positivo no es identificable a simple vista, es decir, es necesario llevar a cabo un análisis e investigación del evento o eventos relacionados con este comportamiento, de modo que después de realizar las pruebas y búsquedas pertinentes se llegue a determinar que el comportamiento analizado represente tráfico válido (este proceso también puede ser complementado y validado por el cliente, quien en muchas ocasiones determina, con base al informe entregado por el SOC si la actividad representa un falso positivo para él o un incidente de seguridad).

Pero ¿a qué nos referimos exactamente cuando hablamos de un falso positivo?

Un falso positivo es una alerta que por alguna razón es disparada por cualquiera de las herramientas sin que dicha alerta signifique realmente un riesgo o problema y, por lo contrario, representa tráfico permitido y legítimo. En pocas palabras, un falso positivo es una falsa alarma (Nathans, 2015, pág. 18).

La mayoría de las herramientas de monitoreo están regidas por reglas, las cuales están configuradas esperando al cumplimiento de alguna condición para ser disparadas y notificadas vía correo electrónico. Estas condiciones pueden ser entre otras: la detección de cierto patrón de comportamiento (uso de algún puerto en específico, tipo de tráfico, intentos de conexión, etc.), que se exceda un umbral establecido de memoria o CPU, acceso de cierto usuario en horarios no permitidos, etc.

Para que quede más claro el concepto, se dan como ejemplos ciertas situaciones comunes que pueden llegar a generar un falso positivo y estas son: el uso de un ping, el cual puede disparar una firma en un *Intrusion Prevention System* (IPS) notificando el intento de la comunicación entre equipos. Un ping podría ser usado por un atacante para comprobar que tiene comunicación con la red, del mismo modo que alguna herramienta de monitoreo de disponibilidad de equipos dentro de la misma red puede estar enviando pings constantemente para identificar cuando algún elemento dentro de la red se encuentre “caído”. Como podemos ver ambas situaciones podrían disparar la misma firma y sin embargo una realmente podría catalogarse como un riesgo, mientras que la otra es una actividad completamente permitida y controlada. Otra de estas situaciones es el exceso en el uso de CPU y memoria de un dispositivo, los cuales podrían ser generados por una inestabilidad o intermitencia por parte de la herramienta en cierto instante de tiempo, sin que ésta signifique el intento de hacer caer algún servicio, de hecho es posible que el umbral permitido se sobrepase por realizar alguna actividad de respaldos o algún procesamiento de información realizado por personal autorizado, el problema vendría si este exceso se prolonga por varios minutos y no se tiene conocimiento de alguna actividad a realizar por el equipo de administración del dispositivo en cuestión.

Por los aspectos mencionados previamente es de suma importancia que el equipo de administración tenga especial cuidado en la configuración de reglas, así como también en las alertas a notificar.

## Incidentes de seguridad

El *National Institute of Standards and Technology* (NIST) define un incidente como una violación o una amenaza inminente de la violación de las políticas de seguridad de un sistema de cómputo, así como también de las prácticas de seguridad estándar (Grance, Karen, & Kim, 2004).

Para el SOC, un incidente de seguridad es un evento o una serie de eventos que generan una afectación a los principios de seguridad informática (integridad, disponibilidad y confidencialidad) del sistema o la información que se está protegiendo.

Un incidente puede presentarse de varias formas, puede ser un virus que no fue detectado por el software antivirus, 300 intentos de acceso por parte de una cuenta de usuario de un empleado que ya no labora en la institución también se consideraría un incidente, un ataque de denegación de servicio (DoS), la identificación de una nueva vulnerabilidad en el sistema que estamos protegiendo, la pérdida de datos e incluso el robo de algún *appliance*. En términos generales, todo aquello que interrumpa o ponga en riesgo la producción de nuestro cliente en cuanto a sistemas computacionales puede ser considerado como un incidente.

Con el fin de tener un control de los incidentes que pudieran generarse dentro del SOC y tener un marco de referencia para prevenir y mitigar incidentes futuros, es necesario contar con un registro de los mismos, el cual puede documentarse de distintas maneras, sin embargo lo ideal es contar con un sistema de tickets en el que se registre por cliente el problema que se tuvo, el proceso de cómo fue solucionado y el tiempo que tomó solucionarlo, de este modo tendremos métricas que nos permitirán mejorar nuestros tiempos de respuesta y la calidad de atención.

Los SOC existen justamente para prevenir y mitigar incidentes de seguridad y su principal objetivo siempre será que haya la menor cantidad de incidentes posibles, así como atenderlos y corregirlos en el menor tiempo posible también.

Finalmente, una vez detallados los conceptos anteriores es posible afirmar que el proceso de análisis es fundamental en la detección de incidentes de seguridad y que en él se realiza toda la investigación para determinar si un evento es debe ser alertado o representa simplemente un falso positivo, en caso de que el evento detectado se catalogue como alerta, es necesario elaborar un informe en el cual se recopile la información referente al incidente y toda la evidencia que sustente nuestras conclusiones y finalmente agregar todas las recomendaciones necesarias de contención o mitigación según sea el caso.

El proceso de análisis se puede resumir de la siguiente manera:

1. Realizar la investigación pertinente de los parámetros alertados por la herramienta, ya sea una firma, intento de ataque, o patrón de comportamiento que haya sido detectado y notificado por la herramienta en cuestión.
2. Identificar un patrón de comportamiento en los eventos, y realizar la investigación pertinente. De este se realiza una comparativa si es que el patrón encontrado coincide con algún otro patrón conocido e identificado oficialmente como un ataque legítimo.
3. Una vez terminada la investigación se procede a determinar una serie de recomendaciones para el cliente enfocadas al evento detectado, estas pueden ir desde la revisión de activos con versiones vulnerables de software, realizar actualización y aplicación de parches de seguridad en el software si es que el cliente efectivamente cuenta con versiones vulnerables, hasta solicitar un bloqueo de dirección IP o de cierto tipo de tráfico en particular (dependiendo la herramienta es el tipo de bloqueo a realizar).
4. Solicitar al equipo de administración de la herramienta la validación de las recomendaciones para que éstas sean más precisas y también para determinar si son factibles o no.
5. El administrador valida las recomendaciones revisando la naturaleza de la actividad reportada, así como apoyándose en el conocimiento con el que cuenta (tanto a nivel técnico como la información con la que cuente sobre el cliente en cuestión) para complementar el informe, cuando se tiene su visto bueno se continúa con el siguiente paso.
6. Una vez avaladas las recomendaciones, se prepara el informe para envío al cliente ya sea en calidad de informativo o alertamiento dependiendo la severidad de la actividad a reportar. Es de suma importancia en este punto que a la documentación entregada se le anexen las evidencias correspondientes para así poder fundamentar el informe y en base a eso el cliente dé la última palabra.
7. Finalmente, una vez enviado el informe, se espera la retroalimentación que el cliente pueda dar para proceder con la acción de mitigación correspondiente o continuar con el monitoreo según sea el caso. Si el cliente autoriza una acción de mitigación como un bloqueo se avanza al proceso de escalación, el cual se explica en el siguiente capítulo (Soluciones en seguridad S.A., Descripción del modelo de operación del Security Operation Center, s/f).

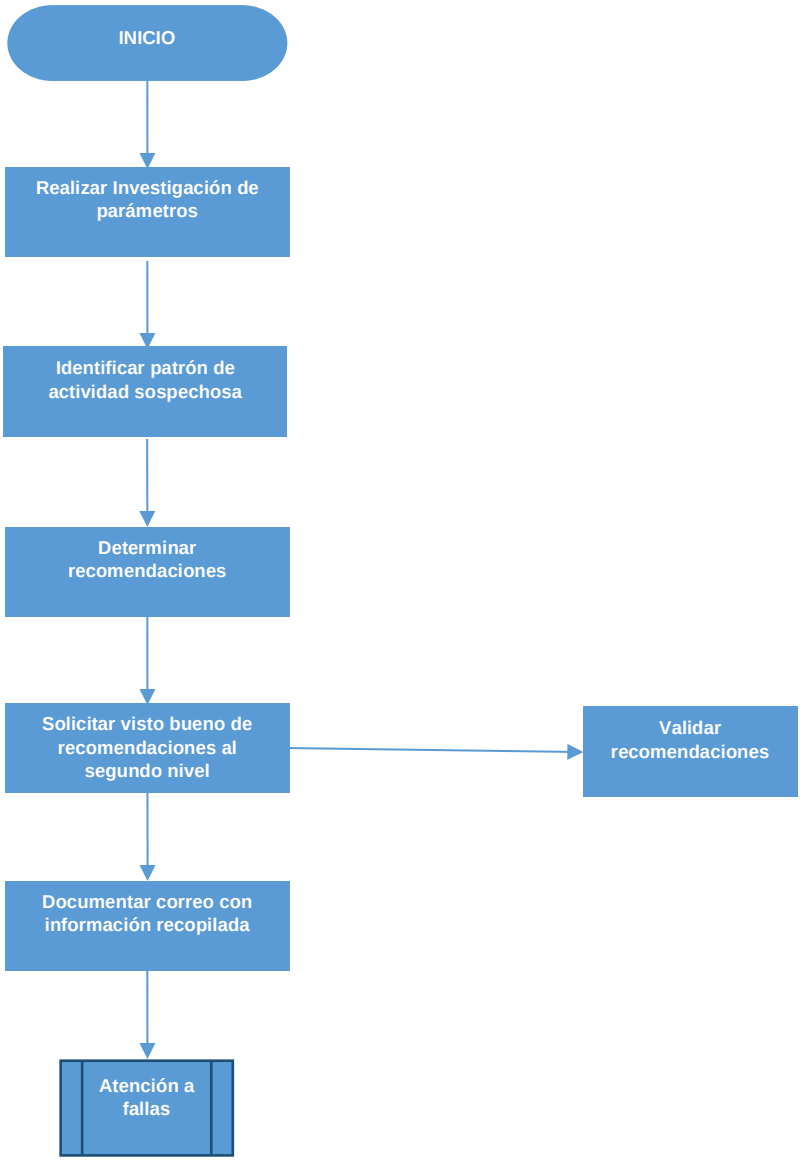



*Diagrama 2.3. Proceso de análisis. Adaptado de (Soluciones en seguridad S.A., Descripción del modelo de operación del Security Operation Center, s/f)*

Así se concluye el segundo proceso comprendido por el área de operación y se da paso al proceso de escalación donde se determina a quién se debe dirigir el incidente detectado.

### 2.3.3 Proceso de escalación

Este es el último proceso que contempla el área de operación y en él concluyen las actividades realizadas por un operador del SOC y comienzan las de niveles superiores. Los procesos posteriores relacionados con contención y mitigación de incidentes corresponden al personal especializado en cada herramienta, encargado de configurar políticas, realizar bloqueos de tráfico, bloqueos de direcciones IP, etc.

Como bien se mencionó en capítulos anteriores el proceso de escalación es aquel en el que se canaliza el incidente o actividad sospechosa una vez analizada con el personal pertinente y con capacidad de mitigarlo o profundizar en la investigación del mismo, si la realizada por el personal de monitoreo no fuera suficiente. En pocas palabras se encargan de pulir el análisis realizado por el operador y determinar si la actividad reportada corresponde a un falso positivo o realmente puede traer consecuencias para el cliente.

Es deber del operador conocer los diferentes niveles de escalación existentes con el fin de dirigir la problemática con el personal correcto. Si fuera el caso, la razón por la que se dirige a los altos mandos es para solicitar la autorización de una acción urgente con las correspondientes pruebas realizadas previamente y justificando al porqué de dicha acción a realizar. Para este fin se cuenta también con documentación especial llamada matriz de escalación en la que se localizan los niveles o personas específicas para cada cliente que cuentan con la facultad de autorizar y tomar ciertas decisiones que pudieran tener un impacto significativo respecto a los activos del cliente como lo muestra la tabla 2.1. Es importante recalcar que en este proceso participan todos los miembros del SOC, tanto el área de operación cómo la de administración. Cada área debe cumplir su parte en el proceso para garantizar que la información sobre la problemática llegue a las manos indicadas.

| Nivel | Rol | Nombre | Número de contacto | Correo |
|---|---|---|---|---|
| **Nivel1** | Ingeniero Nivel 1 | Antonio Aguilar | 55 1111 1111 | antonio.aguilar@empresa.com |
| **Nivel 1** | Ingeniero Nivel 1 | Eduardo Yáñez | 55 2222 2222 | eduardo.yañez@empresa.com |
| **Nivel 1** | Ingeniero Nivel 1 | Javier Hernández | 55 3333 3333 | javier.hernandez@empresa.com |
| **Nivel2** | Jefe de área | Carlos López | 55 4444 4444 | carlos.lopez@empresa.com |
| **Nivel2** | Jefe de área | Pedro Gutiérrez | 55 5555 5555 | pedro.gutierrez@empresa.com |
| **Nivel3** | Directivo | Ricardo Calderón | 55 6666 6666 | ricardo.calderon@empresa.com |

*Tabla 2.1. Ejemplo de Matriz de escalación. Elaboración propia.*

A continuación se describe el proceso de escalación mediante la siguiente secuencia de pasos a seguir:

1. El operador consulta el primer nivel de escalación en la respectiva matriz tomando como criterio la severidad de la actividad sospechosa que se va a alertar.
2. Una vez determinadas las recomendaciones necesarias mediante el proceso de análisis, se procede a enviarlas al nivel de escalación descrito en la matriz.
3. El operador queda a la espera de retroalimentación por parte del nivel de escalación contactado. Si se recibe respuesta por parte del primer nivel de escalación, se determina el tipo de ésta, ya sea requerimiento (extracción de bitácoras, integración a listas negras, continuidad de monitoreo, etc.) o incidente (bloqueo de dirección IP, bloqueo de firma, etc.). En caso de no recibir respuesta, se canaliza el incidente con el siguiente nivel de escalación descrito en la matriz.
4. Si el tipo de respuesta es catalogado como falso positivo se registran los resultados documentando en la base de conocimientos para futuras referencias (Soluciones en seguridad S.A., Descripción del modelo de operación del Security Operation Center, s/f).

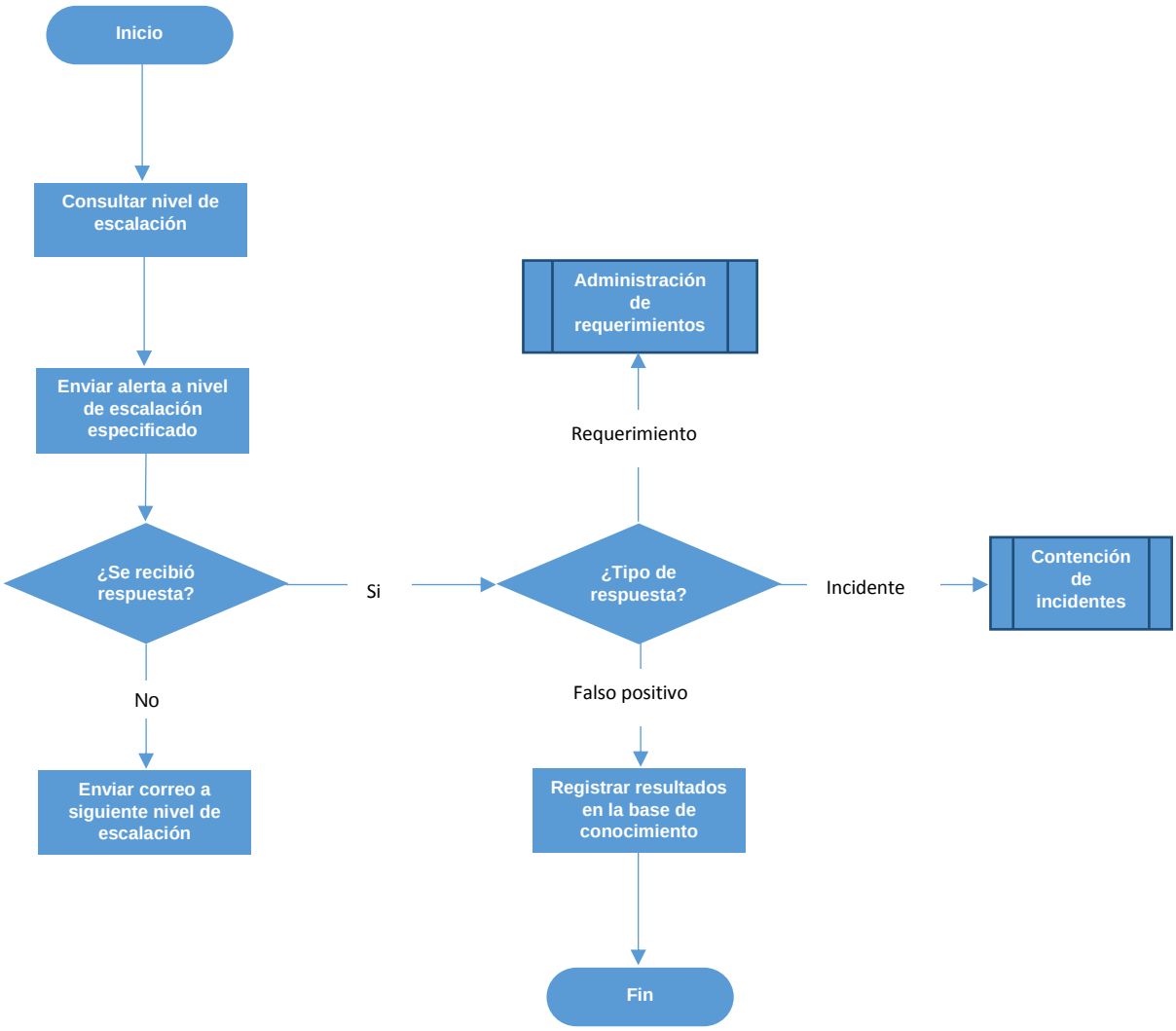



*Diagrama 2.4. Proceso de escalación. Adaptado de (Soluciones en seguridad S.A., Descripción del modelo de operación del Security Operation Center, s/f)*

Estos tres procesos son los que contempla directamente al área de operación y su actividad principal la cual es el monitoreo en tiempo real, sin embargo un SOC cuenta con una cantidad muy amplia de procesos no sólo a nivel operacional y con esto me refiero no sólo a aquellos que involucran directamente trabajar con la información del cliente sino también a las metodologías o buenas prácticas como por ejemplo las normas de la Organización Internacional de Estandarización (ISO) que contemplan procesos para atención a incidentes, procesos para control de cambios, procesos para generar respaldos y procesos de destrucción segura de información entre otros.

# Capítulo 3: Descripción del puesto de operador de un SOC

En este capítulo se habla acerca del perfil con el que debe contar un candidato a operador de un SOC así como los conocimientos y aptitudes que preferentemente debe reunir para un mejor desempeño en el puesto, también se dan a conocer los objetivos que el operador deberá cumplir dentro del SOC.

## 3.1 Perfil del puesto

Como es de suponerse, para poder desempeñar un buen papel dentro de un centro de operaciones de seguridad, es necesario contar con ciertos conocimientos y habilidades básicas, las cuales con el tiempo pueden desarrollarse de tal manera que cuando el SOC lo requiera cuente con el personal adecuado y capaz de llevar acabo análisis cada vez más precisos y profesionales. Pero lo anterior no se da de la noche a la mañana, es decir, todo es parte de un proceso evolutivo por parte del operador o analista hasta convertirse en un experto en seguridad de la información.

Este último aspecto es notorio a medida que pasa el tiempo, ya que al principio la función del operador está basada en seguir procedimientos y metodologías "predefinidas" por parte del SOC y que conforme se adquieren conocimientos y habilidades, el mismo operador puede empezar a dejar un poco de lado este esquema y verse más involucrado y propositivo.

Comenzaré por dar una descripción general del puesto de operador así como los conocimientos requeridos para este rol.

Resulta evidente que si el puesto consiste en el análisis e investigación de eventos relacionados con seguridad informática, los conocimientos necesarios por parte del operador en su mayoría consisten en temas de carácter técnico en áreas cómo redes y seguridad informática como tal, sin embargo, es ideal que el candidato cuente también con conocimientos básicos en áreas como bases de datos y además no podemos dejar de lado la parte administrativa así como el trabajo en equipo y la planeación de proyectos, ya que es importante para el analista el poder desarrollarse hasta llegar a ser capaz de hacerse cargo de un equipo de trabajo.

También es importante que el candidato cuente con interés por la investigación de nuevas vulnerabilidades y ataque informáticos ya que como sabemos el mundo de las TI es constantemente cambiante, por lo que hay que mantenerse al día con todo lo que está pasando "afuera". Por esta razón también es requerido que el candidato sea autodidacta para poder dar seguimiento continuo a las novedades que pudieran presentarse. (Nathans, 2015, pág. 191)

Dentro de los aspectos técnicos requeridos encontramos temas y características como:

- Conocimientos de redes (direccionamiento IP, protocolos, *routing*).
- Conocimientos en metodologías básicas de ataques informáticos.
- Comprensión de general del malware.
- Conocimiento de tecnologías de VPN.
- Habilidad de leer e interpretar diagramas de red.
- Conocimiento básico del modelo OSI.
- Entendimiento de conceptos de administración de redes y software.

## 3.2 Competencias requeridas

"De acuerdo con la Organización para la Cooperación y Desarrollo Económico (OCDE), se entiende por competencias a aquellas habilidades y capacidades adquiridas a través de un esfuerzo deliberado y sistemático por llevar a cabo actividades complejas. Es decir, es la capacidad que se consigue al combinar

conocimientos, habilidades, actitudes y motivaciones y al aplicarla en un determinado contexto: en la educación, el trabajo o el desarrollo personal.” (Ávila, 2016) Una competencia no está limitada a elementos cognitivos (uso de teorías, conceptos o conocimientos implícitos), sino que abarca tanto habilidades técnicas como atributos interpersonales.

Tomando en cuenta la definición anterior, podemos identificar ciertas competencias deseables en un candidato a considerar para laborar en un SOC. Entre ellas encontramos las siguientes:

- **Buena capacidad de redacción:** Es importante debido a que muchas ocasiones se requiere la elaboración de entregables con los cuales se da una explicación a los clientes de qué es lo que está sucediendo con su infraestructura y sus herramientas de seguridad, así que es de suma importancia que estos documentos cuenten con una buena presentación y gran parte de ello se reflejará en la manera en que estén redactadas las ideas.
- **Buena comunicación verbal:** Muchas ocasiones es necesario tener contacto directo con el cliente, por lo que es indispensable una buena transmisión de ideas así como de dejar muy claros todos los puntos que se traten.
- **Habilidades organizacionales:** Una buena organización siempre traerá consigo mayor efectividad y mejores resultados en nuestras actividades.
- **Trabajo bajo presión:** Es importante tener en cuenta que en un SOC los tiempos de respuesta son muy importantes por lo que trabajar bajo presión es una constante que siempre hay que considerar.
- **Resolución de problemas:** Es básicamente la razón de ser de un SOC, así que debemos contar con esta habilidad con el fin de proponer soluciones adecuadas para entregar resultados en tiempo y forma.
- **Técnicas de investigación:** Generalmente esta capacidad se desempeña en el proceso de análisis donde lo más importante es depurar la información de tal manera que nos entregue lo que realmente es importante para cada caso particular.
- **Creatividad y curiosidad:** Son importantes ya que nos ayudan a detectar áreas de oportunidad en el SOC en general.

## 3.3 Objetivos

De acuerdo al perfil establecido previamente, la idea es que el operador desarrolle sus aptitudes y conocimientos de tal manera que pueda, en base a la experiencia y el aprendizaje de nuevas habilidades, ampliar su capacidad de análisis hasta que le

sea posible manejar a su propio equipo de trabajo y buscar mejorar la productividad y eficiencia del SOC. Para lograr este y otros objetivos es importante que el analista se valga de nuevas estrategias y técnicas para conseguir automatizar, optimizar y mejorar los procesos ya existentes, así como proponer nuevos. La idea principal es obtener como resultado mejores tiempos de respuesta y calidad de los servicios prestados.

# Capítulo 4: Reporte de actividades realizadas en el SOC

En este capítulo se desarrollan las actividades correspondientes al informe profesional y se muestra una serie de ejemplos que ilustran las tareas con las que contribuyo dentro del SOC como operador.

## 4.1 Actividades realizadas

A continuación enlistaré las actividades que realizo en el área de monitoreo y pretendo aclarar en qué consisten, así como la importancia que conlleva cada una en el esquema general de monitoreo y detección de incidentes.

Se recomienda al lector consultar el anexo A para una mejor comprensión de las actividades descritas en el presente capítulo, ya que en dicho anexo se encuentra la información técnica correspondiente al monitoreo y la operación de las herramientas, así como ejemplos del alcance que éstas pueden tener de manera más detallada.

### 4.1.1 Estado de salud y Lista de chequeo de herramientas

Como ya hemos mencionado previamente, una parte importante y un objetivo por parte del SOC es cumplir con los principios básicos de la seguridad informática. En esta ocasión me refiero específicamente al principio de disponibilidad, y es que, de nada sirve tener la mejor tecnología existente en detección de amenazas si ésta no se encuentra disponible y funcionando adecuadamente en momentos cruciales. Como proveedores de servicios de seguridad de la información, es de suma importancia que no se detenga la producción de los mismos.

Es por las razones anteriores que existen los términos “lista de chequeo” (*Checklist*) y “estado de salud” (*Health Status*) que en lenguaje coloquial podríamos identificar como “pasar lista” y revisar el estado de salud de las herramientas periódicamente para verificar que todo se encuentre funcionando bien.

Las herramientas de seguridad utilizadas generalmente están divididas en *dashboards*, los cuales son interfaces gráficas que nos ayudan a clasificar y a administrar la información que la herramienta puede proporcionar así como los distintos tipos de funciones que ésta realiza, de esta manera la navegación a través de la herramienta es más fácil y rápida. La Figura 4.1 ilustra cómo se ve el *dashboard* general de una herramienta.

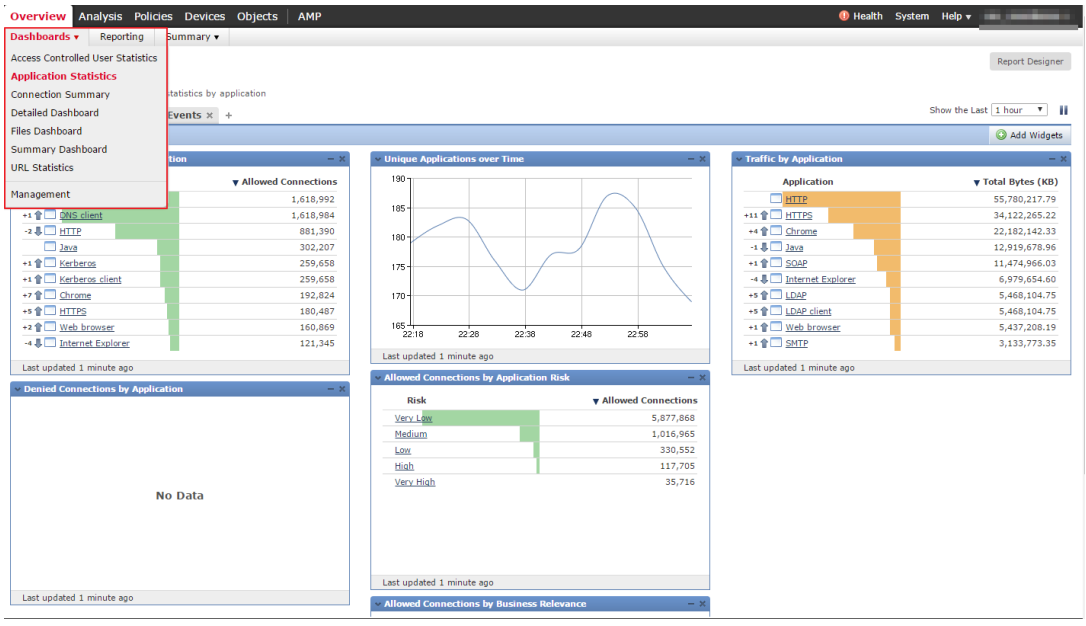



*Figura 4.1. Dashboard principal de un IPS. Obtenida del Software IPS 1.*

La información referente al estado de las herramientas la podemos localizar en el *dashboard* de estado como se muestra a continuación:

La figura 4.2 ilustra el dashboard de estado para un IPS.

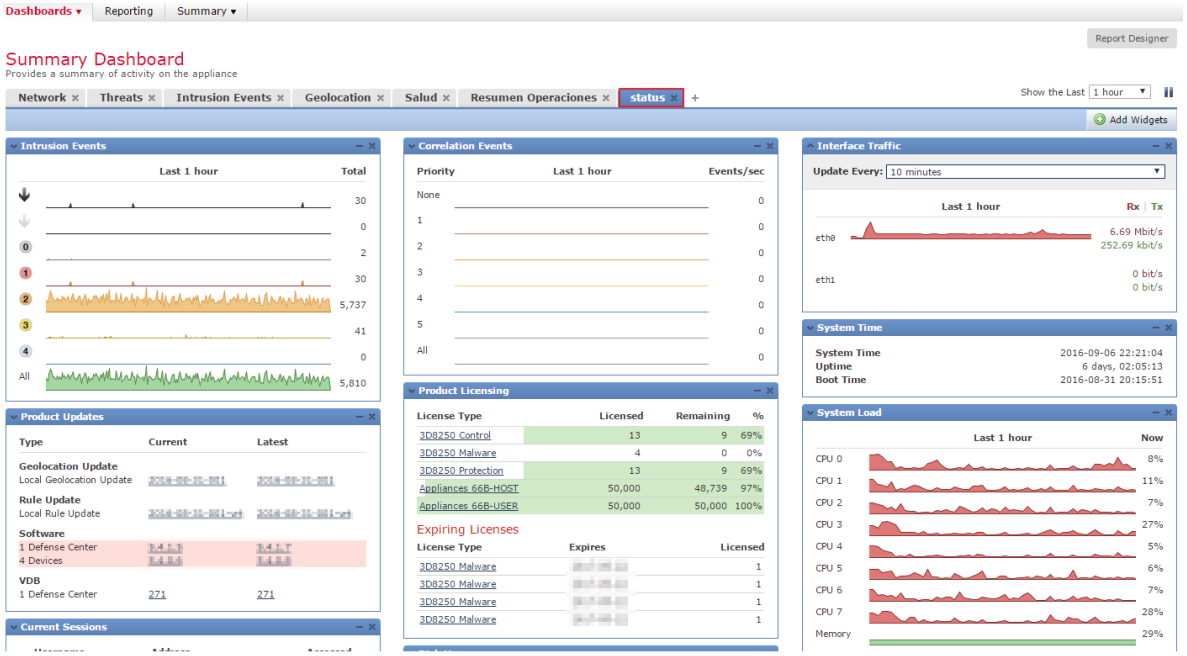



*Figura 4.2. Dashboard de estado de un IPS. Obtenida del Software IPS 1.*

Del mismo modo, la figura 4.3 ilustra el estado de un firewall.

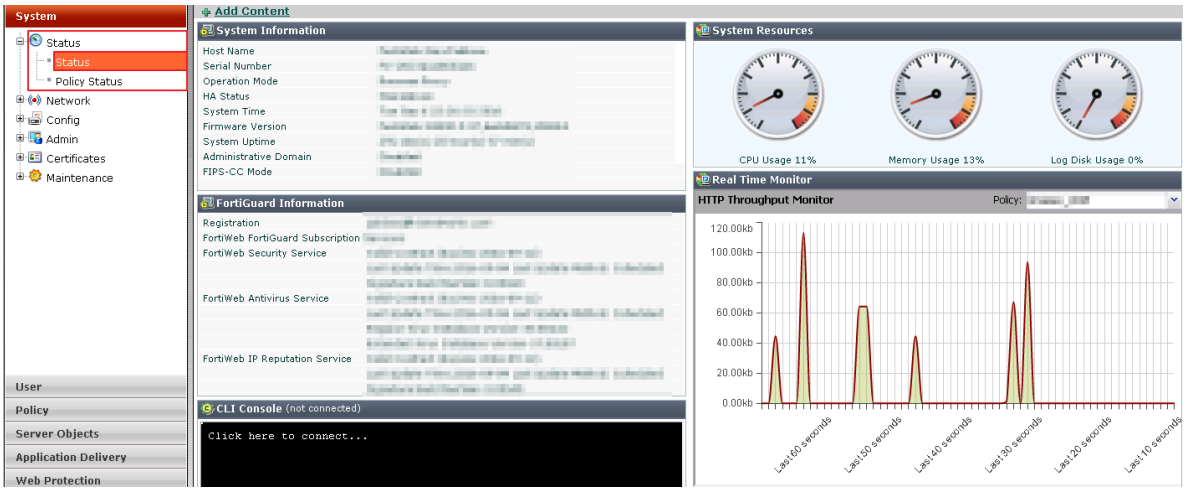



*Figura 4.3. Dashboard de estado de un Firewall. Obtenida del Software Firewall 1.*

Por último, en la figura 4.4 se muestra el estado de un antispam.

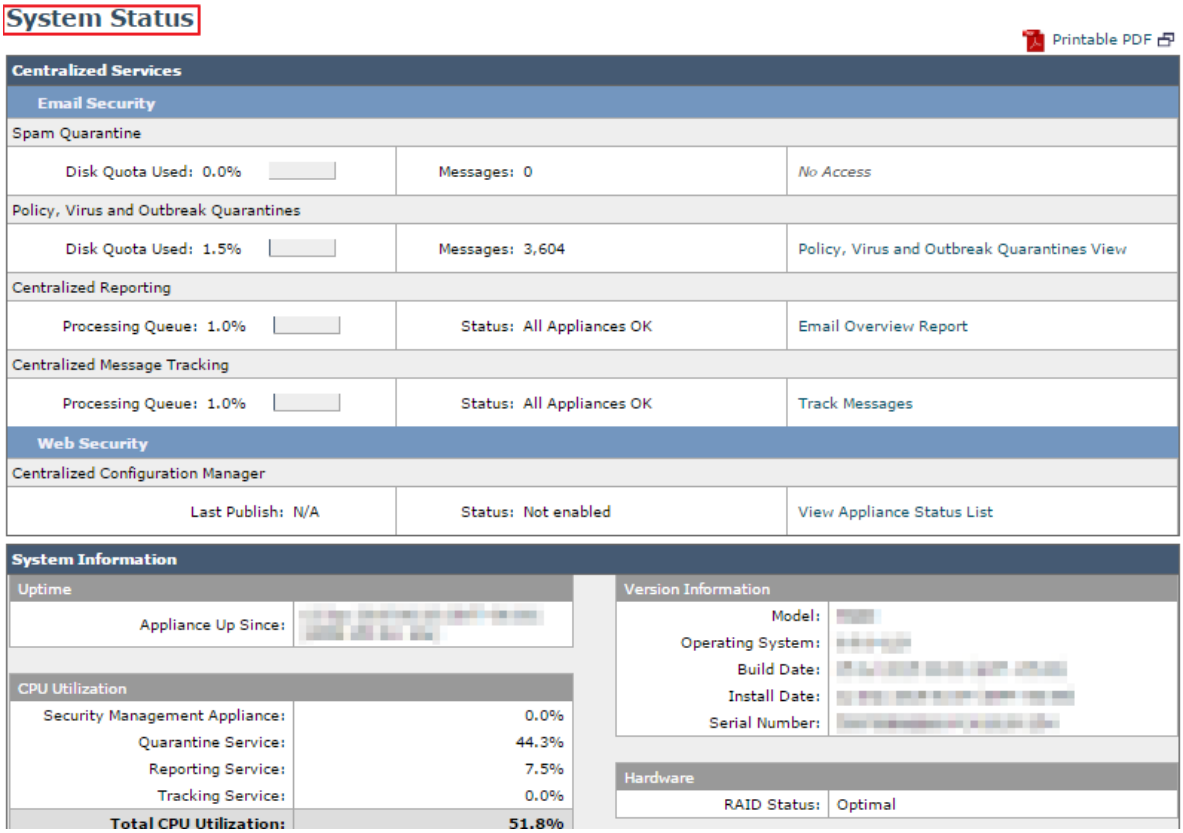



*Figura 4.4. Dashboard de estado de un Antispam. Obtenida del Software Antispam 1.*

Generalmente en estas revisiones lo que se busca es verificar que todos los *appliances* se encuentren “arriba”, que se tenga correcto acceso a cada una de las herramientas de cada cliente, que las herramientas se encuentren recibiendo información en tiempo real y sin interrupciones. Al final de la revisión es necesario realizar un informe con las evidencias correspondientes de los resultados recolectados. En el informe se notificará toda problemática que haya sido localizada y se canaliza con el equipo administrador de la herramienta en cuestión para que se lleven a cabo las acciones necesarias para corregir los fallos.

Es posible configurar correos de alerta por parte de la herramienta para que sean enviados cada vez que se presente una “caída” en un sensor o se rebase algún umbral de memoria o CPU, sin embargo, estas alertas también pueden llegar a presentarse como falsos positivos por lo que es conveniente hacer el chequeo personalmente y así descartar una falsa alarma. En la Figura 4.5 se ilustra un ejemplo de este tipo de notificaciones.

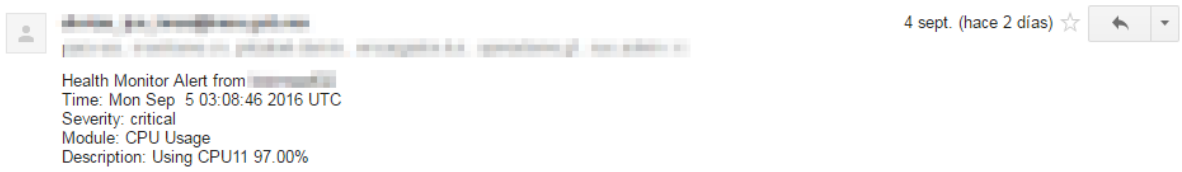



*Figura 4.5. Notificación de uso alto de CPU.*

Para que el *Checklist* cuente con mayor credibilidad y nuestro cliente pueda comprobar que efectivamente todo funciona adecuadamente, es conveniente que en las capturas de pantalla de estado se incluya la evidencia de fecha y hora del sistema dese el cual se realiza el monitoreo, de este modo se puede realizar una comparación entre la fecha y hora del sistema local y las configuradas en cada herramienta para poder detectar alguna anomalía y de ser así, saber el tiempo que ésta lleva presentándose.

Las figuras siguientes ilustran mejor el tipo de evidencia que se debe enviar en el informe.

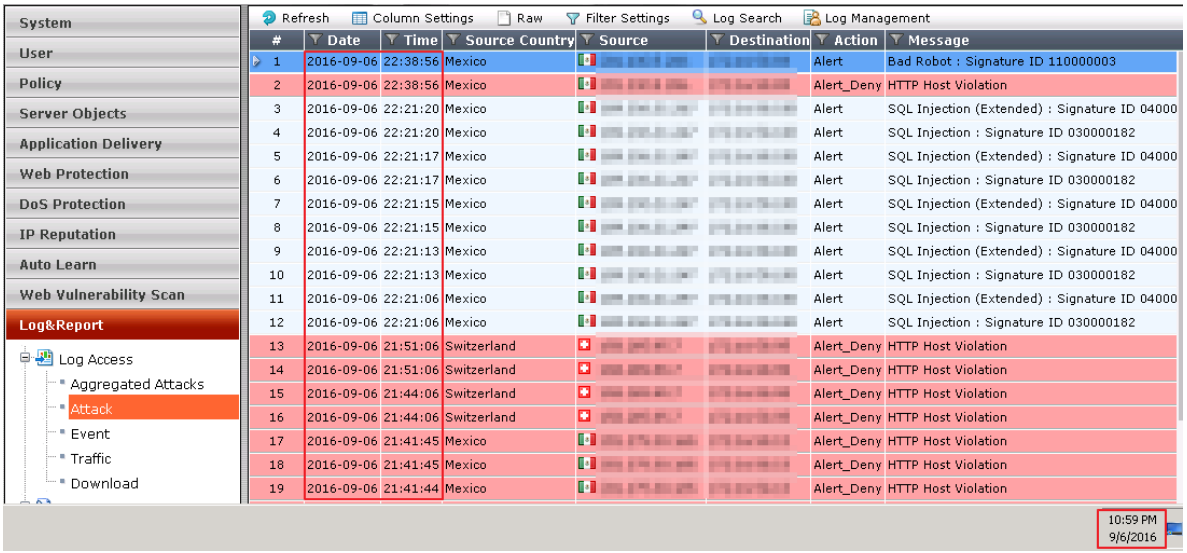



*Figura 4.6. Eventos en tiempo real en un WAF. Obtenida del Software WAF 1.*

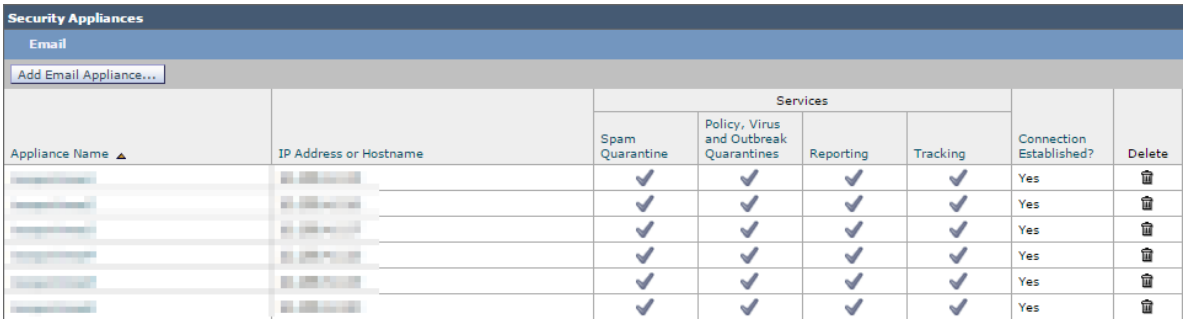



*Figura 4.7. Muestra de estado Ok en todos los sensores de un Antispam. Obtenida del Software Antispam 1.*

Las buenas prácticas de seguridad en cuanto a contraseñas nos indican que es conveniente realizar un cambio de contraseña de acceso al equipo cada cierto tiempo, es por eso que las herramientas se configuran de tal manera que cumplido este periodo, soliciten una nueva contraseña. Este tipo de eventos también deben ser reportados en el *checklist*, de esta manera el administrador tomará en cuenta que el cambio de contraseña en cuestión está próximo y realice la actualización correspondiente. La Figura 4.8 muestra cómo se vería una solicitud de cambio de contraseña por parte de una herramienta.

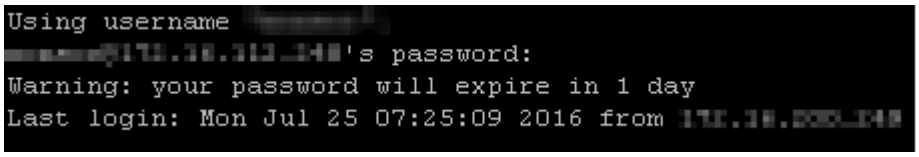



*Figura 4.8. Solicitud de cambio de password vía CLI. Obtenida del Software DAM 1.*

Cabe mencionar que en algunos casos la herramienta cuenta con un registro del tiempo que ha estado activa desde el último reinicio, esta información podemos identificarla en el campo *Uptime* como lo muestra la Figura 4.9. Lo ideal es que este campo de *Uptime* nunca tenga un valor de 0 ya que esto implicaría una caída en el servicio, a menos claro que se tratara de una actividad controlada, para lo cual se debe programar una ventana de mantenimiento en la cual se realicen las actividades requeridas.

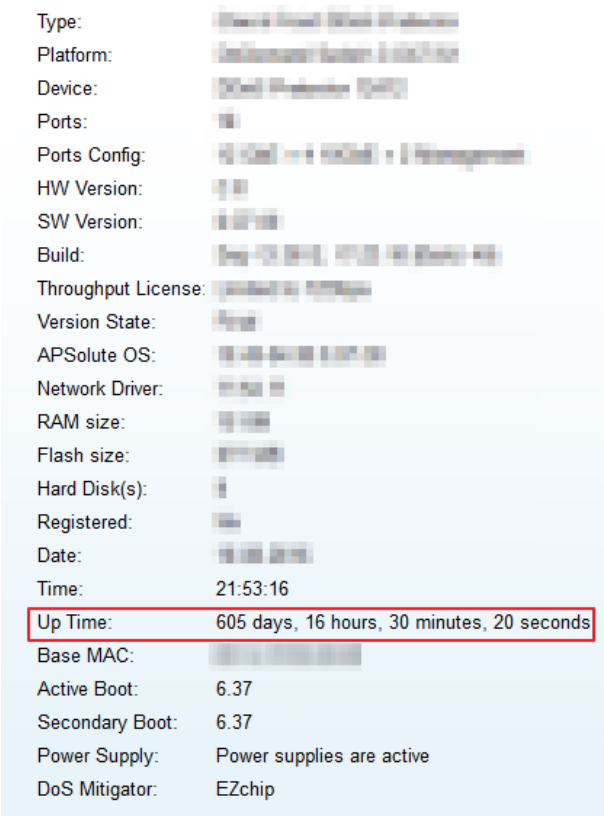



*Figura 4.9. Muestra del Uptime en una herramienta. Obtenida del Software AntiDDoS 1.*

Lo único que resta por ejemplificar es qué tipo de problemáticas pueden presentarse durante la revisión realizada, aunque ya hemos mencionado que principalmente son temas de disponibilidad.

En las figuras 4.10 y 4.11 se ilustra una variación en el estado de una herramienta, indicando el nombre del dispositivo, así como su correspondiente dirección IP, estos datos son importantes para agilizar la solución del problema que se haya presentado. Esta problemática debe registrarse en el *checklist* y además debe ser notificada al personal al de administración para que realice los ajustes necesarios y así poder corregirla.

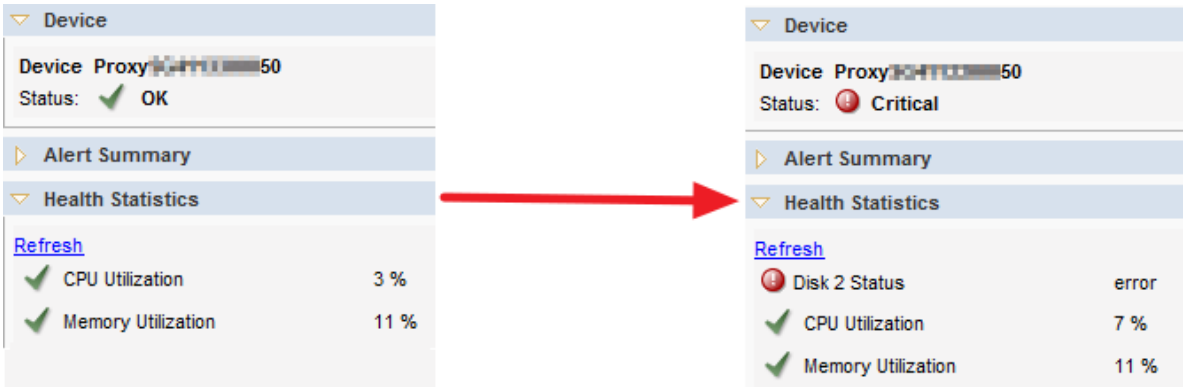



*Figura 4.10. Cambio de estado de Ok a crítico en una herramienta. Obtenida del Software Web Filter 1.*

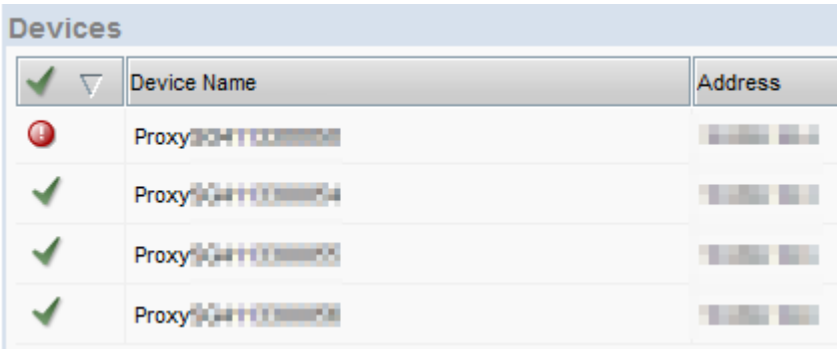



*Figura 4.11. Detalles del estado del sensor con problemas. Obtenida del Software Web Filter 1.*

Finalmente, el informe debe contar con una tabla a manera de resumen donde se registran aquellas problemáticas encontradas en los dispositivos revisados, es ideal que esta tabla se localice al inicio del informe para que el cliente o administrador que la revise pueda enfocarse exclusivamente en la problemática que pudiera llegar a presentarse.

La tabla mencionada deberá tener una forma como la siguiente:

| Dispositivo de Seguridad | Estado |
|---|---|
| **AntiDDoS 1 (x.x.x.x)** | OK |
| **AntiDDoS 2 (x.x.x.x.)** | OK |
| **Sensor IPS 1 (x.x.x.x.)** | OK |
| **Sensor IPS 2 (x.x.x.x.)** | OK |
| **Proxy 1 de Web Filter (x.x.x.x)** | OK |

| Dispositivo de Seguridad | Estado |
|---|---|
| **Proxy 2 de Web Filter (x.x.x.x)** | Critical.<br><br>En el periodo reportado presentó un error en uno de los discos. |
| **Web filter centralizado (x.x.x.x)** | La contraseña expirará en 1 día. |
| **Sensor 1 de Antispam (x.x.x.x)** | OK |
| **Sensor 2 de Antispam (x.x.x.x)** | OK |

*Tabla 4.1. Ejemplo de Checklist de herramientas. Elaboración propia.*

Como se puede notar, es de suma importancia llevar un control de las herramientas para que, en caso de presentar algún incidente ya sea a nivel de red o a nivel físico éste sea escalado y resuelto de manera oportuna, así las operaciones por parte del SOC no se verán interrumpidas.

En el diagrama 6 se muestra el proceso que conlleva la realización de ésta actividad.

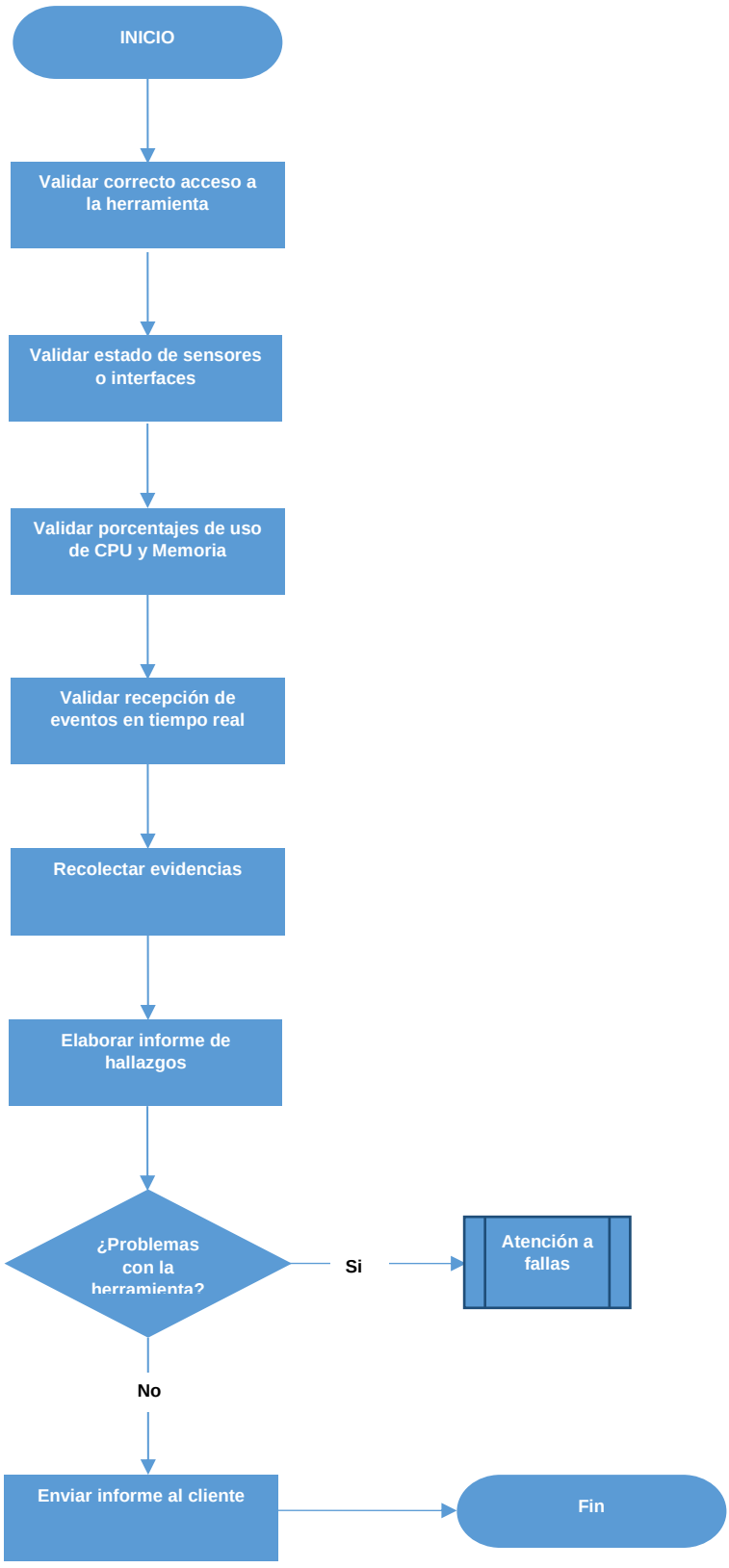



*Diagrama 4.1. Proceso de checklist y health status. Elaboración propia.*

Es aquí donde concluyo la sección correspondiente a esta actividad para dar paso a temas que tienen que ver más con la parte de análisis que como se vio previamente es uno de los procesos principales que desempeña el SOC.

### 4.1.2 Análisis de firmas de IPS

Haciendo un breve recordatorio al proceso de análisis, básicamente consiste en hacer una revisión cada cierto tiempo de acuerdo a lo pactado con el cliente, se extraen las bitácoras de la herramienta, se procesan para su análisis (parseo), y se entrega un informe con la actividad sospechosa encontrada, así como las recomendaciones para su mitigación. En este caso explicaré la forma en que se realiza el análisis de firmas en un IPS basado en detección de firmas.

Existen distintos criterios a considerar por ejemplo el tipo de firma y si el tráfico presentado para la misma es entrante o saliente, incluso puede darse de manera interna (tanto el origen como el destino son activos dentro de la red del cliente), la severidad o impacto de la firma, etc.

El proceso comienza accediendo al IPS en el menú de eventos, los cuales podremos observar en tiempo real como lo muestra la Figura 4.12. En esta primera vista se observa que el IPS proporciona una considerable cantidad de información para cada evento como la fecha y la hora de detección, los puertos empleados, el origen y el destino para el tráfico detectado, el tipo de evento o nombre de la firma y uno de los puntos más importantes: si la firma se encuentra bloqueada por el IPS o no.

Como se requiere analizar un periodo de tiempo en específico es necesario aplicar un filtro en el campo de fecha y hora de eventos para así enfocarnos a los eventos de nuestro interés como lo ilustra la Figura 4.13.

| Time | Priority | Impact | Inline Result | Source IP | Source Country | Destination IP | Destination Country | Source Port / ICMP Type | Destination Port / ICMP Code | SSL Status | VLAN ID | Message |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2016-09-07 04:05:05 | low | 2 | | | USA | | | 65156 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI_CLIENT_BARE |
| 2016-09-07 04:05:00 | low | 2 | | | | | | 52932 / tcp | 32843 / tcp | Unknown (Unknown) | 367 | HI_CLIENT_BARE |
| 2016-09-07 04:05:00 | low | 2 | | | | | | 54385 / tcp | 32843 / tcp | Unknown (Unknown) | 369 | HI_CLIENT_BARE |
| 2016-09-07 04:04:55 | low | 2 | | | USA | | | 65154 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI_CLIENT_BARE |
| 2016-09-07 04:04:53 | low | 2 | | | USA | | | 65152 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI_CLIENT_BARE |
| 2016-09-07 04:04:24 | low | 2 | | | | | | 56182 / tcp | 8003 / tcp | Unknown (Unknown) | 305 | HI_CLIENT_BARE |
| 2016-09-07 04:04:24 | low | 2 | | | | | | 43366 / tcp | 8003 / tcp | Unknown (Unknown) | 305 | HI_CLIENT_BARE |
| 2016-09-07 04:04:23 | low | 2 | | | USA | | | 63100 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI_CLIENT_BARE |
| 2016-09-07 04:04:14 | low | 2 | | | | | | 58883 / tcp | 32843 / tcp | Unknown (Unknown) | 369 | HI_CLIENT_BARE |
| 2016-09-07 04:04:05 | low | 2 | | | USA | | | 65147 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI_CLIENT_BARE |
| 2016-09-07 04:03:55 | low | 2 | | | USA | | | 65145 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI_CLIENT_BARE |
| 2016-09-07 04:03:53 | low | 2 | | | USA | | | 65143 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI_CLIENT_BARE |
| 2016-09-07 04:03:24 | low | 2 | | | | | | 43279 / tcp | 8003 / tcp | Unknown (Unknown) | 305 | HI_CLIENT_BARE |
| 2016-09-07 04:03:24 | low | 2 | | | | | | 56083 / tcp | 8003 / tcp | Unknown (Unknown) | 305 | HI_CLIENT_BARE |
| 2016-09-07 04:03:05 | low | 2 | | | USA | | | 65136 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI_CLIENT_BARE |
| 2016-09-07 04:02:55 | low | 2 | | | USA | | | 65134 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI_CLIENT_BARE |
| 2016-09-07 04:02:53 | low | 2 | | | USA | | | 65132 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI_CLIENT_BARE |
| 2016-09-07 04:02:24 | low | 2 | | | | | | 55996 / tcp | 8003 / tcp | Unknown (Unknown) | 305 | HI_CLIENT_BARE |
| 2016-09-07 04:02:24 | low | 2 | | | | | | 43180 / tcp | 8003 / tcp | Unknown (Unknown) | 305 | HI_CLIENT_BARE |

Page 1 of 144 Displaying rows 1–25 of 3596 rows

*Figura 4.2. Eventos en tiempo real en un IPS. Obtenida del Software IPS 1.*

Events By Priority and Classification (switch workflow)

Drilldown of Event, Priority, and Classification › **Table View of Events** › Packets

2016-09-06 22:00:00 - 2016-09-07 02:00:00 Static

Disabled Columns

▸ Search Constraints (Edit Search Save Search)

Jump to... ▾

| Time | Priority | Impact | Inline Result | Source IP | Source Country | Destination IP | Destination Country | Source Port / ICMP Type | Destination Port / ICMP Code | SSL Status | VLAN ID | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2016-09-07 01:59:55 | low | 2 | | | USA | | | 63910 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI |
| 2016-09-07 01:59:53 | low | 2 | | | USA | | | 63908 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI |
| 2016-09-07 01:59:24 | low | 2 | | | | | | 45131 / tcp | 8003 / tcp | Unknown (Unknown) | 305 | HI |
| 2016-09-07 01:59:24 | low | 2 | | | | | | 60545 / tcp | 8003 / tcp | Unknown (Unknown) | 305 | HI |
| 2016-09-07 01:59:21 | low | 3 | | | | | USA | 64368 / tcp | 5985 / tcp | Unknown (Unknown) | 301 | HI |
| 2016-09-07 01:10:25 | low | 2 | | | | | | 62880 / tcp | 8001 / tcp | Unknown (Unknown) | 310 | HI |
| 2016-09-07 01:10:25 | low | 2 | | | | | | 62876 / tcp | 8015 / tcp | Unknown (Unknown) | 310 | HI |
| 2016-09-07 01:10:24 | low | 2 | | | | | | 55849 / tcp | 8003 / tcp | Unknown (Unknown) | 305 | HI |
| 2016-09-07 00:22:24 | low | 2 | | | | | | 35807 / tcp | 8003 / tcp | Unknown (Unknown) | 305 | HI |
| 2016-09-07 00:22:24 | low | 2 | | | | | | 51223 / tcp | 8003 / tcp | Unknown (Unknown) | 305 | HI |
| 2016-09-07 00:22:22 | low | 2 | | | | | | 52452 / tcp | 8001 / tcp | Unknown (Unknown) | 310 | HI |
| 2016-09-07 00:22:05 | low | 2 | | | USA | | | 62915 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI |
| 2016-09-07 00:22:03 | low | 2 | | | | | | 52421 / tcp | 8001 / tcp | Unknown (Unknown) | 305 | HI |
| 2016-09-06 23:00:32 | low | 2 | | | | | | 46672 / tcp | 7777 / tcp | Unknown (Unknown) | 355 | HI |
| 2016-09-06 23:00:26 | low | 2 | | | USA | | | 55495 / tcp | 8080 / tcp | Unknown (Unknown) | 310 | HI |
| 2016-09-06 23:00:24 | low | 2 | | | | | | 56515 / tcp | 8003 / tcp | Unknown (Unknown) | 305 | HI |
| 2016-09-06 22:00:42 | low | 2 | | | | | | 42582 / tcp | 8003 / tcp | Unknown (Unknown) | 323 | HI |
| 2016-09-06 22:00:39 | low | 2 | | | | | | 36497 / tcp | 8001 / tcp | Unknown (Unknown) | 323 | HI |
| 2016-09-06 22:00:38 | low | 2 | | | MEX | | | 60081 / tcp | 80 (http) / tcp | Unknown (Unknown) | 323 | HI |

*Figura 4.3. Búsqueda de eventos en un periodo de tiempo específico. Obtenida del Software IPS 1.*

Como se puede observar, el IPS arroja una gran cantidad de eventos los cuales sería una tarea muy exhaustiva tratar de analizar a simple vista o directamente en la herramienta, por lo que, para mayor comodidad y facilidad se realiza la extracción del archivo con las bitácoras correspondientes al periodo especificado. Cada IPS cuenta con un menú para extracción de bitácoras como lo muestran las Figuras 4.14 y 4.15, sin embargo, en ambos casos se obtendrá el resultado deseado: un archivo en formato .csv, el cual podremos abrir con un procesador de hojas de cálculo como Excel, donde además de visualizar los eventos podremos realizar filtros, conteos y gráficas en caso de ser requerido.

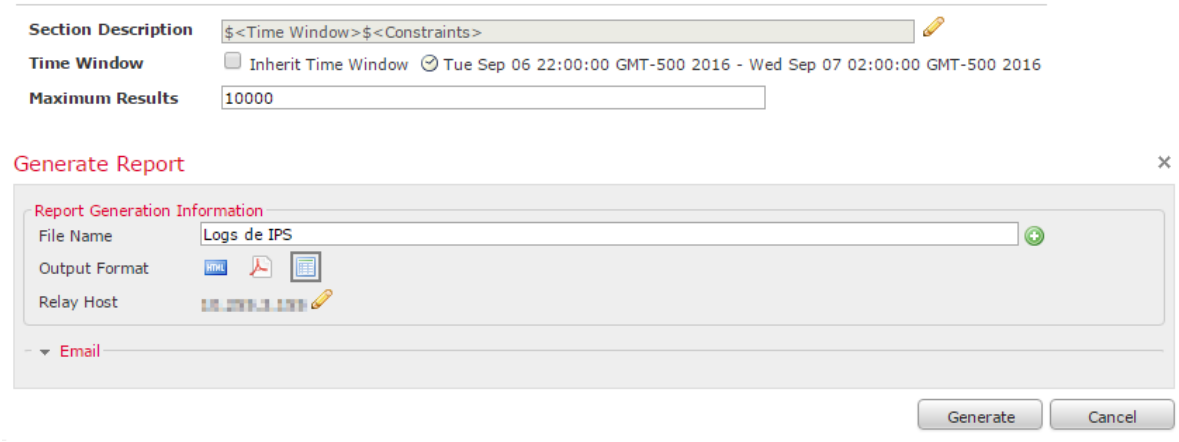



*Figura 4.4. Extracción de bitácoras en un IPS 1. Obtenida del Software IPS 1.*

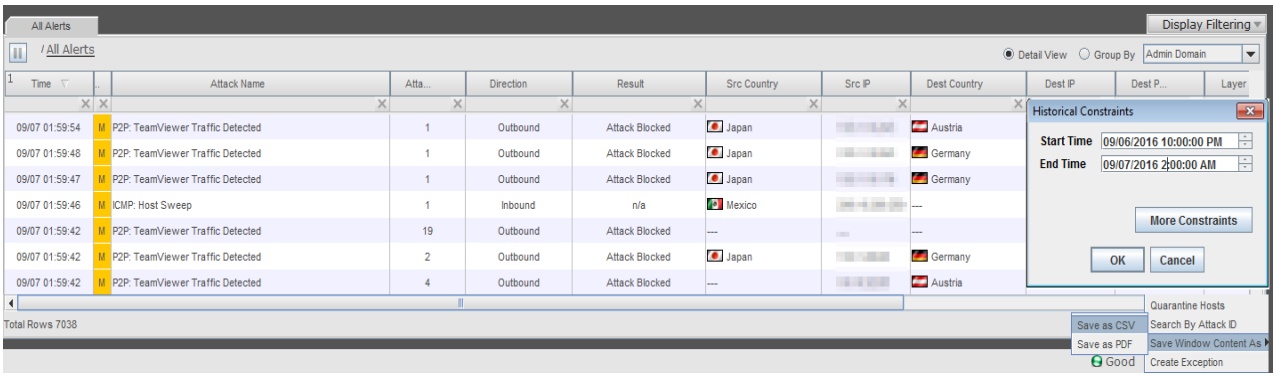



*Figura 4.5. Extracción de bitácoras en un IPS 2. Obtenida del Software IPS 2.*

Una vez descargado el archivo con las bitácoras, se procede a hacer el parseo de la información en Excel, de este modo es posible enfocarse exclusivamente en la información que realmente es útil de acuerdo a los criterios establecidos con el cliente como pueden ser: hacer caso omiso de ciertos eventos especificados por él, sólo analizar los eventos que presenten severidad media o alta, ignorar todos aquellos eventos que presenten tráfico interno, etc.

Esta primera parte del análisis y procesamiento de información se realiza de la siguiente manera. Lo primero que se observará una vez abierto el archivo de bitácoras es la misma información que se encuentra en el *dashboard* de eventos en el IPS separado por columnas y registrando evento por evento, es decir, no se muestra una cuenta general de cuantos hits hubo por cada tipo de evento, sino que cada fila es tratada como un evento independiente. Se podría tener 1000 filas para un mismo tipo de evento, sin embargo, como cada uno fue detectado en un instante de tiempo diferente, se genera un registro por cada uno, esto se muestra en la Figura 4.16.

| Time | Priority | Impact | Inline Result | Source IP | Source Coun | Destination | Destination | Source Port / | Destination | SSL Status | VLAN ID | Message | Classificatior |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 07/09/2016 01:59 | low | Impact 2 | 0 | | USA (United | | | 63910 / tcp | 8080 / tcp | Unknown (U | 310 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:59 | low | Impact 2 | 0 | | USA (United | | | 63908 / tcp | 8080 / tcp | Unknown (U | 310 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:59 | low | Impact 2 | 0 | | | | | 45131 / tcp | 8003 / tcp | Unknown (U | 305 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:59 | low | Impact 2 | 0 | | | | | 60545 / tcp | 8003 / tcp | Unknown (U | 305 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:59 | low | Impact 3 | 0 | | | | USA (United | 64368 / tcp | 5985 / tcp | Unknown (U | 301 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:59 | low | Impact 3 | 0 | | | | USA (United | 64439 / tcp | 5985 / tcp | Unknown (U | 301 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:59 | low | Impact 3 | 0 | | | | USA (United | 64424 / tcp | 5985 / tcp | Unknown (U | 301 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:59 | low | Impact 2 | 0 | | | | | 48270 / tcp | 8003 / tcp | Unknown (U | 323 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:59 | low | Impact 3 | 0 | | | | USA (United | 64388 / tcp | 5985 / tcp | Unknown (U | 301 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:59 | low | Impact 2 | dropped | | USA (United | | | 63904 / tcp | 8080 / tcp | Unknown (U | 310 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:59 | low | Impact 3 | dropped | | | | USA (United | 64362 / tcp | 5985 / tcp | Unknown (U | 301 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:58 | low | Impact 2 | dropped | | USA (United | | | 63901 / tcp | 8080 / tcp | Unknown (U | 310 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:58 | low | Impact 2 | dropped | | USA (United | | | 63899 / tcp | 8080 / tcp | Unknown (U | 310 | HI_CLIENT_BARE_BYTE | Not Suspicio |
| 07/09/2016 01:58 | low | Impact 3 | dropped | | | | USA (United | 64418 / tcp | 5985 / tcp | Unknown (U | 301 | HI_CLIENT_BARE_BYTE | Not Suspicio |

*Figura 4.6. Archivo de bitácoras sin parsear.*

Ya que la cantidad de registros es muy alta, es aquí donde se hace uso de las funciones que proporciona una herramienta como lo es Excel, de tal manera que es posible utilizar un conjunto de filtros para “desechar” toda aquella información que no fuera relevante para el análisis que se está llevando a cabo. Cabe mencionar que se puede hacer un arreglo con filtros directamente en el IPS, sin embargo, la información sólo se puede visualizar y no se podría manipular de la misma manera para buscar más detalles. Es posible filtrar por un tipo de evento en particular, por dirección de origen, por severidad, etc. Dependiendo qué tan específico se quiera realizar el análisis, se puede considerar otras utilidades de Excel como se verá más adelante, ya que en este caso se mostrarían todos los campos asociados a cada registro o evento, es decir, se realiza la búsqueda por tipo de evento por ejemplo y se visualizarían todos los datos además de los que son de interés.

Si se quiere ser más específico en el análisis (que sería ideal) es posible apoyarse de una utilidad de Excel llamada tablas dinámicas, las cuales ofrecen opciones de filtrado más avanzadas y permiten agrupar la información para que sea más fácil realizar búsquedas y la visualización sea más cómoda. Las tablas dinámicas lo que hacen es que permiten clasificar la información mediante una especie de jerarquía de árbol con la cual es posible buscar información concreta referente a cada campo, además de que concentran todos los registros y muestra sólo aquellos que nos interesan más. Además, las tablas dinámicas realizan el conteo automáticamente de cuantos registros existen por cada categoría, de tal manera que proporcionan la información necesaria para poder responder las siguientes cuestiones ¿cuántos tipos diferentes de firmas se registraron durante el periodo a analizar?, de esas firmas, ¿cuántos hits hubo por cada una?, ¿cuántas firmas de severidad alta fueron detectadas en el periodo?, entre otras.

Las Figuras 4.17 y 4.18 ejemplifican mejor lo que quiero decir en este punto. En ellas primero se indica que clasifique los eventos por severidad, después se coloca el tipo de firma que se presentó seguido de las direcciones tanto de origen como destino. Si fuera necesario contemplar algún otro campo como el puerto, el sensor

que lo capturó, entre otros, bastaría con agregarlo a la tabla dinámica para que éste sea mostrado también.

| Firmas clasificadas por severidad | Hits |
|---|---|
| high | 201 |
| BLACKLIST DNS request for known malware domain msnsolution.nicaze.net - Genome Trojan (1:26583:1) | 71 |
| BLACKLIST DNS request for known malware domain megabrowse.biz - Win.Trojan.Mudrop (1:30833:2) | 67 |
| BLACKLIST DNS request for known malware domain luckyleap.net - Win.Trojan.Mudrop (1:30832:2) | 32 |
| BLACKLIST DNS request for known malware domain browsesmart.net - Win.Trojan.Mudrop (1:30826:2) | 22 |
| BLACKLIST DNS request for known malware domain mda.no-ip.org - Win.Trojan.Jenxcus (1:29848:1) | 6 |
| INDICATOR-COMPROMISE Suspicious .pw dns query (1:28039:5) | 3 |
| low | 4322 |
| HI_CLIENT_BARE_BYTE (119:4:1) | 2980 |
| HI_CLIENT_IIS_UNICODE (119:7:1) | 792 |
| SMTP_B64_DECODING_FAILED (124:10:1) | 545 |
| HI_CLIENT_DOUBLE_DECODE (119:2:1) | 3 |
| HI_CLIENT_WEBROOT_DIR (119:18:1) | 2 |
| medium | 15583 |
| HI_CLIENT_OVERSIZE_DIR (119:15:2) | 15540 |
| DCE2_EVENT__SMB_INVALID_SHARE (133:26:2) | 28 |
| SERVER-APACHE Apache mod_proxy reverse proxy information disclosure attempt (1:20528:12) | 7 |
| FTPP_FTP_INVALID_CMD (125:2:2) | 4 |
| DCE2_EVENT__CL_DATA_LT_HDR (133:42:2) | 2 |
| DCE2_EVENT__SMB_BAD_NBSS_TYPE (133:2:2) | 2 |
| Total general | 20106 |

*Figura 4.7. Firmas clasificadas por severidad.*

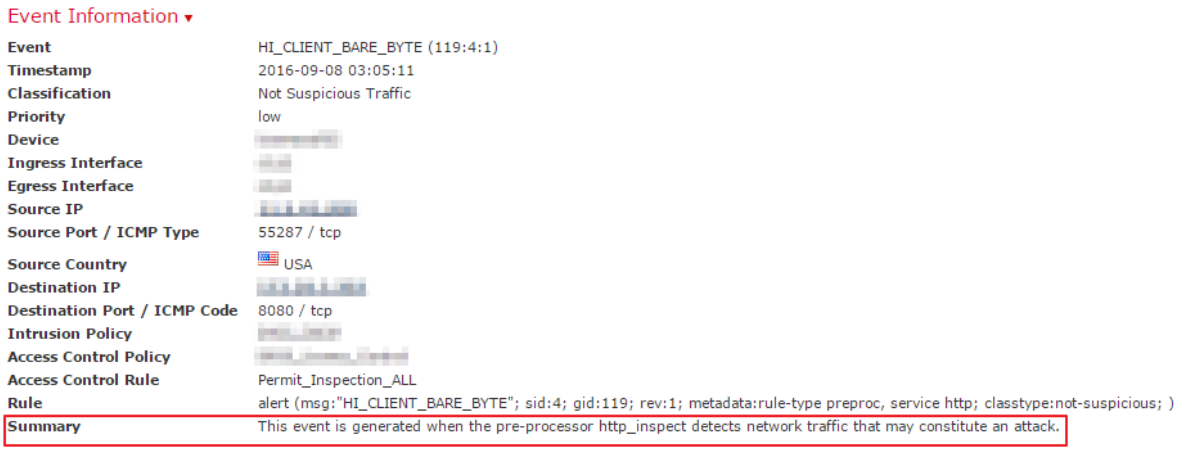
| Firmas clasificadas por severidad y por direcciones de origen y destino | Hits |
|---|---|
| high | 201 |
| BLACKLIST DNS request for known malware domain msnsolution.nicaze.net - Genome Trojan (1:26583:1) | 71 |
| IP origen x.x.x.x | 18 |
| IP Destino1 x.x.x.x | 2 |
| IP Destino2 x.x.x.x | 1 |
| IP Destino3 x.x.x.x | 1 |

*Figura 4.8. Firmas clasificadas por severidad, origen y destino.*

Es así como es posible generar datos estadísticos mediante la creación de *Top's* para identificar ciertas tendencias y patrones que pudieran representar una afectación, pero eso se verá más adelante en el tema correspondiente al reporteo.

La siguiente etapa del análisis consiste en que una vez parseadas las bitácoras, se procede a buscar información adicional que pudiera ayudar a descartar falsos positivos, detalles como la descripción de la firma, la reputación de la dirección IP de origen, búsqueda en listas blancas proporcionadas por el cliente, por mencionar algunos, ayudan bastante al operador y al equipo de administración para determinar si el evento requiere una mayor atención.

Nos enfocaremos ahora en la búsqueda de información y detalles de una firma, la cual en algunos casos el mismo IPS proporciona (Figura 4.19), sin embargo, muchas veces estos detalles no son suficientes y es necesario profundizar un poco más. Para ello es posible apoyarse de la documentación que se encuentra en sitios dedicados a la investigación de vulnerabilidades, virus y malware; entre estos se puede mencionar el portal de CISCO (https://tools.cisco.com/security/center/publicationListing.x), Snort (https://www.snort.org/) y Virus Total (https://www.virustotal.com/es/). Para realizar la investigación pueden utilizarse los datos arrojados por el IPS como pueden ser el nombre de la firma en sí, el ID de la vulnerabilidad o el CVE (*Common Vulnerabilities and Exposures*) el cual es un diccionario de vulnerabilidades que brinda información general de la vulnerabilidad, ya que pudieran existir variantes de la misma firma, sin embargo, haciendo uso del CVE se identificará cual es la firma raíz sin importar el nombre que se maneje en cada IPS.


Event Information ▾

| | |
|---|---|
| **Event** | HI_CLIENT_BARE_BYTE (119:4:1) |
| **Timestamp** | 2016-09-08 03:05:11 |
| **Classification** | Not Suspicious Traffic |
| **Priority** | low |
| **Device** | |
| **Ingress Interface** | |
| **Egress Interface** | |
| **Source IP** | |
| **Source Port / ICMP Type** | 55287 / tcp |
| **Source Country** | USA |
| **Destination IP** | |
| **Destination Port / ICMP Code** | 8080 / tcp |
| **Intrusion Policy** | |
| **Access Control Policy** | |
| **Access Control Rule** | Permit_Inspection_ALL |
| **Rule** | alert (msg:"HI_CLIENT_BARE_BYTE"; sid:4; gid:119; rev:1; metadata:rule-type preproc, service http; classtype:not-suspicious; ) |
| **Summary** | This event is generated when the pre-processor http_inspect detects network traffic that may constitute an attack. |

*Figura 4.9. Detalles de firma proporcionados por el IPS. Obtenida del Software IPS 1.*

Una vez conocidos los detalles de la firma, se realiza una comparación con las características registradas por el IPS para determinar si el evento efectivamente presenta un patrón de comportamiento similar al documentado en Snort o el portal consultado y de ser así, proceder con el alertamiento correspondiente siempre y cuando no se encuentre bloqueada y si es que pudiera representar una afectación. Si no presenta un patrón malicioso, se puede considerar la firma como falso positivo y continuar con las actividades de monitoreo, ya que como se mencionó en capítulos previos, no siempre un evento no bloqueado representa una amenaza.

Un par de datos adicionales que pueden ayudar a complementar el análisis son la localización geográfica de la dirección de origen y la reputación de la misma. Para verificar estos parámetros existen muchas herramientas en línea, estando Whois

(https://who.is/), MXTOOLBOX (https://mxtoolbox.com/) y Whatsmyipadress (https://whatismyipaddress.com/) entre las más populares. Estos datos son muy importantes ya que nos ayudan a determinar si una conexión puede ser maliciosa o no (si el cliente a su vez sólo cuenta con usuarios de carácter nacional, sería extraño que reciba peticiones desde la India o China). La Figura 4.20 ilustra el tipo de información que arroja una página como lo es CQ Counter (http://www.cqcounter.com/whois/). Entre los detalles proporcionados se encuentran el país, la organización o empresa de procedencia y una vista previa de la ubicación. Por otro lado, la Figura 4.21 ilustra los detalles proporcionados por MXTOOLBOX para la reputación de una dirección IP; básicamente aquí lo importante es conocer si la dirección en cuestión se encuentra en listas negras (evidentemente entre más listas negras la registren, más pobre es su reputación, por lo que puede hacernos desconfiar de la legitimidad de la petición) y si es así, cuál es la razón por la que cada portal la considera como una dirección de baja reputación; algunas de las razones más comunes son que han sido identificadas como potenciales fuentes de spam o que han sido identificadas como parte de alguna *botnet* para realizar ataques de DoS.

## 69.109.123.185 - Geo Information

| | |
|---|---|
| IP Address | 69.109.123.185 |
| Host | adsl-69-109-123-185.dsl.pltn13.pacbell.net |
| Location | US, United States |
| City | Fulton, CA 95439 |
| Organization | AT&T Internet Services |
| ISP | AT&T Internet Services |
| AS Number | AS7018 AT&T Services, Inc. |
| Latitude | 38°49'50" North |
| Longitude | 122°77'28" West |
| Distance | 10360.82 km (6437.91 miles) |

## Map Location new

World Map | Google Maps | Yahoo Maps

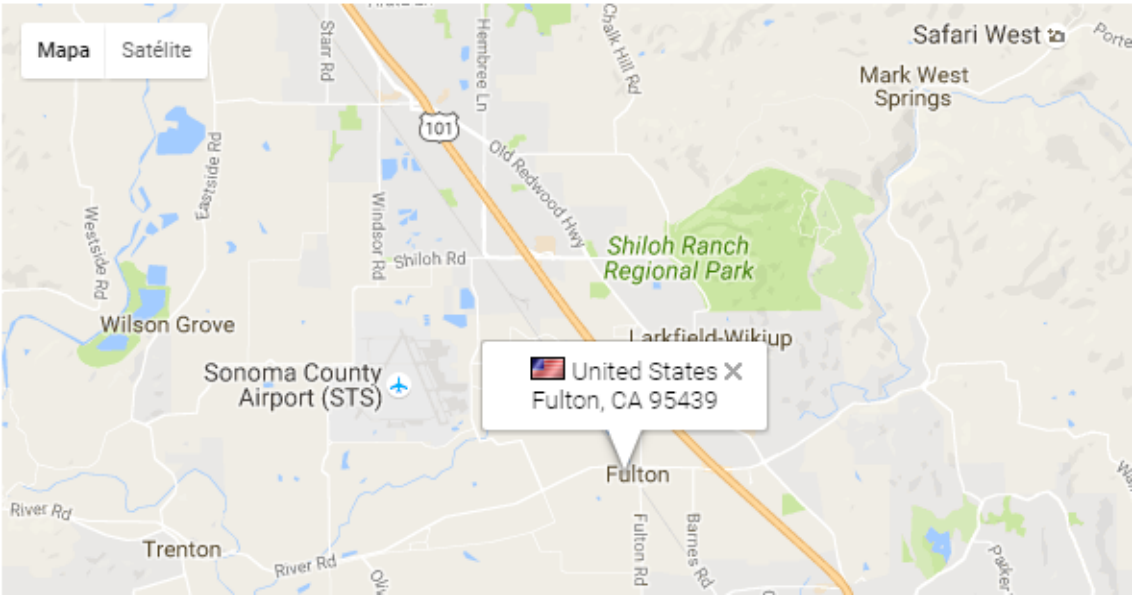



*Figura 4.20. Detalle de información proporcionada sobre una dirección IP por la herramienta whois de CQ counter.*

Checking **69.109.123.185** against **97** known blacklists...
Listed **3** times with **0** timeouts

| | Blacklist | Reason | TTL | ResponseTime |
|---|---|---|---|---|
| LISTED | Protected Sky | 69.109.123.185 was listed Detail | 7200 | 281 |
| LISTED | SORBS DUHL | 69.109.123.185 was listed Detail | 3600 | 63 |
| LISTED | Spamhaus ZEN | 69.109.123.185 was listed Detail | 300 | 78 |

*Figura 4.10. Detalle de reputación de una dirección IP con MXTOOLBOX.*

Por último, ya contemplando todos los puntos anteriores, si se llega a la conclusión de que el evento representa actividad sospechosa, se realiza un alertamiento el cual consiste en un informe con la evidencia y las causas por las cuales se determina alertar, así como las recomendaciones para cada caso (parches, actualizaciones, bloqueo, etc.).

En el diagrama 7 se resume el proceso llevado a cabo para esta actividad.

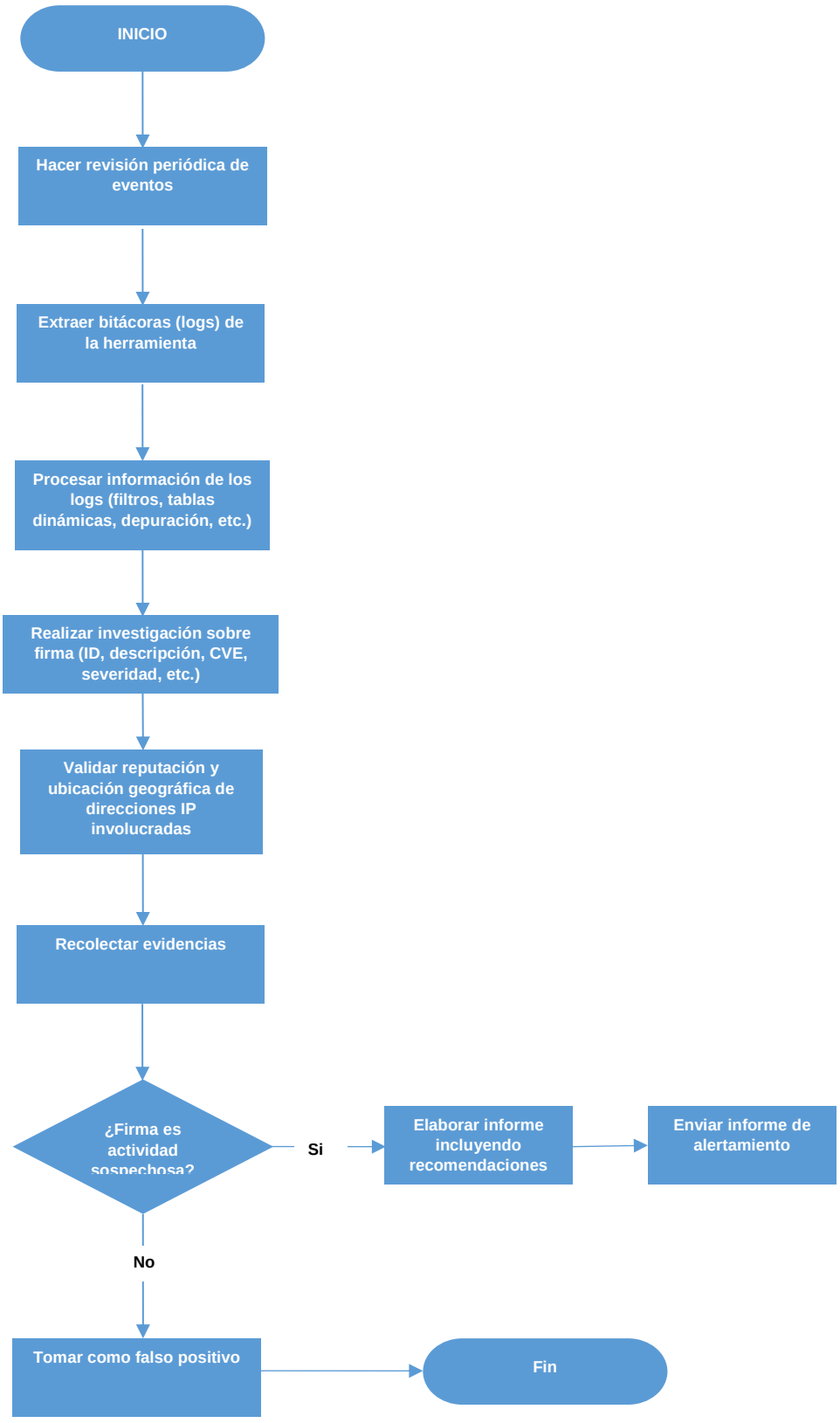





*Diagrama 4.2. Proceso de análisis de firmas en IPS. Elaboración propia.*

De este modo doy por finalizado lo referente al tema de análisis en IPS, el cual representa una herramienta que no puede faltar para la protección de la infraestructura de red de cualquier empresa.

### 4.1.3 Análisis de eventos de AntiDDoS

En el presente tema se explicará el procedimiento empleado en el análisis de eventos en un AntiDDoS, ya que los ataques DDoS representan un peligro potencial cuando se habla de disponibilidad de un servicio, por lo que este tipo de herramientas representan un filtro más, cuando lo que se quiere es mantener los servicios sin interrupciones.

El proceso de análisis es muy similar al visto con anterioridad en un IPS, sin embargo, existen algunos criterios y factores a considerar de diferente manera, debido a la naturaleza que presenta un posible ataque de DDoS.

Al igual que con el análisis en IPS, el primer paso es realizar revisiones periódicas de los eventos detectados por la herramienta y extraer las bitácoras correspondientes para su análisis y así determinar si es necesario realizar un alertamiento o no.

Para este tipo de herramienta en particular se establece con el cliente un umbral permitido de actividad, el cual representaría un comportamiento normal. La determinación de este umbral se realiza durante un periodo de prueba en la etapa de implementación de la herramienta con el fin de llevar a cabo una observación del comportamiento de la red en condiciones normales y en un entorno controlado. Si se rebasa el límite establecido, se debe llevar a cabo el análisis de eventos para determinar si existe comportamiento anómalo y de ser así, se notifica inmediatamente.

Ahora bien, si se va a verificar que el número de eventos se encuentre dentro del umbral acordado, es necesario recurrir a la gráfica que presenta el AntiDDoS, ya que en ella se mostrarán los picos detectados en cada instante de tiempo, así como el número de hits que se presentaron en cada uno de estos picos. Por lo tanto, lo primero que se hace es poner un filtro de tiempo para establecer el periodo a analizar como lo muestra la Figura 4.22; al hacer la consulta, la herramienta arrojará una gráfica parecida a la mostrada en la Figura 4.23. Ahora es posible verificar si el límite de eventos corresponde al umbral permitido, si éste se encuentra dentro del rango establecido, se considera actividad normal, por el contrario, si se identifica que el umbral ha sido rebasado, se procede a un análisis de eventos (no necesariamente implica que se trate de un ataque, sin embargo, es necesario indagar un poco más para ver cómo se comportan las direcciones involucradas).


*Figura 4.11. Búsqueda de eventos en un periodo de tiempo específico. Obtenida del Software AntiDDoS 1.*

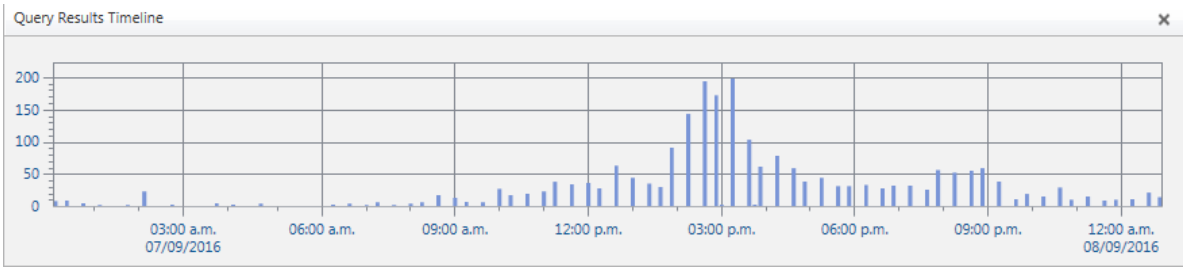



*Figura 4.12. Gráfica de eventos detectados por el AntiDDoS. Obtenida del Software AntiDDoS 1.*

A continuación se explica en qué consiste el proceso de extracción de bitácoras para su posterior análisis.

Al igual que en un IPS, el AntiDDoS cuenta con un menú que permite extraer los eventos detectados en un periodo de tiempo específico. Una vez indicado el periodo de tiempo a analizar en la barra de filtros, se continúa con la extracción de las bitácoras (Figura 4.24). El resultado, al igual que el visto previamente en el IPS, será un archivo en formato .csv que contendrá todos los eventos registrados en el periodo de tiempo especificado; al abrir este archivo en Excel le indicaremos que convierta los datos separados por comas en columnas, de esta manera, la información estará clasificada de un modo más conveniente para su análisis.

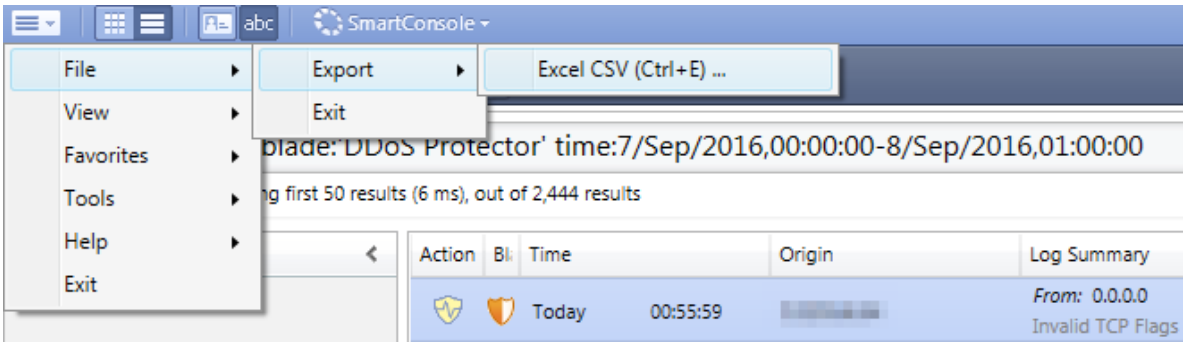



*Figura 4.13. Menú de extracción de bitácoras (logs). Obtenida del Software AntiDDoS 1.*

Entre la información que las bitácoras proporcionan se encuentran nuevamente las direcciones tanto de origen como destino, el protocolo empleado, puertos, etc. (ver Figura 4.25). Pero uno de los datos más importantes a considerar es el campo

Descripción, ya que éste indica la clasificación del posible ataque que la petición pudiera estar generando *(Unrecognized L2 Format (Anomalies), HTTP Page Flood Attack (HttpFlood), etc.)*, es decir, nos indica la razón por la cual el AntiDDoS está capturando el evento. Cabe mencionar que no todos los eventos corresponden a un posible intento de ataque; en ciertas ocasiones la recepción de paquetes malformados o con banderas inválidas propician que el AntiDDoS las detecte como peticiones ilegítimas que pudieran dar paso a un ataque DDoS.

| Time | Description | Action | Attack Name | default_devi | Source | Destination | Severity | Source Port |
|---|---|---|---|---|---|---|---|---|
| 08/Sep/2016,00:55:59 | Invalid TCP Flags (Anomalies) Detected | Detect | Anomalies | <180>Defens | | | Medium | 0 |
| 08/Sep/2016,00:55:59 | Unrecognized L2 Format (Anomalies) Detected | Detect | Anomalies | <180>Defens | | | Medium | 0 |
| 08/Sep/2016,00:55:59 | Invalid TCP Flags (Anomalies) Detected | Detect | Anomalies | <180>Defens | | | Medium | 80 |
| 08/Sep/2016,00:55:59 | Invalid TCP Flags (Anomalies) Detected | Detect | Anomalies | <180>Defens | | | Medium | 80 |
| 08/Sep/2016,00:55:59 | Invalid TCP Flags (Anomalies) Detected | Detect | Anomalies | <180>Defens | | | Medium | 80 |
| 08/Sep/2016,00:55:59 | HTTP Page Flood Attack (HttpFlood) Detected | Detect | HttpFlood | <180>Defens | | | High | 0 |

*Figura 4.14. Logs sin parsear.*

Para comenzar con el siguiente paso, que es propiamente el análisis de los eventos, se utilizarán nuevamente las tablas dinámicas, similar a lo visto previamente con el IPS.

En esta ocasión los datos considerados para la tabla dinámica son la hora y el minuto en que se registró el evento, la descripción del evento, la dirección IP de origen y la de destino. De este modo podremos conocer el instante de tiempo en el que se disparó el pico en cuestión, así como hacia donde fue dirigido el posible ataque. La Figura 4.26 ejemplifica cómo se vería la información mencionada; en ella se aprecia que en el periodo correspondiente a las 17 horas hubo un total de 130000 hits detectados de la siguiente manera: a las 17:08 hrs. se detectaron 1000 hits provenientes de la dirección 1.1.1.1 a la dirección x.x.x.x, a las 17:16 hrs. se detectaron 66000 hits que a su vez se subdividen de la siguiente manera: la dirección 2.2.2.2 hacia la dirección y1.y1.y1.y1 tuvo un total de 13000 hits, la dirección 3.3.3.3 presentó 1000 hits hacia la dirección y2.y2.y2.y2, y así sucesivamente se desglosan las direcciones origen y destino hasta completar el total de 66000. Finalmente, a las 17:36 hrs. se detectaron 63000 hits, de los cuales 43000 provienen de la dirección 4.4.4.4 hacia la dirección z.z.z.z, lo cual representaría un comportamiento sospechoso o anómalo debido a que implica una gran cantidad de hits de un mismo origen a un mismo destino.

| Detalles | Hits |
|---|---|
| **17** | **130** |
| **8** | **1** |
| Unrecognized L2 Format (Anomalies) Detected | 1 |
| **1.1.1.1** | **1** |
| x.x.x.x | 1 |
| **16** | **66** |
| HTTP Page Flood Attack (HttpFlood) Detected | 13 |
| **2.2.2.2** | **13** |
| y1.y1.y1.y1 | 13 |
| Invalid TCP Flags (Anomalies) Detected | 52 |
| **3.3.3.3** | **1** |
| y2.y2.y2.y2 | 1 |
| **36** | **63** |
| Invalid TCP Flags (Anomalies) Detected | 52 |
| **4.4.4.4** | **43** |
| z.z.z.z | 43 |

*Figura 4.15. Eventos analizados.*

Una vez clasificada la información en las tablas dinámicas se procede a la interpretación de los resultados obtenidos, y se reportará aquella actividad que represente características de un ataque DDoS, los casos más comunes serían por ejemplo: actividad persistente por parte de una misma dirección o un segmento de red hacia un mismo activo durante un considerable periodo de tiempo (pueden ser algunas horas o incluso hasta días, sin embargo esta última opción no es aceptable ya que es labor del SOC mitigar estos comportamientos), un número excesivo de hits desde un mismo origen (o desde varios si se trata de un DDoS) hacia un activo en un corto lapso de tiempo, etc.

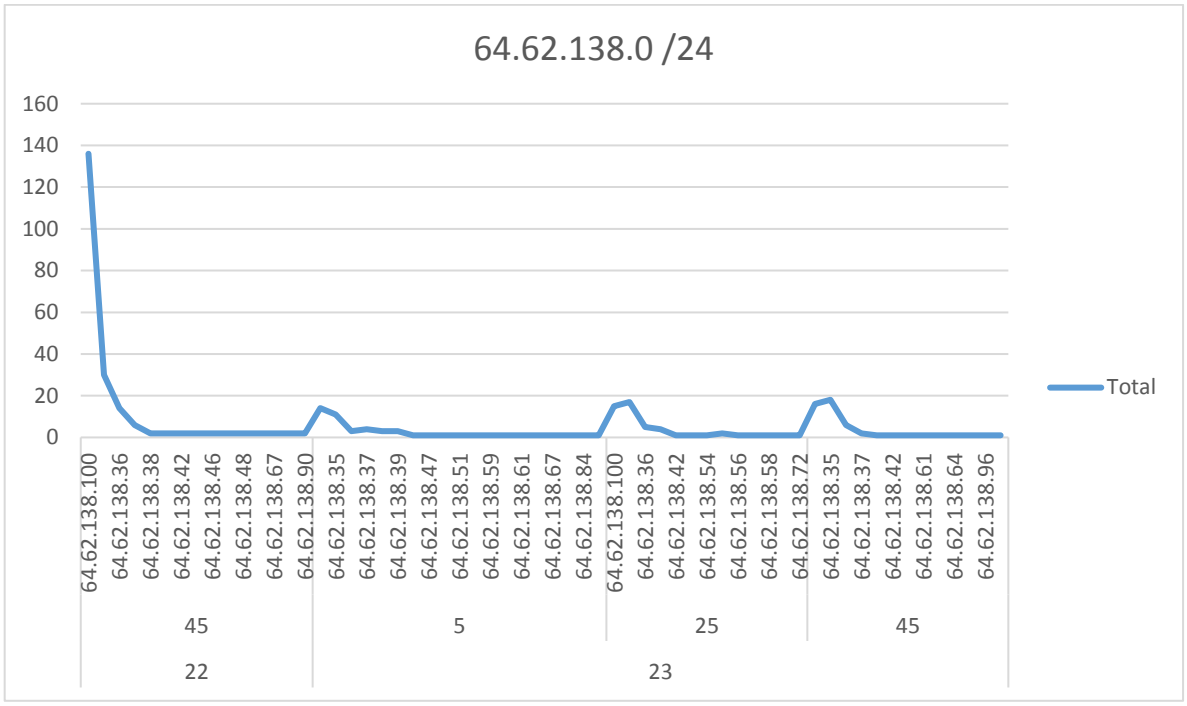
A continuación se muestra cómo se vería uno de los comportamientos mencionados previamente, para este caso particular se ilustra un segmento de red persistente (64.62.138.0 /24) hacia distintos activos del cliente, por lo que es necesario realizar un rastreo (revisión) de eventos en un lapso de 1 hora (entre las 22 y 23 hrs.). Lo que se quiere determinar en este caso es la actividad registrada por el segmento mencionado, por lo cual sólo nos enfocaremos en la dirección de origen y el número de eventos que generó.

En la tabla 4.2 se ejemplifica un análisis por hora y minuto de actividad en un antiDDoS.

| Hora de detección | Hits |
|---|---|
| **22** | **208** |
| **45** | **208** |
| 64.62.138.100 | 136 |
| 64.62.138.35 | 30 |
| 64.62.138.36 | 14 |
| 64.62.138.37 | 6 |
| 64.62.138.38 | 2 |
| 64.62.138.41 | 2 |
| 64.62.138.42 | 2 |
| 64.62.138.43 | 2 |
| 64.62.138.46 | 2 |
| 64.62.138.47 | 2 |
| 64.62.138.48 | 2 |
| 64.62.138.63 | 2 |
| 64.62.138.67 | 2 |
| 64.62.138.68 | 2 |
| 64.62.138.90 | 2 |
| **23** | **153** |
| **5** | **51** |
| 64.62.138.100 | 14 |
| 64.62.138.35 | 11 |
| 64.62.138.36 | 3 |
| 64.62.138.37 | 4 |
| 64.62.138.38 | 3 |
| 64.62.138.39 | 3 |
| 64.62.138.46 | 1 |
| 64.62.138.47 | 1 |
| 64.62.138.50 | 1 |
| 64.62.138.51 | 1 |
| 64.62.138.58 | 1 |
| 64.62.138.59 | 1 |
| 64.62.138.60 | 1 |
| 64.62.138.61 | 1 |
| 64.62.138.62 | 1 |
| 64.62.138.67 | 1 |
| 64.62.138.78 | 1 |
| 64.62.138.84 | 1 |
| 64.62.138.85 | 1 |
| **25** | **51** |
| 64.62.138.100 | 15 |
| 64.62.138.35 | 17 |
| 64.62.138.36 | 5 |
| 64.62.138.37 | 4 |
| 64.62.138.42 | 1 |
| 64.62.138.49 | 1 |
| 64.62.138.54 | 1 |
| 64.62.138.55 | 2 |
| 64.62.138.56 | 1 |
| 64.62.138.57 | 1 |
| 64.62.138.58 | 1 |
| 64.62.138.71 | 1 |
| 64.62.138.72 | 1 |
| **45** | **51** |
| 64.62.138.100 | 16 |
| 64.62.138.35 | 18 |
| 64.62.138.36 | 6 |
| 64.62.138.37 | 2 |
| 64.62.138.38 | 1 |
| 64.62.138.42 | 1 |
| 64.62.138.43 | 1 |
| 64.62.138.61 | 1 |
| 64.62.138.63 | 1 |
| 64.62.138.64 | 1 |
| 64.62.138.68 | 1 |
| 64.62.138.96 | 1 |
| 64.62.138.97 | 1 |
| **Total general** | **361** |

*Tabla 4.2. Ejemplo de análisis en AntiDDoS. Elaboración propia.*

Es posible hacer ahora una gráfica (gráfica 1) para poder apreciar mejor el patrón que ha generado el segmento investigado, obteniendo los resultados siguientes.




*Gráfica 4.1. Patrón de actividad en el AntiDDoS. Elaboración propia.*

Por último, una vez interpretada la información, sólo resta verificar el origen de la misma, con lo cual contaremos con un plus de información antes de hacer un diagnóstico final. Para ello nos apoyaremos también de las ya mencionadas listas negras, así como de la geolocalización (un excesivo número de hits provenientes de Noruega o Islandia podrían ser indicador de que está sucediendo algo extraño). Con esta última etapa el análisis ha concluido y ya se puede canalizar el informe de actividad sospechosa con sus respectivas evidencias y recomendaciones con el equipo de administración, para que éste realice las acciones de mitigación pertinentes.

El diagrama 8 muestra el proceso correspondiente a esta actividad.

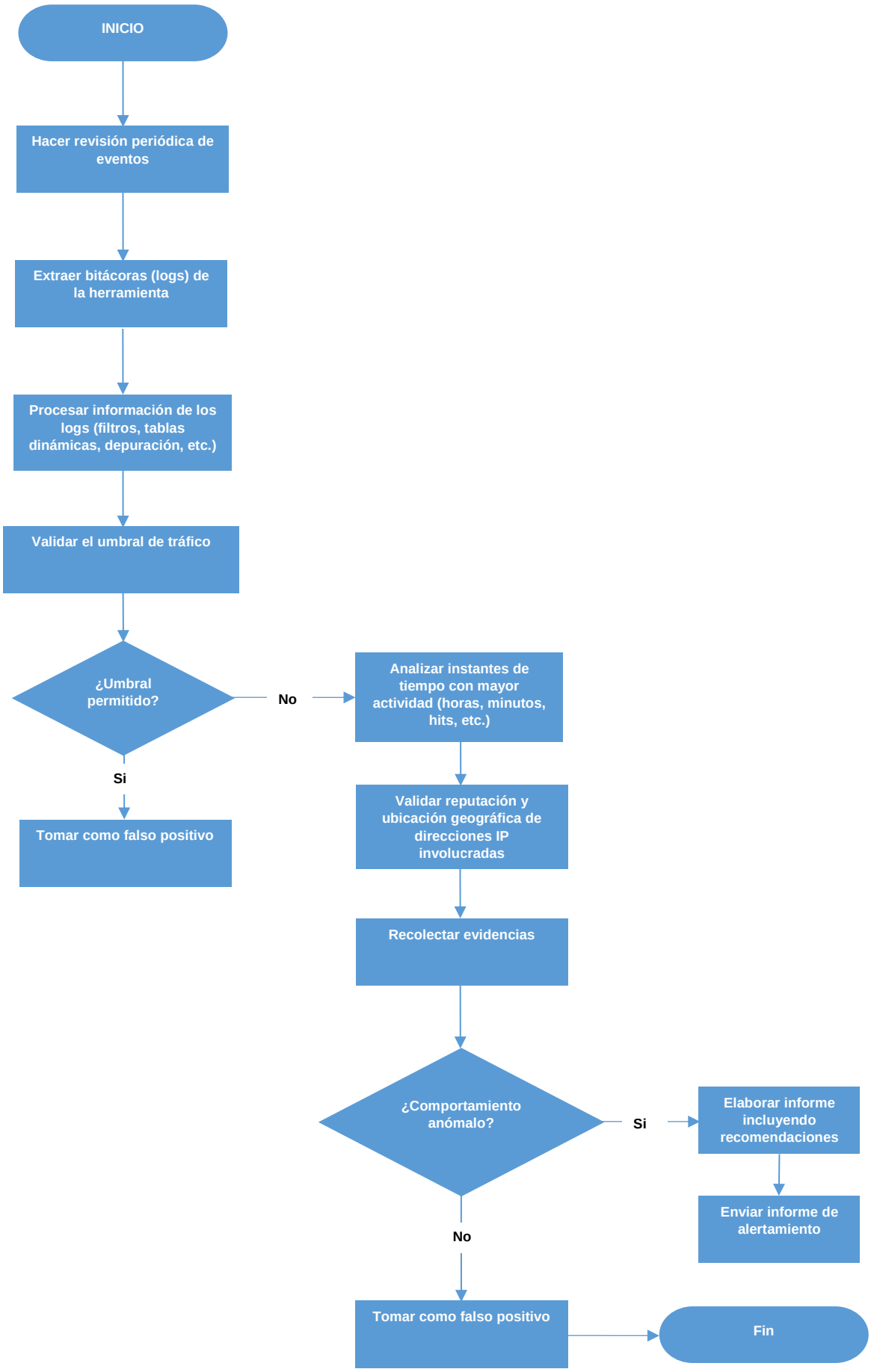





*Diagrama 4.3. Proceso de análisis de eventos en AntiDDoS. Elaboración propia.*

### 4.1.4 Documentación de tickets

Dentro de las principales razones por las cuales un SOC debe contar con un sistema de gestión de tickets se encuentran las siguientes: la primera de ellas es poder tener acceso a documentación acerca de todos los incidentes que se presenten, así como la forma en que se solucionaron los mismos (base de conocimiento), de este modo es posible consultar un registro cada vez que sea necesario en caso de que se presente una problemática similar a una que se haya resuelto antes, ahorrando tiempo en la resolución y respuesta de ésta. El segundo caso corresponde a contar con un control del cumplimiento de los acuerdos de nivel de servicio y así poder desarrollar un proceso de mejora continua en la atención al cliente.

De ambos casos hablaré a detalle a continuación.

El sistema de gestión de tickets, como su nombre lo indica, permite tener control y acceso a los registros de los incidentes que día con día se atienden en el SOC. Por cada incidente o requerimiento solicitado por el cliente se debe generar un ticket en el que se irá recolectando la información referente al progreso en la resolución de dicho incidente hasta que se proporcione una respuesta definitiva y con esta, el cierre del ticket. La información contenida en cada ticket puede incluir notas respecto a las acciones que se han tomado hasta el momento, pruebas realizadas, evidencias de las pruebas, diagnósticos, etc. Finalmente, una vez resuelto el problema en cuestión se deberán anexar notas de cierre de ticket en donde se especifique la solución, así como la razón por la cual el incidente se considera como atendido.

El contar con un sistema de tickets no solo ayuda a los analistas del SOC a solucionar problemas a nivel operacional, sino que también permite realizar una autoevaluación en cuanto a la atención que se le está dando al cliente y la prueba de ello es el tiempo que toma el proporcionarle una solución satisfactoria. Es aquí donde se introduce el concepto de “Acuerdo de Nivel de Servicio” o SLA por sus siglas en inglés (*Service Level Agreement*), el cual es un convenio escrito que contempla las condiciones y compromisos que el SOC tiene con cada uno de sus clientes (Polanco, 2010); los SLA se encuentran definidos directamente en el contrato que el cliente firma con el SOC y contemplan los tiempos establecidos para la atención de incidentes y su resolución (de este tema en particular hablaré más adelante en el tema correspondiente a reportes mensuales).

Existen diferentes sistemas de tickets a elegir, pero todos ellos están encaminados a la misma función: generar una línea de comunicación en este caso entre SOC y el cliente, de tal manera que el mismo cliente sea capaz de consultar el avance en la solución de sus problemáticas y pueda mantenerse informado de lo acontecido hasta que la solución le sea proporcionada.

La Figura 4.27 muestra los datos que se pueden almacenar en un gestor de tickets, por políticas de confidencialidad de la empresa, nombraremos al gestor de tickets utilizado como TicketServer.

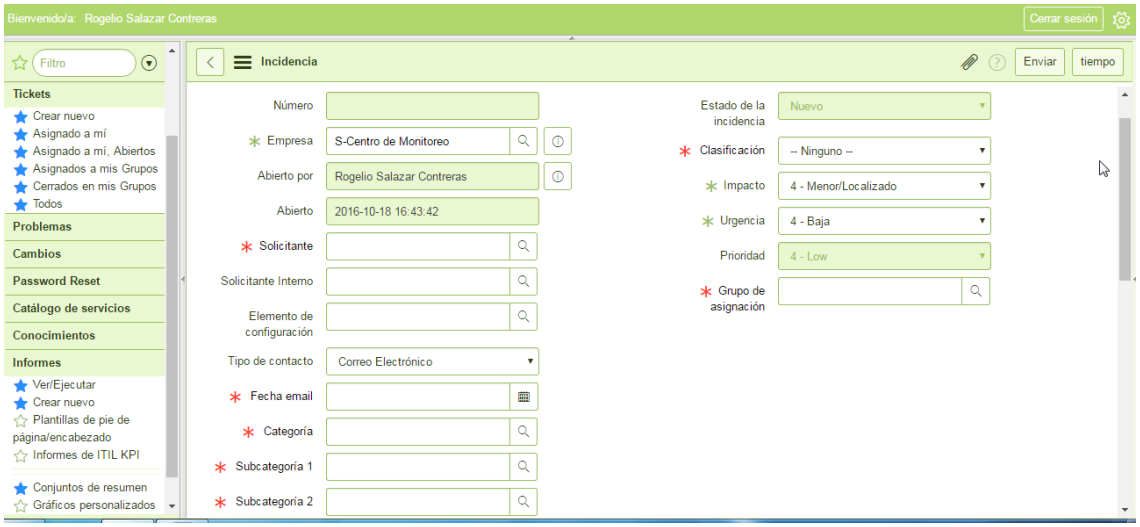



*Figura 4.16. Creación de un ticket en el gestor TicketServer.*

En el diagrama 9 se ilustra el proceso que conlleva la documentación de un ticket.

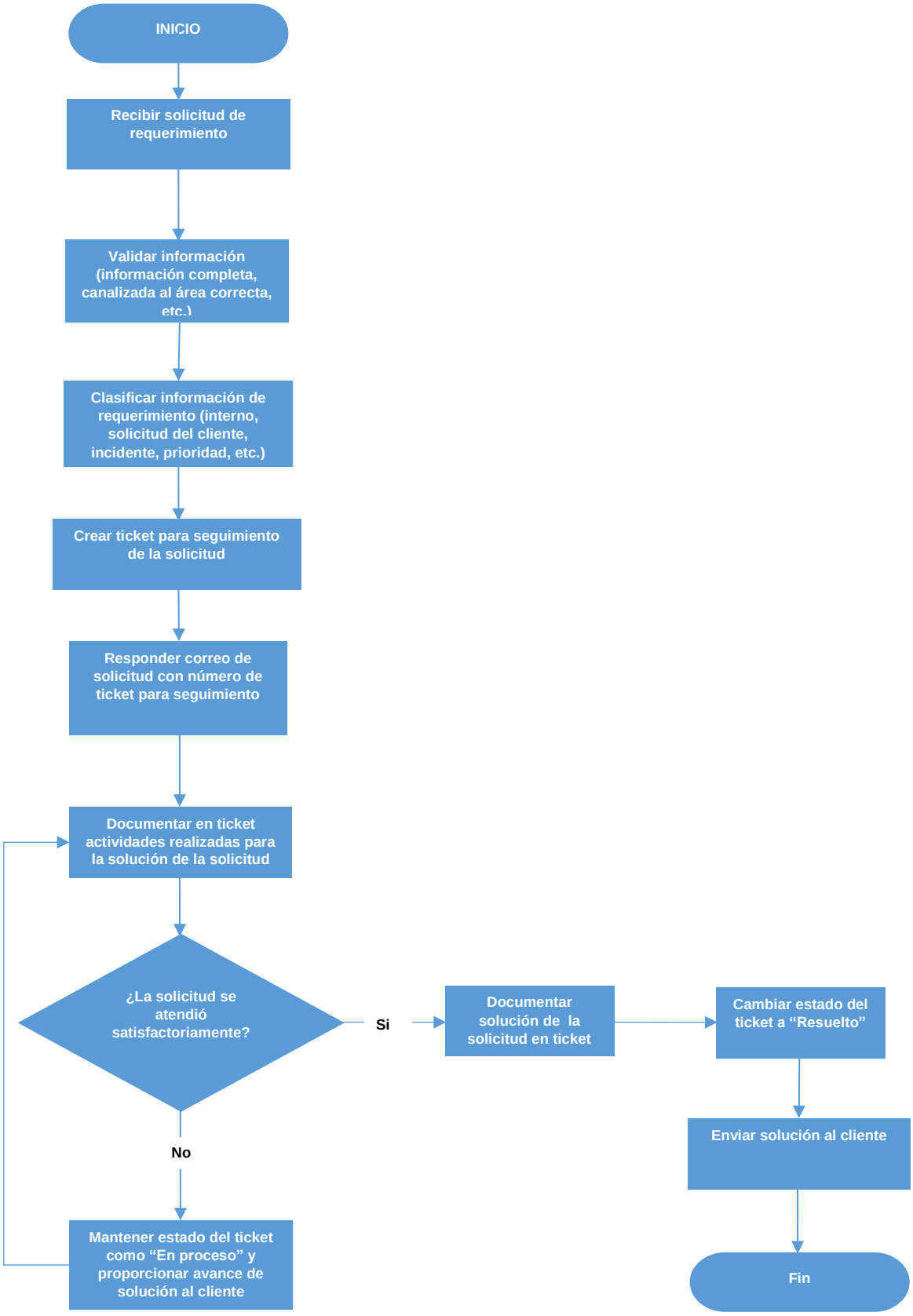



*Diagrama 4.4. Proceso de documentación de tickets. Elaboración propia.*

### 4.1.5 Registro de rendimiento de herramientas de seguridad

Hemos comentado previamente que las herramientas de seguridad monitoreadas y administradas por el SOC deben permanecer en óptimas condiciones para que no existan problemas de indisponibilidad, es por esta razón que se considera de suma importancia llevar un control del rendimiento que éstas desempeñan día con día para que no se vean interrumpidas sus funciones. Los activos a monitorear en este registro son uso de CPU y uso de memoria, dependiendo de las especificaciones proporcionadas por el cliente, esta revisión puede formar parte de la lista de chequeo general, o puede realizarse independientemente, en “horas clave” cuando se sabe que hay mayor demanda de recursos debido a alguna actividad programada; de estas dos, la primera es la opción más recomendada.

Generalmente la información referente al uso de recursos la localizamos en el *dashboard* de estado de cada herramienta y se expresa en porcentaje de utilización (Figuras 4.28 y 4.29).

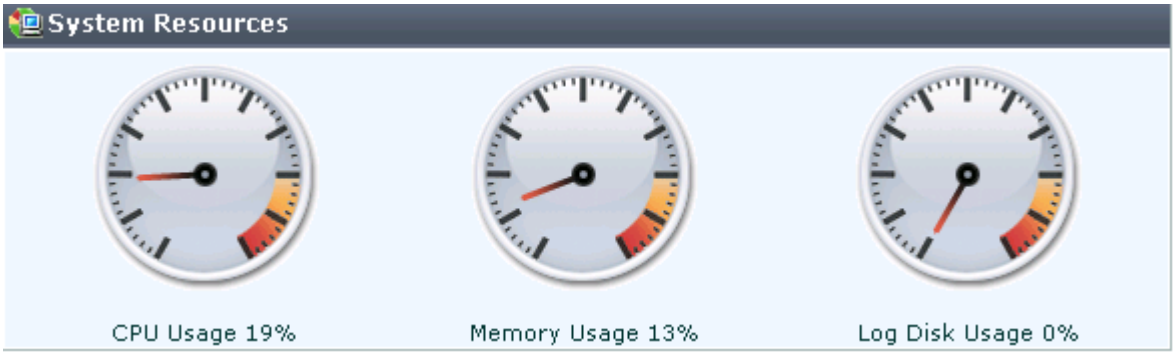



*Figura 4.17. Detalle del rendimiento de un IPS. Obtenida del Software IPS 3.*

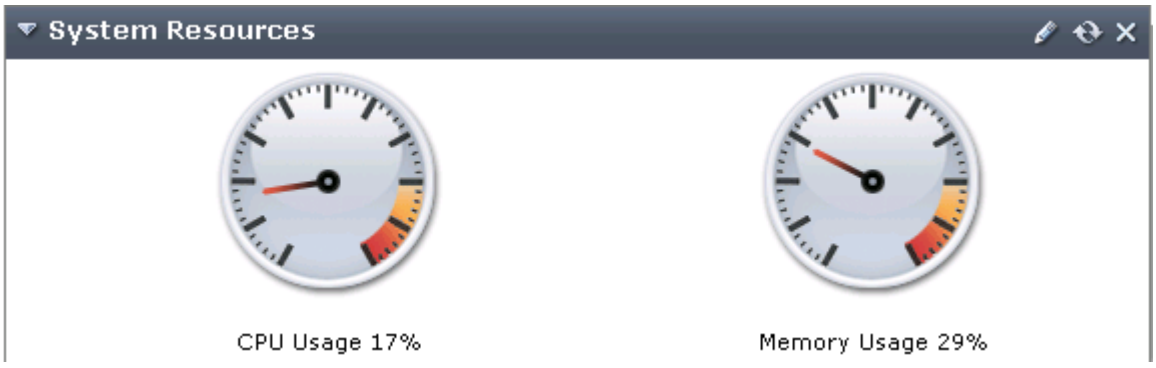



*Figura 4.18. Detalle del rendimiento de un WAF. Obtenida del Software WAF 1.*

Cabe señalar que es posible realizar el chequeo individual herramienta por herramienta, lo cual representa una opción efectiva pero un tanto incómoda ya que hay que validar una por una, lo cual puede resultar tedioso, o está la otra opción y es que existen herramientas especiales de monitoreo de disponibilidad, que centralizan los dispositivos y se encargan de hacer el chequeo por nosotros; de este modo basta con posicionarse sobre el dispositivo a revisar para obtener las estadísticas requeridas como se muestra en la Figura 4.30, lo cual ahorra bastante tiempo, ayudando a optimizar esta labor. Otro aspecto destacable de estas herramientas de monitoreo de disponibilidad es la capacidad de generar reportes estadísticos en los cuales se muestra el registro del uso de recursos tanto de manera tabular, como de manera gráfica, al final del mes se deben entregar los números y en este caso esta funcionalidad resulta bastante útil.

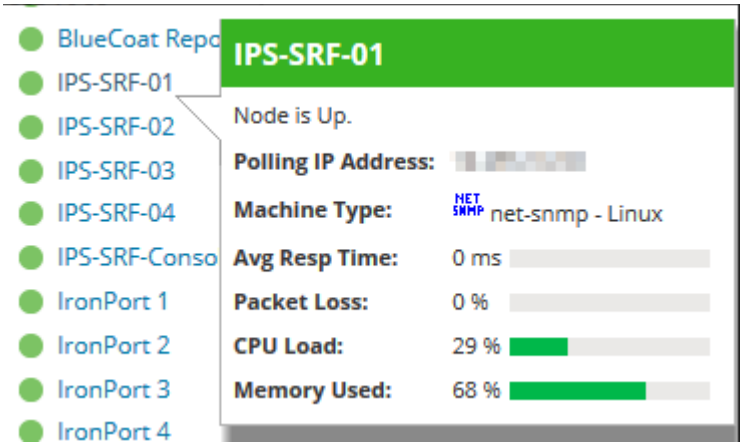



*Figura 4.30. Detalle de rendimiento de un IPS mediante una herramienta de monitoreo. Obtenida del Software Monitor 1.*

La tabla 4.3 ejemplifica cómo se presenta el registro de rendimiento de una herramienta al final del mes, así como sus respectivas gráficas (Figura 4.31 y Figura 4.32).

| No. Registro | Uso de CPU % | Uso de memoria % | Fecha | Hora |
|---|---|---|---|---|
| **1** | 29.00% | 8.00% | 01-ago-16 | 12:00 a.m. |
| **2** | 21.00% | 9.00% | 02-ago-16 | 12:00 a.m. |
| **3** | 19.00% | 9.00% | 03-ago-16 | 12:00 a.m. |
| **4** | 13.00% | 9.00% | 04-ago-16 | 12:00 a.m. |
| **5** | 8.00% | 9.00% | 05-ago-16 | 12:00 a.m. |
| **6** | 10.00% | 9.00% | 06-ago-16 | 12:00 a.m. |
| **7** | 23.00% | 10.00% | 07-ago-16 | 12:00 a.m. |
| **8** | 20.00% | 13.00% | 08-ago-16 | 12:00 a.m. |

| No. Registro | Uso de CPU % | Uso de memoria % | Fecha | Hora |
|---|---|---|---|---|
| **9** | 27.00% | 14.00% | 09-ago-16 | 12:00 a.m. |
| **10** | 24.00% | 14.00% | 10-ago-16 | 12:00 a.m. |
| **11** | 12.00% | 15.00% | 11-ago-16 | 12:00 a.m. |
| **12** | 9.00% | 15.00% | 12-ago-16 | 12:00 a.m. |
| **13** | 9.00% | 15.00% | 13-ago-16 | 12:00 a.m. |
| **14** | 29.00% | 15.00% | 14-ago-16 | 12:00 a.m. |
| **15** | 17.00% | 15.00% | 15-ago-16 | 12:00 a.m. |
| **16** | 26.00% | 16.00% | 16-ago-16 | 12:00 a.m. |
| **17** | 21.00% | 16.00% | 17-ago-16 | 12:00 a.m. |
| **18** | 8.20% | 16.00% | 18-ago-16 | 12:00 a.m. |
| **19** | 18.79% | 16.00% | 19-ago-16 | 12:00 a.m. |
| **20** | 8.96% | 16.00% | 20-ago-16 | 12:00 a.m. |
| **21** | 7.25% | 16.00% | 21-ago-16 | 12:00 a.m. |
| **22** | 19.79% | 16.00% | 22-ago-16 | 12:00 a.m. |
| **23** | 20.21% | 16.42% | 23-ago-16 | 12:00 a.m. |
| **24** | 19.46% | 16.63% | 24-ago-16 | 12:00 a.m. |
| **25** | 22.71% | 17.00% | 25-ago-16 | 12:00 a.m. |
| **26** | 18.21% | 17.00% | 26-ago-16 | 12:00 a.m. |
| **27** | 11.40% | 17.00% | 27-ago-16 | 12:00 a.m. |
| **28** | 6.79% | 17.00% | 28-ago-16 | 12:00 a.m. |
| **29** | 17.74% | 17.77% | 29-ago-16 | 12:00 a.m. |
| **30** | 20.42% | 17.68% | 30-ago-16 | 12:00 a.m. |
| **31** | 19.99% | 18.00% | 31-ago-16 | 12:00 a.m. |
| **Promedio** | **17.32%** | **14.37%** | | |

*Tabla 4.3. Tabla de registro de rendimiento mensual. Elaboración propia.*

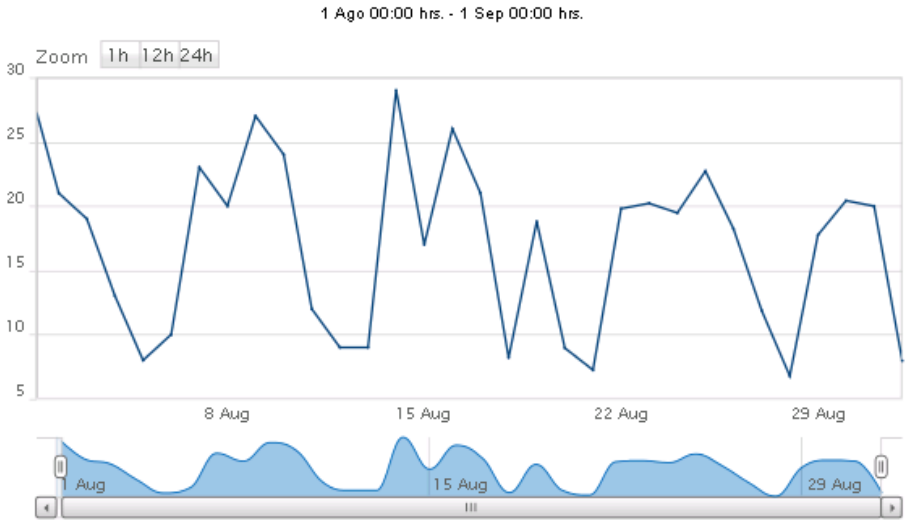



*Figura 4.19. Rendimiento mensual de CPU. Obtenida del Software WAF 1.*

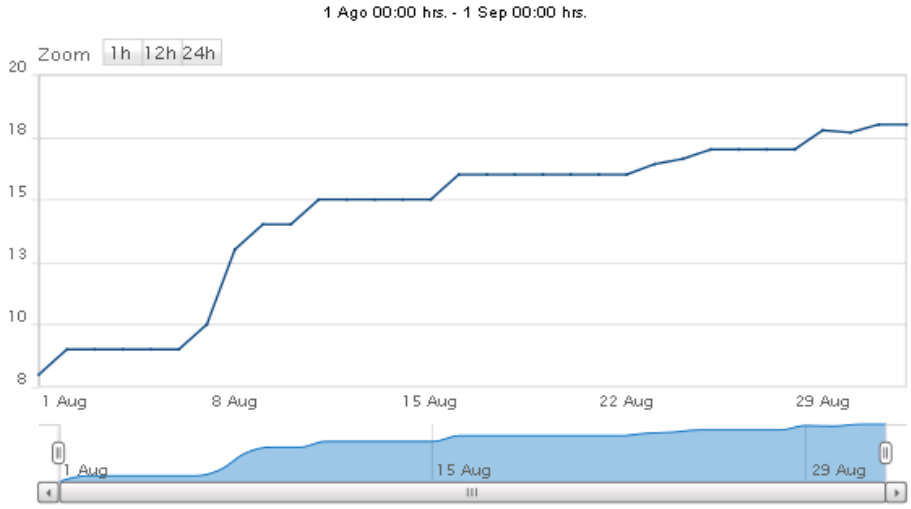



*Figura 4.20. Rendimiento mensual de memoria. Obtenida del Software WAF 1.*

Adicionalmente, en el diagrama 10 se muestra el proceso correspondiente a esta actividad.

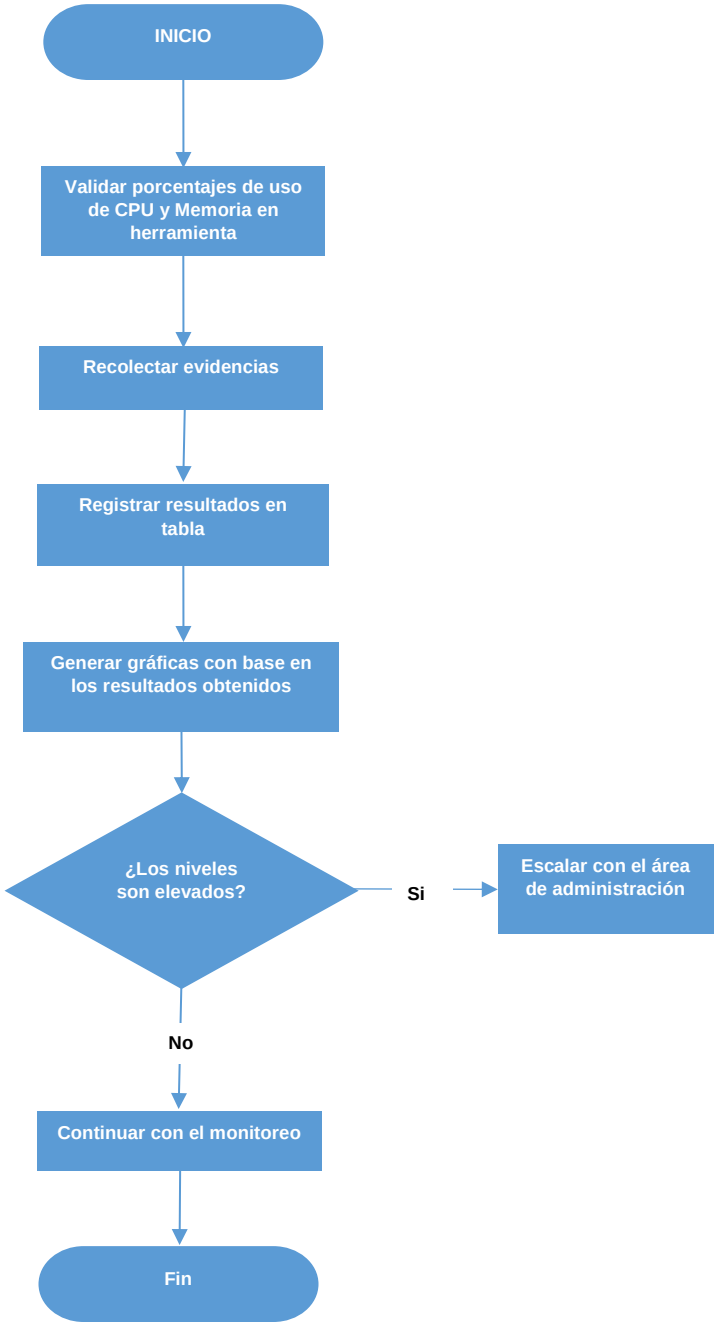



*Diagrama 4.5. Proceso de registro de rendimiento. Elaboración propia.*

### 4.1.6 Reportes mensuales

Finalmente, en este último tema describiré la manera en que se realiza el reporteo.

Este servicio brindado por el SOC es importante debido a que es en este punto donde se entrega un resumen de todo lo acontecido con las herramientas durante el mes, además se evalúa el desempeño que se ha tenido por parte del SOC. También es aquí donde realmente se ven reflejados los resultados de todos los aspectos pactados en los SLA.

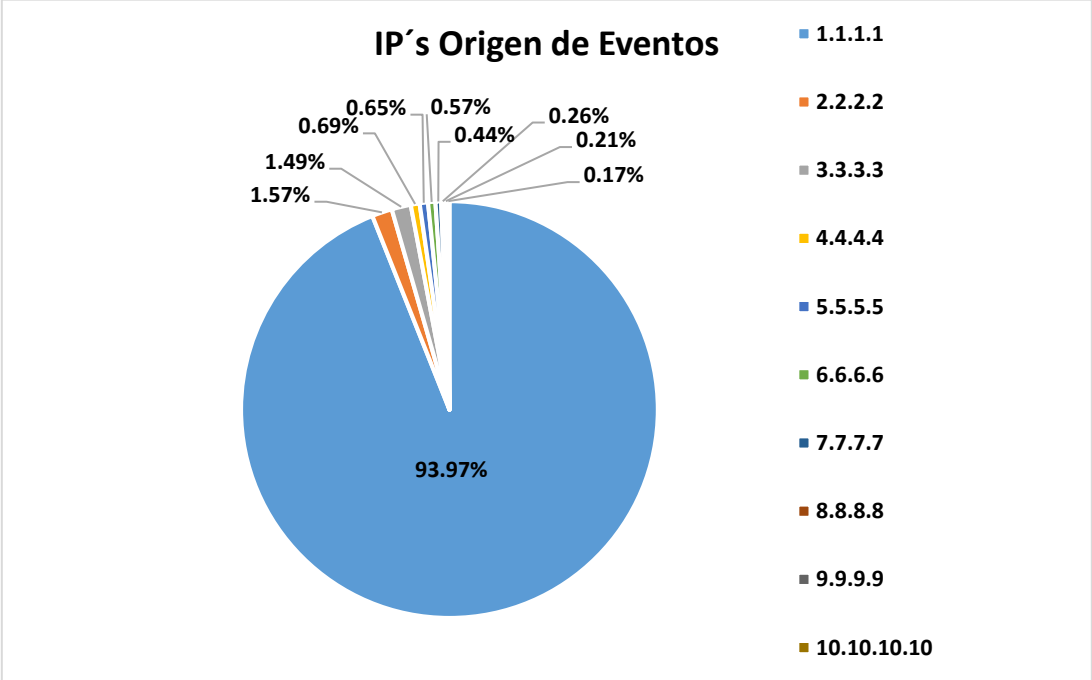
Comenzaré por comentar que el reporteo se realiza por cada una de las herramientas con las que cuente el cliente, y en cada reporte realizado se contemplan todos los rubros estipulados en los SLA como pueden ser: disponibilidad, informe de actividad sospechosa, rendimiento, control de cambios, etc. En un reporte mensual se presenta la información de la manera más completa y clara posible para que el cliente pueda realizar su propia evaluación del servicio recibido.

A pesar de que en el reporte mensual se registran todos los aspectos referentes a la actividad de cada herramienta, la sección correspondiente a la actividad sospechosa registrada y alertada durante el mes es la que más peso tiene dentro del reporte. Esto es de imaginarse ya que para ello es necesario realizar el resumen de todos los incidentes detectados durante el mes y en dicha sección se contemplan aspectos como los siguientes: Top 10 de direcciones de origen, Top 10 de direcciones de destino, Top 10 de firmas o eventos más recurrentes, Top 10 de países atacantes, así como un Top 10 de horas en las que se registró mayor actividad. Dependiendo las especificaciones del cliente es posible que existan más rubros a reportar, sin embargo, son los mencionados los que no pueden faltar en cada reporte.

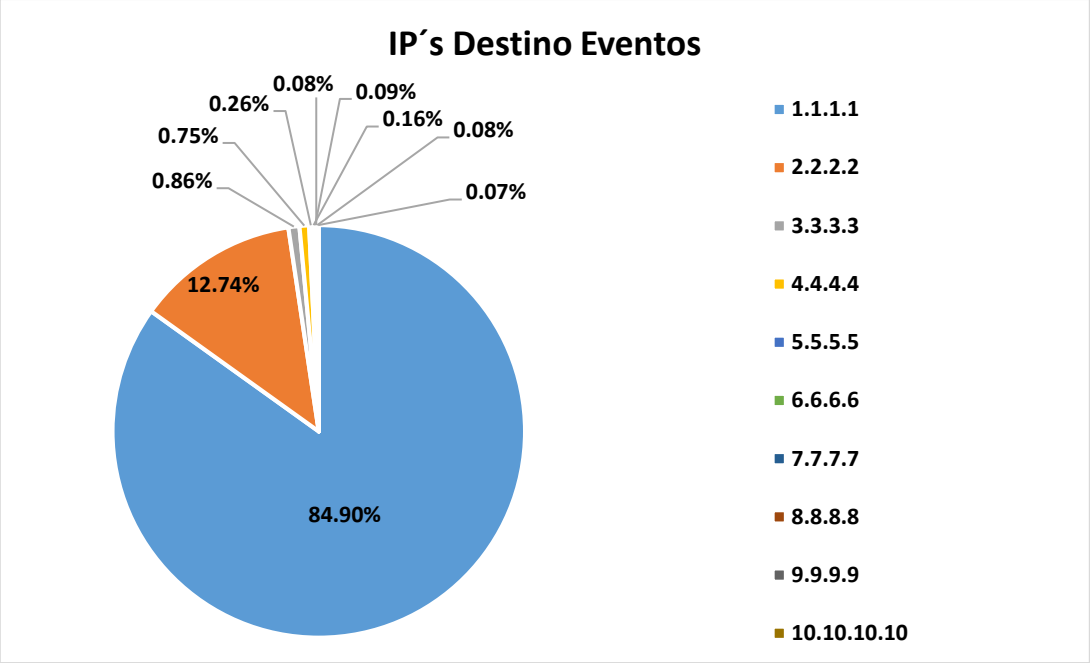
Pero ¿Qué hace a estos aspectos tan útiles y tan importantes como para que no se pasen por alto mes con mes? La respuesta es simple, con ellos es posible establecer tendencias y detectar patrones de comportamiento, lo cual resulta de mucha utilidad en la clasificación de los eventos y a la hora de establecer cuales pueden representar de falsos positivos y proceder de una manera adecuada como puede ser una integración a listas blancas o incluso realizar un bloqueo por área geográfica o segmento de red según sea el caso.

En las gráficas 4.2 a la 4.5 se ejemplifica la manera en que se presentan estás estadísticas al cliente mediante el reporte mensual.


*Gráfica 4.2. Eventos detectados en un mes. Elaboración propia.*




*Gráfica 4.3. Top 10 de direcciones IP de origen detectadas en un mes. Elaboración propia.*




*Gráfica 4.4. Top 10 de direcciones IP de destino detectadas en un mes. Elaboración propia.*


*Gráfica 4.5. Top 10 de horas con mayor actividad durante un mes. Elaboración propia.*

Para poder concluir con este tema es necesario hablar también de la sección que le interesa directamente al cliente y es aquella donde se hace mención del

cumplimiento de los SLA. Por ejemplo, si en el informe se entrega la estadística de que se atendieron *n* número de incidentes, debe existir en nuestro sistema gestor de tickets *n* número de evidencias que sustenten las respectivas soluciones, o en su defecto el estado en el que se encuentran las mismas. El mismo gestor de tickets proporciona el tiempo de atención que se registró para cada incidente desde que se dio de alta hasta que se resolvió y son justamente estos tiempos los que el cliente toma en cuenta para su evaluación final. Para este caso, de no cumplir con las condiciones establecidas se puede llegar incluso a penalizaciones las cuales también se encuentran descritas en los SLA.

La tabla 4.4 es un ejemplo de cómo se registran los incidentes así como su respectiva sustentación basada a en el sistema de tickets.

| Fecha | Descripción | Ticket | Estado | Tiempo de atención |
|---|---|---|---|---|
| **08/04/2016** | Su apoyo para validar si las siguientes direcciones IP se encuentran en listas negras de WAF y AntiDDoS:<br>1.1.1.1<br>2.2.2.2 | TCK1111111 | Resuelto | 20 minutos |
| **14/04/2016** | Se solicita integrar el certificado SSL adjunto en el correo al portal http://portalsolicitado.com a la herramienta WAF. | TCK2222222 | Resuelto | 2 horas y 9 minutos |
| **16/04/2016** | Se solicita realizar el bloqueo de las siguientes direcciones en la herramienta WAF.<br>1.1.1.1<br>2.2.2.2 | TCK3333333 | Resuelto | 40 minutos |
| **20/04/2016** | Se envía información del comportamiento anómalo siguiente:<br>Fecha y hora de caída del Portal<br>20/04/2016 21:43 Hrs.<br>Activo Afectado<br>http://portalafectado.com | TCK4444444 | Resuelto | 8 minutos |

*Tabla 4.4. Ejemplo de tabla con tickets de incidentes atendidos durante un mes. Elaboración propia.*

Como podemos notar, el reporte mensual refleja el trabajo de todo el equipo, por lo que es de mucha importancia darle su lugar a cada detalle en cada proceso así como tener una buena comunicación entre las áreas involucradas, mientras más atención se tenga en los detalles, las probabilidades del éxito del SOC son mayores.

En el diagrama 4.6 se resume el proceso a realizar para el reporteo.

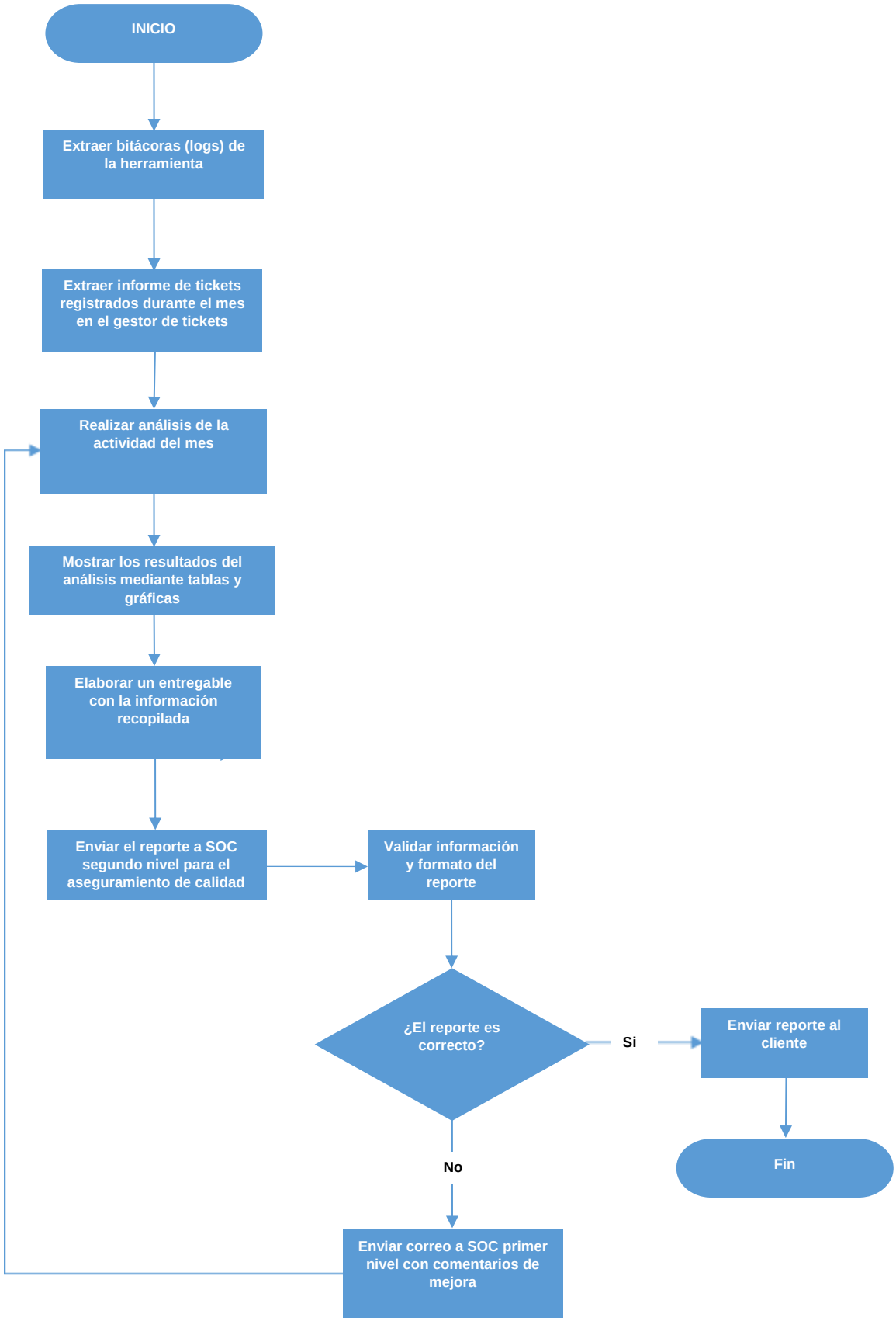



*Diagrama 4.6. Proceso de reporteo. Elaboración propia.*

# Conclusiones

Los riesgos y amenazas informáticas son una constante que siempre estará presente cada vez que se hable de un sistema computacional. Tomando en cuenta que en la actualidad todas las empresas importantes cuentan con estos sistemas, esto implica que se encuentran expuestos a ser vulnerados en cualquier momento y es por ello que la seguridad de la información juega un rol fundamental dentro de las grandes organizaciones. Dado lo anterior, es conveniente que las organizaciones se valgan de profesionales en seguridad de la información que asuman la tarea de disminuir estos riesgos empleando una serie de procesos y mecanismos especializados en detección y mitigación de amenazas. Estos profesionales pueden ejercer sus labores ya sea formando parte de la misma institución o a través de un outsourcing de seguridad que se encargue de proporcionarle al cliente los servicios adecuados para sus necesidades en cuanto a protección de sus activos.

En la actualidad cada vez más organizaciones se acercan a los proveedores de seguridad con la finalidad de contratar los servicios proporcionados por los SOC, lo cual nos habla de una concientización por parte de las mismas respecto a los

riesgos existentes con el manejo de internet y el aumento de amenazas que pueden comprometer la integridad, confidencialidad y disponibilidad de sus activos y su información.

La importancia de un Centro de Operaciones de Seguridad radica en su capacidad de detección y contención de incidentes, así como sus tiempos de respuesta para la atención de los mismos. El cumplimiento de estos objetivos se logra en gran medida gracias a la labor de monitoreo realizada por su personal de operación ya que de ellos depende la oportuna detección de actividad sospechosa que podría derivar en un incidente de seguridad, así mismo el personal de administración de tecnologías de seguridad dentro del SOC también cumple un papel muy importante en el proceso de contención de incidentes ya que son los encargados de aplicar las medidas correctivas para el incidente en cuestión.

Los ejemplos mostrados a lo largo del presente reporte de actividades proporcionan al lector una visión general de cómo se llevan a cabo los procesos de operación dentro de un SOC y cómo estas acciones contribuyen al cumplimiento de los Acuerdos de Nivel de Servicio establecidos con sus clientes. En estos ejemplos se mostró paso por paso la manera en que se realizan las distintas actividades de monitoreo y análisis.

En otro orden de ideas, concluyo también que durante nuestro paso como estudiantes de la Facultad de Ingeniería adquirimos una serie de conocimientos técnicos los cuales representan la base de nuestra formación profesional, tanto desde el punto de vista teórico como práctico; éstos abarcan desde antecedentes de la computación hasta la aplicación de diversas técnicas y metodologías para la resolución de problemas reales. Sin embargo, no es sino hasta cuando nos encontramos en el campo laboral, que realmente podemos observar y comprobar la importancia de los temas tratados a lo largo de nuestra carrera como parte de un todo en donde cada pieza se relaciona.

Es responsabilidad del profesionista acrecentar y ampliar los conocimientos adquiridos para lograr su mejor desempeño en el campo laboral, teniendo en cuenta que el aprendizaje es un proceso que no termina y que le ayudará a lograr una mejora continua en sus aptitudes y habilidades.

Concretamente hablando del área de redes y seguridad, puedo citar ciertos puntos que en mi particular experiencia he tenido la posibilidad de retomar y llevar a la práctica, ya que mis actividades dentro del SOC así lo requieren.

En primer lugar, ya en el ejercicio de la profesión de ingeniero en computación dentro de un SOC, he podido fortalecer el entendimiento de los principios básicos de la seguridad de la información, así como verlos aplicados en casos reales a través de las diferentes herramientas monitoreadas y las actividades realizadas día con día. Tal es el caso de la integridad de la información, la cual relaciono con el monitoreo de herramientas como es el DAM, con el cual es posible conocer qué

modificaciones se han realizado en una base de datos y el monitoreo de SIEM el cual concentra la actividad de distintos sistemas y es posible conocer en qué momento se realizó un cambio en las consideraciones definidas por los clientes, como pueden ser algún cambio de contraseña o de privilegios para cierto usuario, etc. Por otro lado la disponibilidad la asocio con actividades como la validación del estado de salud de las herramientas, así como la revisión de equipos mediante herramientas de monitoreo de disponibilidad, en las cuales podemos consultar el estado de la comunicación con los activos; también otro punto que toco respecto a la disponibilidad es el almacenamiento de respaldos de configuración y de información en diferentes ubicaciones con el fin de garantizar que estos datos estarán disponibles cada vez que el cliente los requiera. Por último, la confidencialidad la asocio con actividades como lo son el monitoreo de eventos mediante herramientas como DLP, con la cual es posible validar la fuga de información de carácter confidencial para el cliente, revisando su contenido, identificando qué usuario extrae información sensible, su ubicación, así como la fecha y hora exactas de la extracción. Del mismo modo en este rubro menciono el uso de herramientas de cifrado de información, mediante las cuales podemos compartir documentos y mensajes con la certeza de que sólo serán vistos por las personas indicadas, ya que deberán contar con la respectiva llave de descifrado.

Otro aspecto importante a mencionar con relación a la experiencia adquirida dentro del campo laboral es el poder conocer y familiarizarme con ciertas normativas y estándares que en mi caso particular no tuve oportunidad de desarrollar durante mi etapa como estudiante y que representan gran importancia en el área de la seguridad informática, a tal grado que para las empresas proveedoras de servicios de seguridad de la información resulta ideal que el personal que en ella labora cuente con capacitación en dichas normativas, con el fin de generar mayor confianza hacia la empresa y sus servicios por parte de los clientes con los que ya cuenta, así como atraer nuevos. Específicamente me refiero a la norma ISO 27001 e ITIL, de las cuales, la primera está relacionada con la preservación de la integridad, disponibilidad y confidencialidad de los activos de información de los clientes y contempla los rubros que se deben cubrir para establecer un sistema de gestión de seguridad de la información, mediante el uso de políticas, procesos y protocolos, mientras que la segunda hace referencia a una biblioteca de infraestructura de tecnologías de información y abarca la gestión de servicios de TI, basándose en el uso de mejores prácticas las cuales consisten en innovaciones exitosas implementadas por organizaciones líderes para cubrir las deficiencias en la calidad de los servicios.

Finalmente, también he de mencionar que durante mi estadía en el SOC, he reforzado el conocimiento en el uso de aplicaciones que me permiten desempeñar mis actividades de manera eficiente y segura, como lo son el manejo de clientes FTP para transferencia remota de archivos, uso de clientes VPN y SSH para conexiones remotas seguras, el uso de sistemas operativos Windows y Linux, así

como también aspectos enfocados a la documentación y comprensión de los procesos como lo son los flujos de información mediante diagramas y la colaboración en la documentación de planes de trabajo y memorias técnicas.

Este trabajo sirve de manera introductoria al lector para que conozca la forma en la que trabajan las empresas proveedoras de servicios de seguridad informática y sobre todo, cómo se proporcionan los servicios de monitoreo y administración en un SOC.

El objetivo establecido para este reporte de actividades se cumplió, ya que a través de este trabajo se introdujo un concepto como lo es el SOC, desconocido para muchos pero que cada vez es más frecuente que se mencione cuándo se habla de seguridad informática en las organizaciones.

# Anexo A: Operación y monitoreo de herramientas de seguridad

**Firewall de aplicación web (WAF)**

Al igual que un Firewall convencional, el *Web Aplication Firewall* (WAF) permitirá proteger la red, sin embargo, un WAF va más allá ya que ayuda a proteger las aplicaciones web de ataques especializados y concretamente enfocados a explotar fallos de seguridad en el protocolo HTTP.

Un firewall convencional es un dispositivo o software que es configurado en una red con el fin de filtrar la entrada y salida de paquetes, basándose en puertos, direcciones IP y tipo de tráfico. Estos dispositivos trabajan en la capa de red y funcionan de acuerdo a las reglas, permisos o privilegios que el administrador configura previamente.

Los WAF se pueden encontrar como dispositivos físicos (*appliances*) o de manera lógica como un *plugin* de los servidores web y navegadores, incluso existen WAF que ofrecen sus servicios de protección a través de la nube. Cualquiera que sea el modo empleado, la importancia del WAF radica en un conjunto de reglas que filtran y analizan el tráfico web entre un web server y la red externa (internet), es decir, los datos que recibimos por parte del usuario y las respuestas enviadas por el servidor al usuario final. Se puede decir entonces que un WAF actúa como un intermediario entre una aplicación web y el servidor que la contiene.

Muchos de los WAF trabajan comprobando firmas de ataques web conocidos, pero su misión principal es el funcionamiento de ataques que incluyen la manipulación de parámetros, cabeceras de las peticiones, Javascript, etc. Los WAF son capaces de proteger todo tipo de aplicaciones web alojadas en cualquier servidor, sin importar el lenguaje de programación en el que hayan sido desarrolladas. (Díaz, 2013)

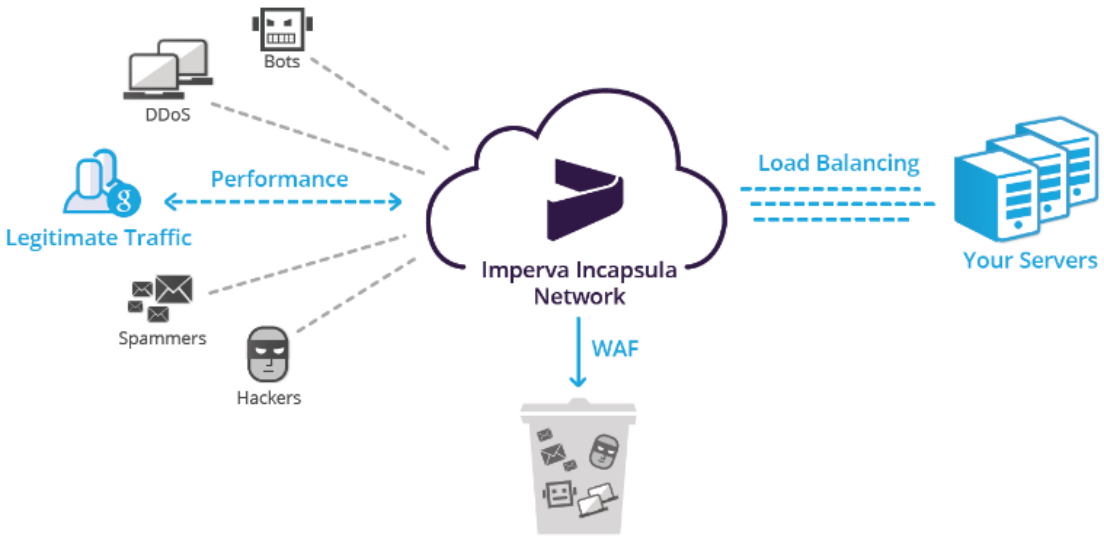



*Figura A1. Esquema de un WAF en la nube. (IMPERVA, 2017)*

Como se ha comentado previamente, los WAF trabajan basados en reglas configuradas por los administradores dentro de la herramienta, las cuales son patrones normalmente escritos como expresiones regulares encargadas de hacer el filtrado de la información que pasará o no pasará a través de nuestra red. Una vez activadas las reglas, toda la información que pasa a través del servidor es procesada y se determina si hace "*match*" con alguna de las reglas. Si la regla detecta alguna anomalía, la petición es bloqueada o notificada al administrador, de acuerdo a lo que se haya configurado.

Otra de las características de los WAF es que son capaces de reconocer tendencias como un número determinado de eventos concretos o incluso analizar cómo va navegando el usuario para conectarse a la página web en cuestión. De ahí que existan WAF que incluyen un modo de auto aprendizaje.

Los WAF tienen la capacidad de detectar y bloquear peticiones con contenido que la herramienta pudiera identificar como ataques potenciales entre los cuales encontramos CrossSite Scripting (XSS), SQL Injection (SQLi), Remote File Incusion (RFI), Bots maliciosos y Acceso a Recursos Ilegales, entre otros.

- **Bots maliciosos:** Agentes de búsquedas que refieren al sitio en cuestión. Para estos casos, los mismos *bots* pueden estar relacionados a la cosecha de direcciones de correo para realizar *spam*, programas que descargan sitios y reducen el ancho de banda disponible, *bots* que reutilizan el contenido de los sitios, etc.
- **Remote File Inclusion (RFI):** Intentos de subir archivos no validos al sistema o aplicación que pudieran afectar el rendimiento en general.
- **SQL Injection:** Ataques de inyección de información hacia las bases de datos relacionadas a la aplicación que pudieran subir o descargar información sensible, así como modificación de las tablas que gestionan la información.
- **CrossSite Scripting:** Ataques de ejecución de código malicioso en un sitio web que pueden afectar la experiencia del usuario presentando información falsa o irrelevante mediante comandos o peticiones específicas que modifican las cabeceras que interpreta el navegador.
- **Acceso a Recursos Ilegales:** Intentos de acceso a enlaces vulnerables, páginas de administración o ver y ejecutar archivos del sistema que pueden contener información sensible sobre la aplicación o el sistema en general. (IMPERVA, 2017)

De acuerdo a la configuración que se tenga en el WAF, es posible también realizar bloqueos y búsquedas de eventos de manera manual en lugar de que sean automáticos.

A continuación se muestran una serie de ejemplos en los cuales se realizan consultas personalizadas, así como las diferentes opciones de bloqueo que ofrece un WAF a través de la nube, el cual nos brinda protección contra todos los posibles ataques antes mencionados.

Como se puede observar, dentro de la herramienta existen una serie de filtros los cuales permiten realizar búsquedas concretas de acuerdo a la investigación o análisis que se quiera efectuar. Entre las opciones que se tienen se encuentra la posibilidad de hacer búsquedas por dirección IP, por tipo de ataque, por país de origen, etc.


*Figura A2. Búsqueda por tipo de ataque. Obtenida del Software WAF 2.*

También es posible hacer una combinación de criterios para una búsqueda más detallada.

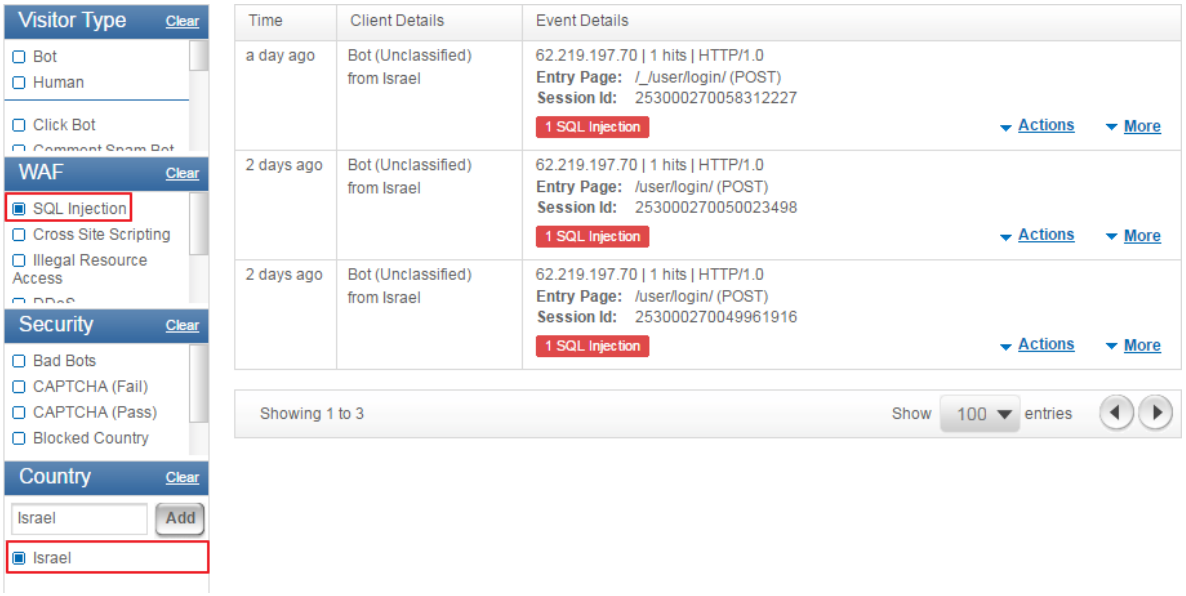



*Figura A3. Búsqueda por ataque y por país. Obtenida del Software WAF 2.*

Ahora bien, si es necesario, se pueden realizar distintos tipos de bloqueos dependiendo las necesidades o solicitudes del cliente y éstos pueden ser por tipo de ataque, por país, por dirección URL o por dirección IP. Las siguientes Figuras ilustran las opciones de bloqueo mencionadas.

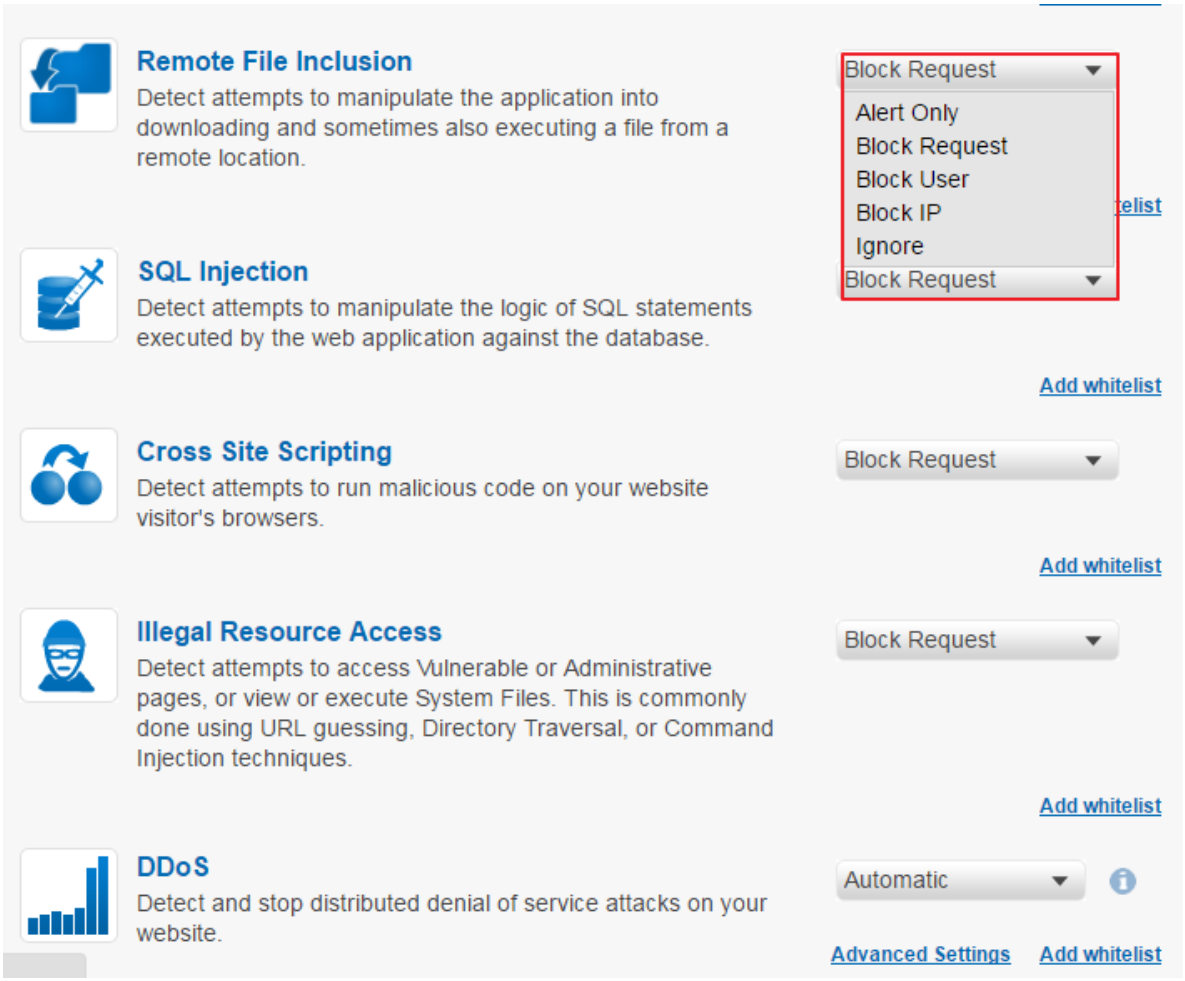



*Figura A4. Bloqueo por firma o tipo de ataque. Obtenida del Software WAF 2.*

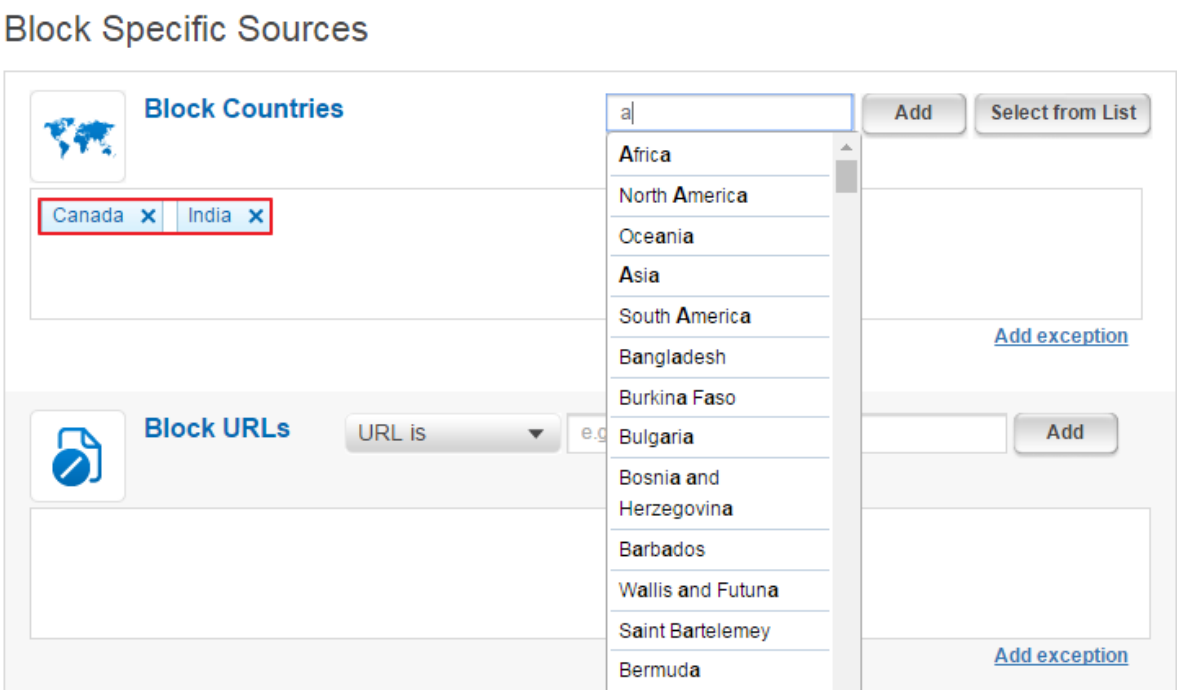



*Figura A5. Bloqueo por país. Obtenida del Software WAF 2.*

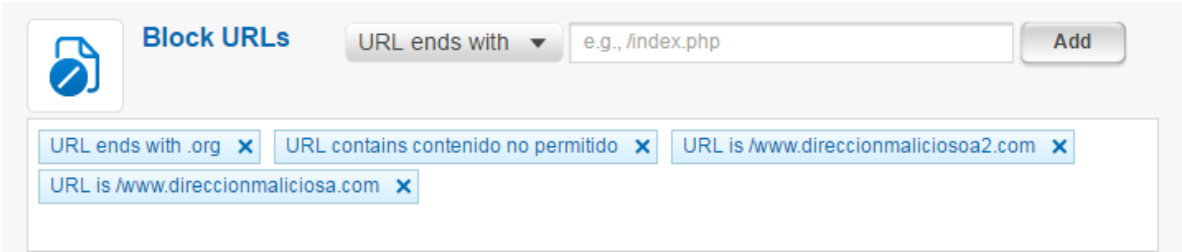



*Figura A6. Bloqueo por URL. Obtenida del Software WAF 2.*


*Figura A7. Bloqueo por dirección IP. Obtenida del Software WAF 2.*

Por último, el WAF también brinda la posibilidad de agregar una lista blanca, en la cual podemos registrar las direcciones específicas para las cuales queremos permitir que el tráfico pase sin ser filtrado por las reglas de seguridad y por lo tanto siempre será permitido su acceso a los sitios web. La Figura A8 ilustra el apartado de lista blanca.

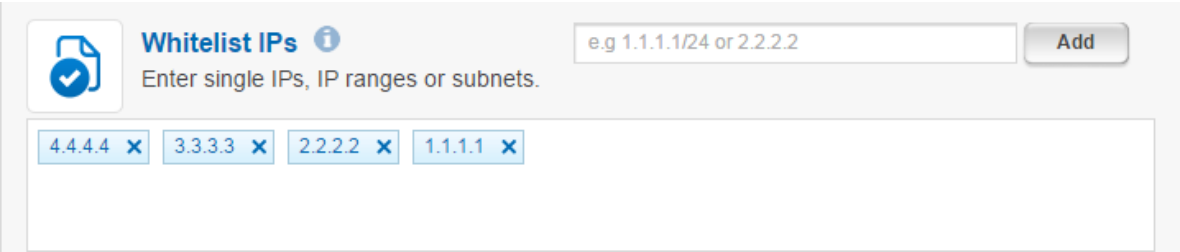



*Figura A8. Lista blanca del WAF. Obtenida del Software WAF 2.*

En conclusión podemos decir que un WAF bien configurado controla, analiza y permite o niega las peticiones que reciben los portales, utilizando motores que determinan si dichas peticiones son legítimas o si representan un riesgo para los sitios web de los clientes.

**Monitor de Actividad de Bases de Datos (DAM)**

En la actualidad la mayor parte de la información sensible para las organizaciones (ya sea parte del mismo negocio o de sus dependientes) se encuentra alojada en bases de datos a las cuales no debería tener acceso cualquier intruso. Adicionalmente siempre existe también el riesgo de que esta información pueda ser comprometida por parte del personal interno que realice cambios no autorizados, es decir, tanto dentro del negocio cómo fuera de él se corren riesgos que ponen en peligro la integridad y la confidencialidad de la información.

Es por eso que se han desarrollado herramientas que se encargan de auditar las bases de datos existentes dentro de la organización, de manera que el administrador de las bases de datos o el personal correspondiente tenga una completa visibilidad de todo lo que ocurre con las mismas. Una de esas herramientas es el *Database Activity Monitoring* (DAM), el cual proporciona monitoreo en tiempo real de todas las consultas y operaciones realizadas sobre una base de datos, así como información de usuarios (privilegiados y no privilegiados), direcciones de origen y destino, control de acceso, etc.

Mediante el DAM se puede visualizar de manera centralizada la actividad ocurrida en las bases de datos sin importar su ubicación y generalmente soportan todos los manejadores de bases de datos más conocidos, utilizando agentes inteligentes que

reportan la actividad al servidor central del DAM, el cual se encarga de desplegar la información mediante una interfaz gráfica, de tal manera que no sea necesario implementar procedimientos adicionales que le permitan al administrador saber qué actividad se hizo, así como quién y cuándo la realizó. (IMPERVA, 2010)

Las Figuras A9 y A10 ejemplifican la manera en la que se muestra la información de un evento en el DAM. En este caso corresponde a un evento de Acceso fallido.

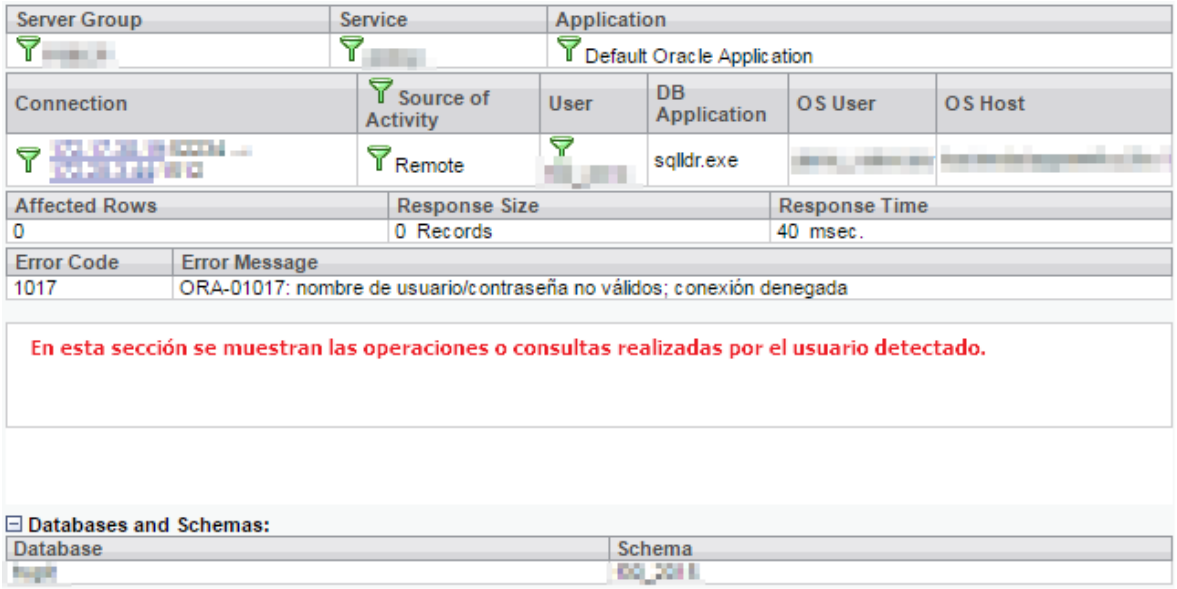



*Figura A9. Evento de acceso fallido en un DAM. Obtenida del Software DAM 1.*

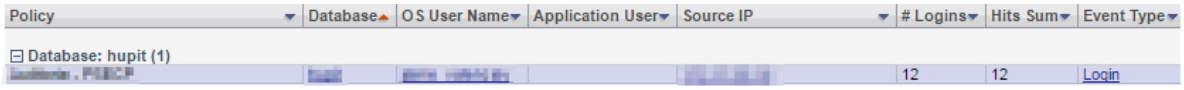



*Figura A10. Detalle de acceso fallido. Obtenida del Software DAM1.*

Existen diversos puntos a considerar para definir el tipo de eventos que se van a monitorear referente a las bases de datos, por lo que es importante que las organizaciones cuenten con una serie de políticas bien definidas que contemplen aspectos como la identificación de tablas que contengan datos sensibles, limitar el acceso a los datos a ciertos usuarios, establecer los horarios laborales, determinar los usuarios que puedan realizar cambios de configuraciones y cambios de privilegios de las cuentas, etc. En pocas palabras, hay que tener bien identificado qué se puede hacer y qué no. (Murillo, 2011)

Una de las características que resulta muy útil de esta herramienta es que brinda la posibilidad de crear y ejecutar reportes detallados de la actividad registrada sobre

las bases de datos a auditar, de este modo es posible tener un mejor control, así como un panorama más amplio de lo que está sucediendo con las bases de datos y de ser necesario realizar las acciones de mitigación correspondientes.

La herramienta cuenta con un módulo especial, el cual permite administrar reportes y configurar las opciones de los mismos (Figura A11).

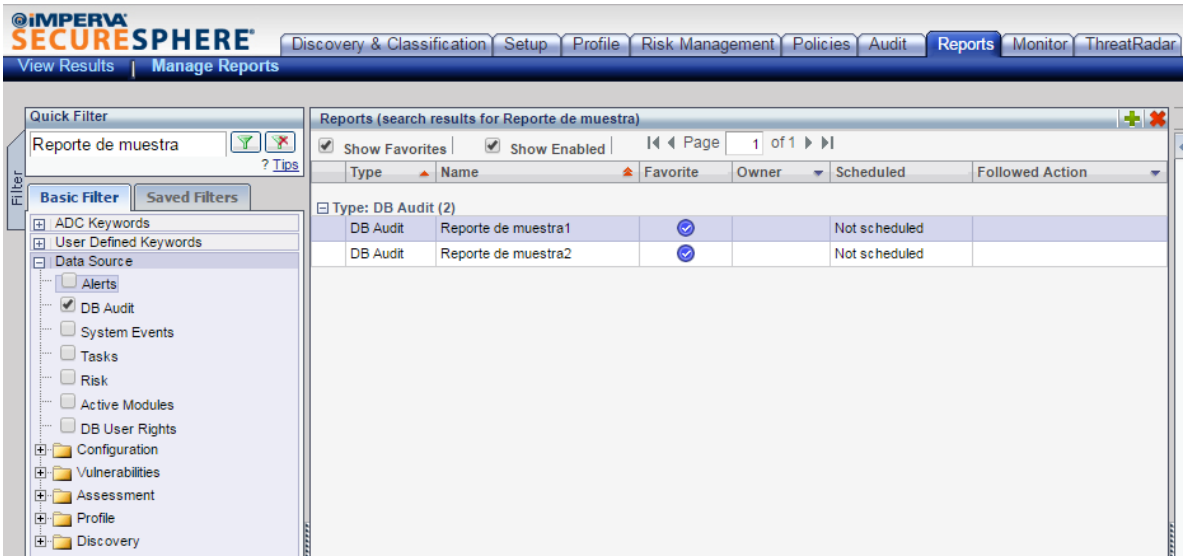



*Figura A11. Módulo de reportes de un DAM. Obtenida del Software DAM 1.*

A continuación se ejemplifica cómo es el proceso de creación de un reporte, así como el alcance que éste puede tener.

Existen distintos campos a considerar para configurar la ejecución del reporte así como la manera en que se desea se muestren los datos. Entre estos campos, los más importantes son: *General Details* que es donde elegimos el formato del reporte a generar (pdf o csv), *Data Scope* que es donde especificamos los criterios de coincidencia o de *match* para que el DAM capture únicamente los eventos que cumplan dichas características y finalmente *Tabular* que es donde indicamos qué información queremos que nos muestre el DAM sobre cada evento (direcciones de origen y de destino, usuarios, puertos, etc.).

Para este ejemplo se creará un reporte que muestre la información sobre qué operaciones de DML (*Insert, Update y Delete*) han ejecutado los usuarios *Usuariuo1, Usuario2, Usuario 3 y Usuario4* sobre la base de datos *base de muestra1*. En las Figuras A12 y A13 se muestran los ajustes necesarios para obtener el reporte mencionado.

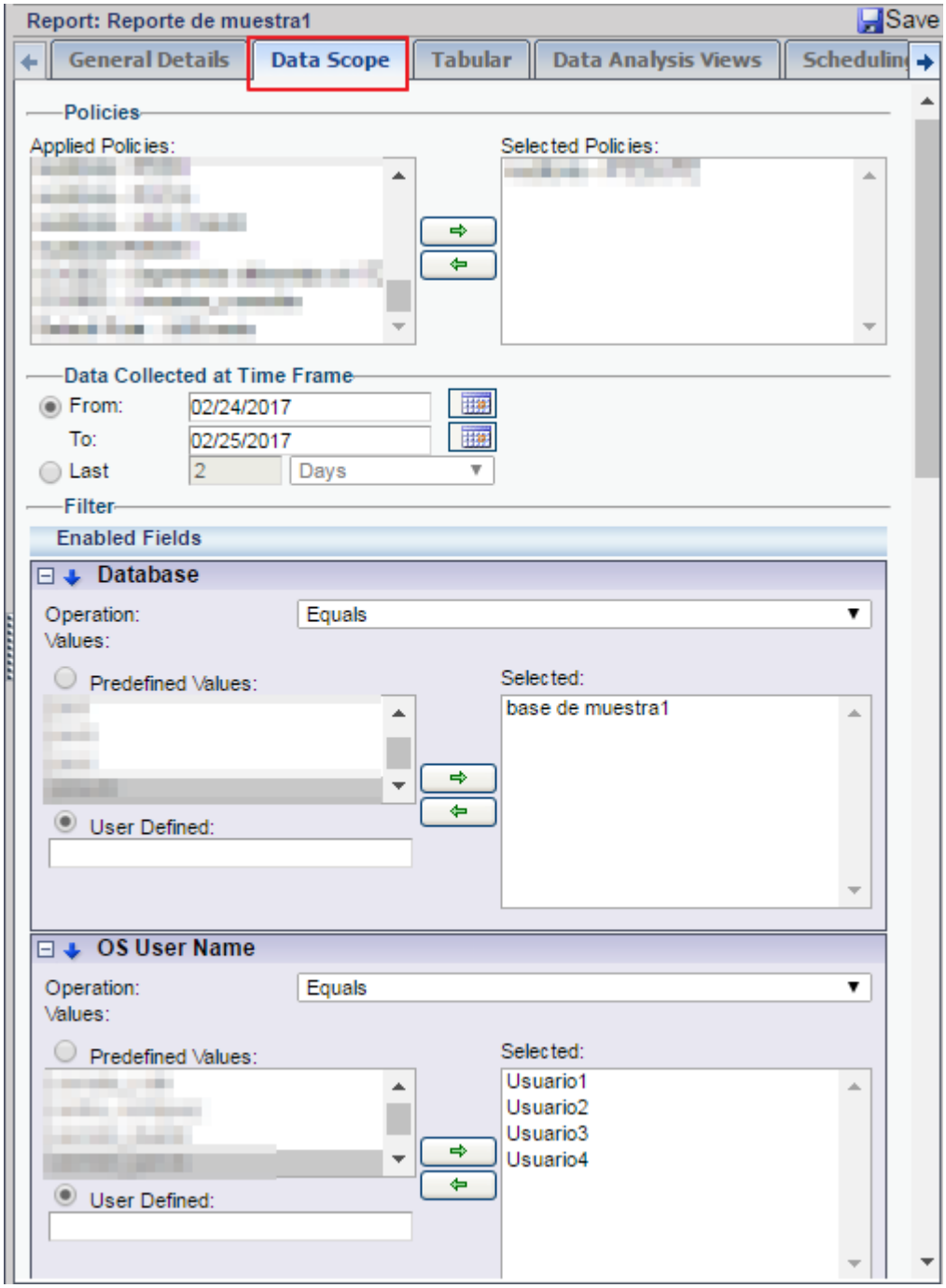



*Figura A12. Ajustes de match de fecha, base de datos y usuarios en un reporte en el DAM. Obtenida del Software DAM 1.*

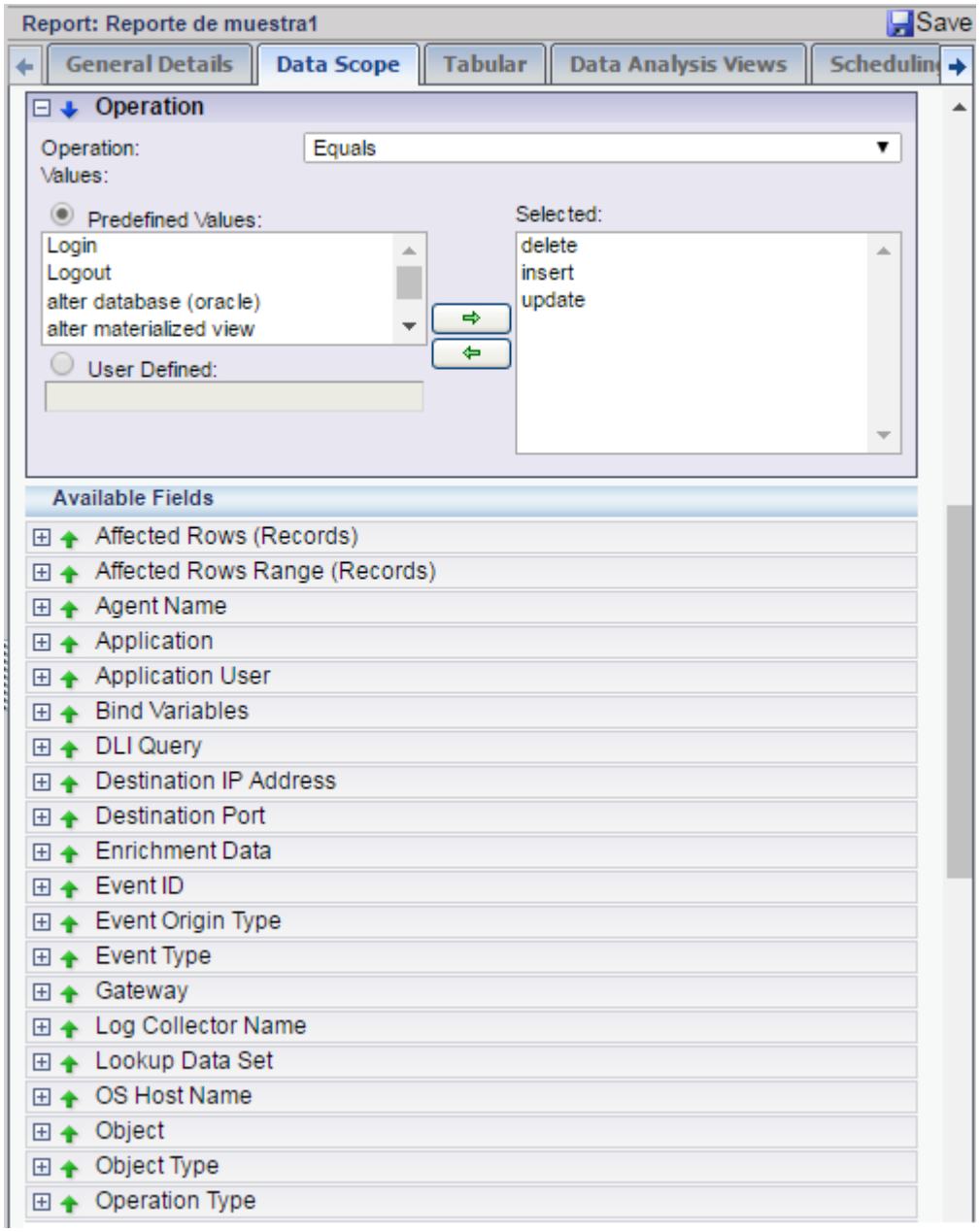



*Figura A13. Ajustes de match de operaciones en un DAM. Obtenida del Software DAM 1.*

Ahora procedemos a especificar la información que se desea mostrar para cada evento capturado con los criterios anteriores (Figura A14)

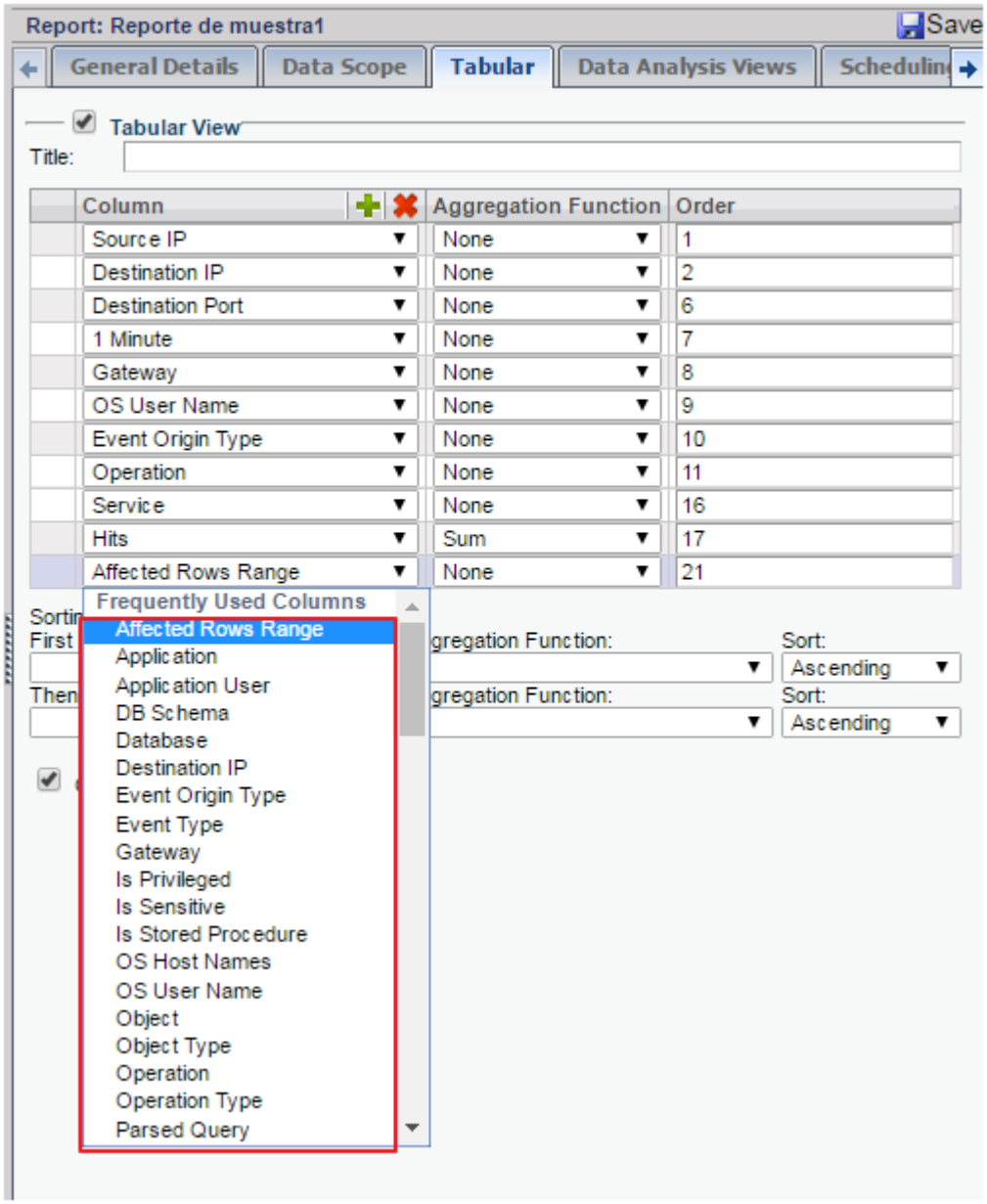



*Figura A14. Especificación de columnas que contendrá el reporte. Obtenida del Software DAM 1.*

Finalmente, al ejecutar el reporte obtendremos un resultado como el siguiente:

| Source IP | Destination IP | Destination Port | Time Group - 1 Minute | Gateway Noi | OS User Name | Event Origin Type | Operation | Service | Hits Sum |
|---|---|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | 1669 | 02/24/2017 4:34:00 PM | [redacted] | Usuario3 | Network | Update | base de muestra1 | 39 |
| [redacted] | [redacted] | 1669 | 02/24/2017 9:04:00 AM | [redacted] | Usuario4 | Network | Update | base de muestra1 | 28 |
| [redacted] | [redacted] | 1669 | 02/24/2017 9:18:00 AM | [redacted] | Usuario1 | Network | Update | base de muestra1 | 8 |
| [redacted] | [redacted] | 1669 | 02/24/2017 8:51:00 AM | [redacted] | Usuario1 | Network | Update | base de muestra1 | 6 |
| [redacted] | [redacted] | 1669 | 02/24/2017 8:59:00 AM | [redacted] | Usuario2 | Network | Update | base de muestra1 | 5 |
| [redacted] | [redacted] | 1669 | 02/24/2017 8:15:00 AM | [redacted] | Usuario1 | Network | Update | base de muestra1 | 5 |
| [redacted] | [redacted] | 1669 | 02/24/2017 9:44:00 AM | [redacted] | Usuario2 | Network | Update | base de muestra1 | 4 |
| [redacted] | [redacted] | 1669 | 02/24/2017 1:15:00 PM | [redacted] | Usuario1 | Network | insert | base de muestra1 | 4 |
| [redacted] | [redacted] | 1669 | 02/24/2017 9:54:00 AM | [redacted] | Usuario2 | Network | insert | base de muestra1 | 4 |
| [redacted] | [redacted] | 1669 | 02/24/2017 1:38:00 PM | [redacted] | Usuario2 | Network | insert | base de muestra1 | 4 |
| [redacted] | [redacted] | 1669 | 02/24/2017 9:45:00 AM | [redacted] | Usuario1 | Network | Update | base de muestra1 | 3 |
| [redacted] | [redacted] | 1669 | 02/24/2017 9:01:00 AM | [redacted] | Usuario1 | Network | Delete | base de muestra1 | 3 |
| [redacted] | [redacted] | 1669 | 02/24/2017 9:07:00 AM | [redacted] | Usuario3 | Network | Delete | base de muestra1 | 2 |
| [redacted] | [redacted] | 1669 | 02/24/2017 8:46:00 AM | [redacted] | Usuario1 | Network | insert | base de muestra1 | 2 |
| [redacted] | [redacted] | 1669 | 02/24/2017 2:26:00 PM | [redacted] | Usuario1 | Network | Delete | base de muestra1 | 2 |
| [redacted] | [redacted] | 1669 | 02/24/2017 10:06:00 AM | [redacted] | Usuario3 | Network | Update | base de muestra1 | 1 |
| [redacted] | [redacted] | 1669 | 02/24/2017 9:38:00 AM | [redacted] | Usuario4 | Network | insert | base de muestra1 | 1 |
| [redacted] | [redacted] | 1669 | 02/24/2017 8:55:00 AM | [redacted] | Usuario4 | Network | Delete | base de muestra1 | 1 |
| [redacted] | [redacted] | 1669 | 02/24/2017 2:24:00 PM | [redacted] | Usuario1 | Network | Update | base de muestra1 | 1 |
| [redacted] | [redacted] | 1669 | 02/24/2017 12:22:00 PM | [redacted] | Usuario1 | Network | Update | base de muestra1 | 1 |
| [redacted] | [redacted] | 1669 | 02/24/2017 1:17:00 PM | [redacted] | Usuario1 | Network | Update | base de muestra1 | 1 |

*Figura A15. Muestra del reporte configurado.*

Como podemos observan la información es presentada en forma de tabla con todos los campos especificados previamente. Al abrir este informe con una hoja de cálculo como Excel, es posible realizar gráficas para presentar una mejor evidencia de la actividad registrada al cliente.

Otro aspecto a considerar con esta herramienta es que, como ya se mencionó, está regida por políticas las cuales se encargan de capturar los eventos de acuerdo a los criterios especificados; a estas políticas se les asigna un determinado espacio de almacenamiento el cual puede variar dependiendo la cantidad de eventos que se generen día con día para cada una de las políticas. De tal manera que, si el espacio destinado se llega a terminar, se corre el riesgo de que la política en cuestión deje de registrar eventos nuevos, por lo que en estos casos es requerido realizar un respaldo del contenido de cada política (a este respaldo se le conoce como *archive*) una vez que la mismo deje de capturar información y posteriormente depurarla para que comience nuevamente el proceso de recolección de eventos (a dicha depuración se le conoce como *purge*).

Al realizar el respaldo de la política se generará un archivo especial con extensión .mprv que se puede cargar directamente en el *appliance* para una consulta posterior en caso de ser requerida.

La Figura A16 ilustra la pérdida de eventos para una política las últimas 24 horas, sin embargo, los 7 días previos colectó eventos sin inconvenientes. Mientras que la Figura A17 muestra las acciones *archive* y *purge* para respaldar y depurar respectivamente.

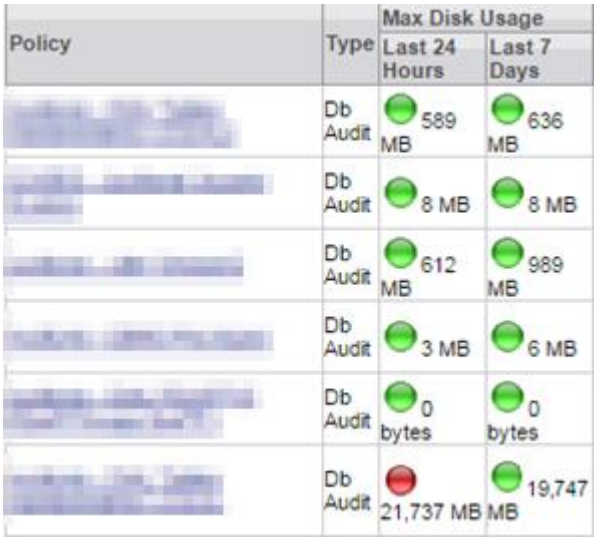



*Figura A16. Pérdida de eventos durante las últimas 24 horas. Obtenida del Software DAM 1.*

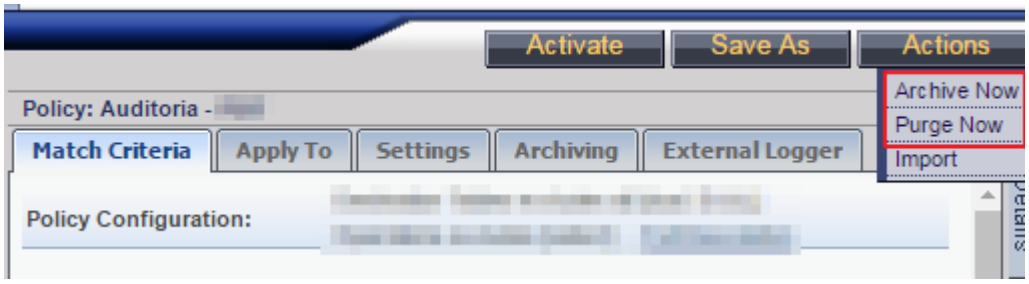



*Figura A17. Opciones de Archive y Purge. Obtenida del Software DAM 1.*

Cabe mencionar que la revisión del estado de las políticas generalmente se lleva a cabo dentro de una actividad programada conocida como lista de chequeo.

### Sistema de Detección de Intrusos (IDS) y Sistema de Prevención de Intrusos (IPS)

Los *Intrusion Detection System* (IDS) son dispositivos tanto físicos como lógicos cuya función es analizar el tráfico de red para identificar posibles paquetes maliciosos o anómalos. Se dice que son mecanismos pasivos de defensa debido a que su principal característica es la de alertar la actividad sospechosa, sin embargo, no realizan acciones de contención o mitigación de ataques, por lo tanto, representan una herramienta de visibilidad. (Santillán Arenas, 2011)

Los IDS son capaces de identificar actividades como violaciones de políticas de seguridad, infecciones como virus y troyanos, fugas de información mediante software espía, etc.

Los IDS utilizan los siguientes métodos de detección para poder realizar sus funciones:

- **Detección basada en firmas:** La detección por firmas consiste en definir patrones de comportamiento basados en amenazas conocidas. Contienen características como tipo de tráfico, dirección de flujo, protocolo, direcciones IP, puertos o incluso el contenido de los datos dentro del paquete. Cuando un paquete de red coincida con este patrón, entonces se enviará la alerta correspondiente con la información relacionada que recolectó el IDS (Santillán Arenas, 2011).

  Los IDS cuentan con una base de datos de firmas, también llamada archivo o paquete de firmas, el cual el IDS utiliza para comparar el tráfico de red contra los patrones de datos contenidos en la librería de archivos de firma. Mediante esta comparación el IDS puede detectar posible tráfico malicioso. Es por eso que dicho archivo de firmas debe mantenerse actualizado en sus últimas versiones, de este modo la red será menos vulnerable ante nuevas amenazas (CISCO, 2005).
- **Detección basada en anomalías:** Funciona mediante la definición de criterios base, que suponen un funcionamiento normal de la red. Esta línea de base es una descripción del comportamiento de red aceptado, aprendido o especificado por los administradores de red, o ambos (Foster, 2017). Cuando se detecta cierta actividad que no corresponde con los criterios base, entonces el IDS cataloga la actividad como una anomalía y por lo tanto, puede representar tráfico malicioso. Algunos métodos para detectar tráfico que pudiera considerarse anormal se basan en la comparación del comportamiento esperado de cierto tipo de protocolos de comunicación. Es decir, si se tiene bien identificado el comportamiento del tráfico según su naturaleza, entonces cualquier patrón fuera de ella representa un factor para poder identificarlo como anormal (Santillán Arenas, 2011).

  La detección de anomalías tiene una ventaja sobre los motores basados en firmas y es que un nuevo ataque para el que no existe una firma (ataque de día cero) puede ser detectado si cae fuera de los patrones normales de tráfico (Foster, 2017).

Los IDS pueden ser de tres tipos, los cuales se muestran a continuación:

### IDS basados en host

Este tipo de IDS funciona monitoreando la actividad de un sistema local. Por su esquema de funcionamiento analiza el tráfico de red que entra y sale del equipo, así como los cambios en el sistema de archivos y la actividad del sistema en general (Santillán Arenas, 2011).

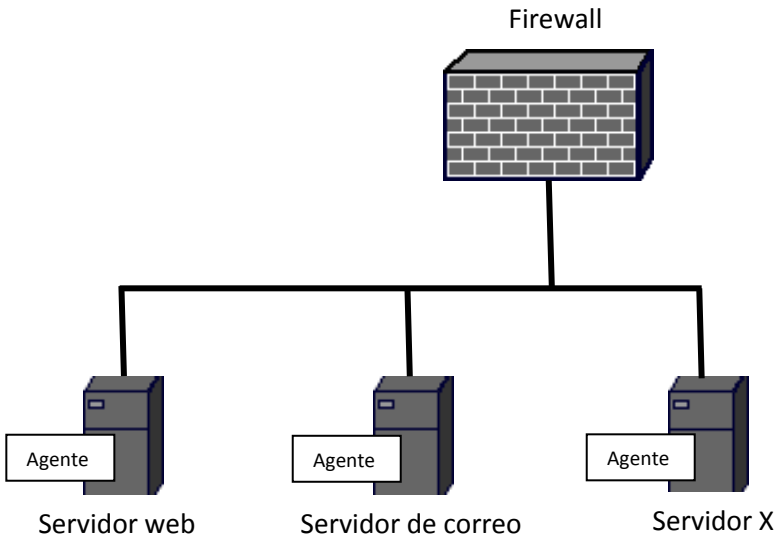



*Figura A18. Esquema de un IDS basado en host. Adaptado de (Santillán Arenas, 2011)*

### IDS basados en red

Este tipo de IDS analiza el tráfico de un equipo o red. Puede instalarse en un equipo analizando sólo el tráfico que fluye a través de él, sin embargo, para que funcione plenamente, debe implementarse un esquema donde reciba el tráfico de todos los equipos conectados a la red. Generalmente se instala en el perímetro de la red o subred para poder monitorear el tráfico de entrada y salida de la misma (Santillán Arenas, 2011).

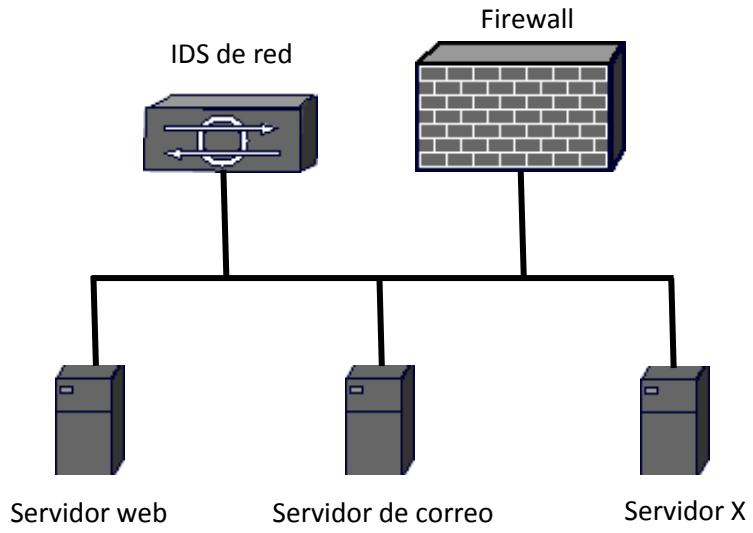



*Figura A19. Esquema de un IDS basado en red. Adaptado de (Santillán Arenas, 2011)*

### IDS distribuidos

Es un esquema de varios IDS desplegados a lo largo de la red los cuales funcionan como sensores y envían el tráfico detectado a un servidor que centraliza la información. Este tipo de esquema es muy útil en redes de gran tamaño y es el más común usado en las organizaciones debido a que es posible poner un sensor en cada área o departamento de la misma y de este modo tener un mejor control para identificar en dónde se pudiera presentar la actividad sospechosa (Santillán Arenas, 2011).

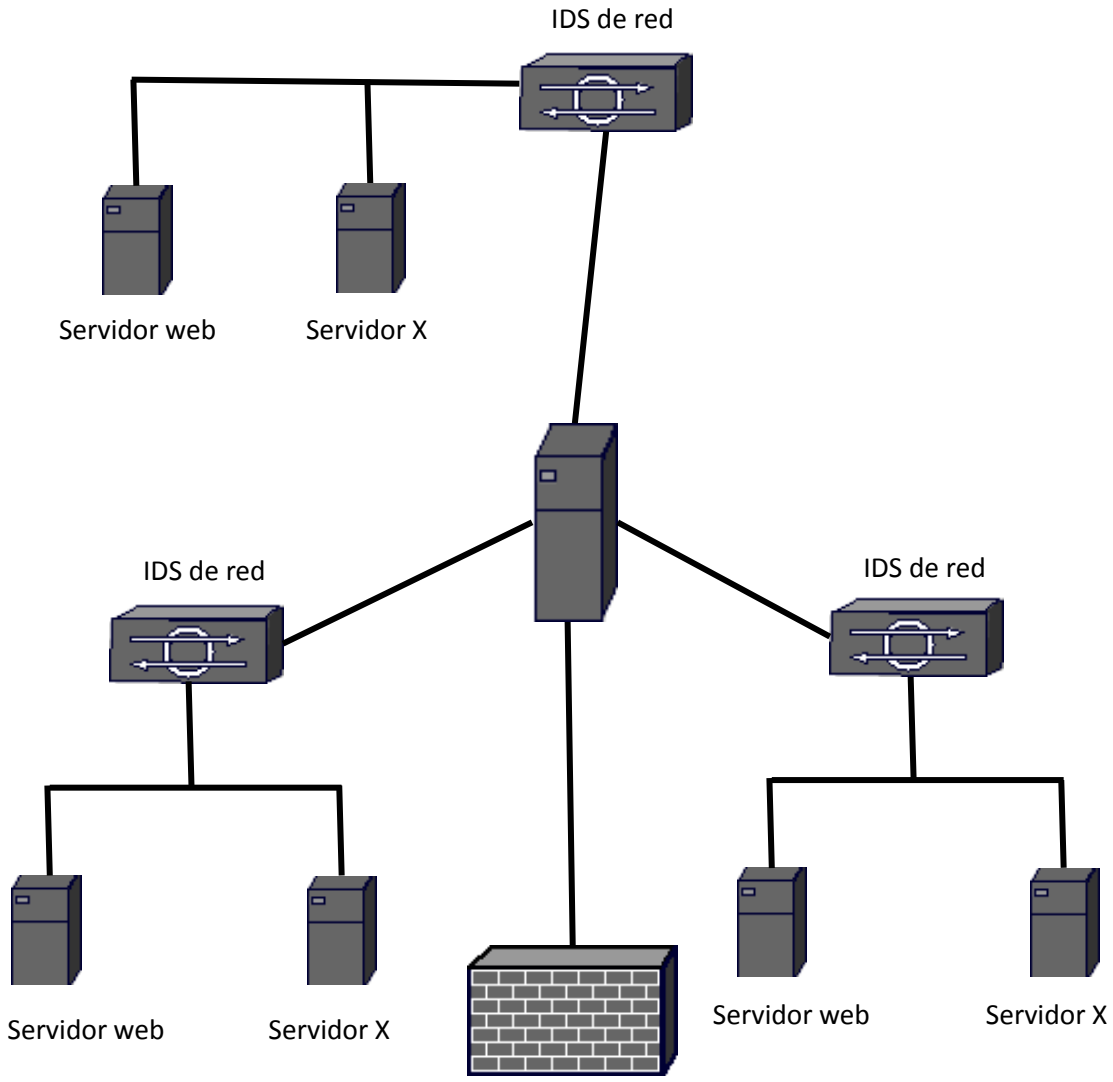



*Figura A20. Esquema de un IDS distribuido. Adaptado de (Santillán Arenas, 2011)*

Ahora bien, los *Intrusion Prevention System* (IPS) son también dispositivos físicos o lógicos para la detección de tráfico malicioso y representan un mecanismo de control dentro de la red. Al igual que los IDS trabajan basados en firmas y anomalías, sin embargo, la principal diferencia entre ambos es que los IPS son dispositivos activos, es decir, actúan bajo demanda según las alertas detectadas. A partir de que un evento es detectado, el IPS puede aplicar automáticamente una medida de mitigación (a este proceso de respuesta se le conoce como *inline*) (Santillán Arenas, 2011). Una característica del funcionamiento de un IPS es que todo el tráfico que pasa a través del él está permitido, a menos que haga *match* con alguna de las reglas, la cual bloqueará el problema de seguridad asociado a dicha regla (Snyder, 2017).

Un aspecto importante a considerar a la hora de implementar un IPS son los falsos positivos, debido a que mientras en el IDS estos no representan afectación como tal en el desempeño de la red, en el IPS ocurre lo contrario, ya que una regla mal aplicada puede dar como resultado una auto-negación de servicio, es decir, puede existir bloqueo de tráfico legítimo debido a que si el IPS identifica un comportamiento similar al de una firma, éste ejecutará automáticamente una acción de mitigación. Es por eso que las firmas deben definirse con el criterio más acertado posible para minimizar el número de falsos positivos (Santillán Arenas, 2011). La detección por firmas es bastante útil para realizar búsqueda de comportamientos de ataques específicos, es decir, si se tiene la sospecha de que cierto ataque se está presentando en la red, lo ideal es agregar una firma en el IPS que haga la búsqueda de dicho comportamiento y en caso de detectarlo realice el bloqueo correspondiente.

Como se puede observar, tanto IDS como IPS representan herramientas muy poderosas y útiles para la protección de los sistemas en general. En el capítulo correspondiente al análisis de firmas de este trabajo se explica el procedimiento de análisis en un IPS basado en firmas.

### Correlacionador de eventos (SIEM)

Es común que las instituciones presenten una gran cantidad de diferentes dispositivos en su infraestructura de TI, desde lo más esencial para realizar sus actividades cotidianas como estaciones de trabajo (PC) y routers, hasta equipos especiales de seguridad como IPS, IDS y Firewalls. Por lo que la gestión de eventos de seguridad se vuelve más compleja y difícil de visualizar debido a que todos estos eventos provienen de diferentes fuentes y ubicaciones, a pesar de ser parte de la misma red.

Para evitar que esta situación represente una labor más exhaustiva existen las herramientas de correlación de eventos también conocidas como *Security Information and Event Managment* (SIEM).

Los SIEM son herramientas capaces de concentrar y gestionar los eventos de una gran cantidad de dispositivos haciendo posible la detección de patrones que pudieran representar algún incidente de seguridad.

Un SIEM es la combinación de las tecnologías *Security Information Management* (SIM) y *Security Event Manager* (SEM). La primera de ellas está enfocada en el monitoreo en tiempo real, correlación de eventos y notificaciones; mientras que la segunda se encarga del almacenamiento, el análisis y la comunicación de los datos de registro (Operador, 2013).

Las tecnologías SIEM representan un filtro de seguridad muy poderoso, el cual ayuda a reforzar la protección de la red. Dentro de sus funciones se encuentran las siguientes:

- **Agregación de datos:** Se considera su capacidad de administrar bitácoras desde diversas fuentes como redes, equipos de seguridad, bases de datos, servidores, etc. (Operador, 2013).
- **Correlación:** Es la capacidad de recolectar eventos de diferentes tipos y encontrar interrelaciones entre ellos con el fin de identificar patrones, de este modo, una serie de eventos aislados al conjuntarse se convierten en información para el analista (Romero, 2013).
- **Alertas:** Una característica fundamental de los SIEM es la generación de alertas respecto a los eventos detectados, estas se configuran en las reglas establecidas por los administradores y se pueden visualizar directamente en el historial de la herramienta o es posible que éstas notificaciones sean enviadas mediante un correo electrónico el cual contiene datos generales del evento como dirección, origen, nombre del dispositivo, número de hits y tipo común de evento (un acceso fallido es notificado como tal sin importar si se trata de un sistema windows, linux o appliance conectado al SIEM).
- **Retención:** Se refiere a la capacidad de almacenamiento a largo plazo, la cual es esencial para un posible análisis forense (Operador, 2013).
- **Normalización:** Consiste en dejar los eventos en un formato estándar independiente de la plataforma original de donde provienen (Polanco, 2010).
- **Dashboard:** Son interfaces que nos permiten la visualización de los eventos de forma más amigable para el usuario. En ellos se toman los datos del evento y son presentados en forma de tablas informativas o gráficas que facilitan la observación de comportamientos permitidos y no permitidos.

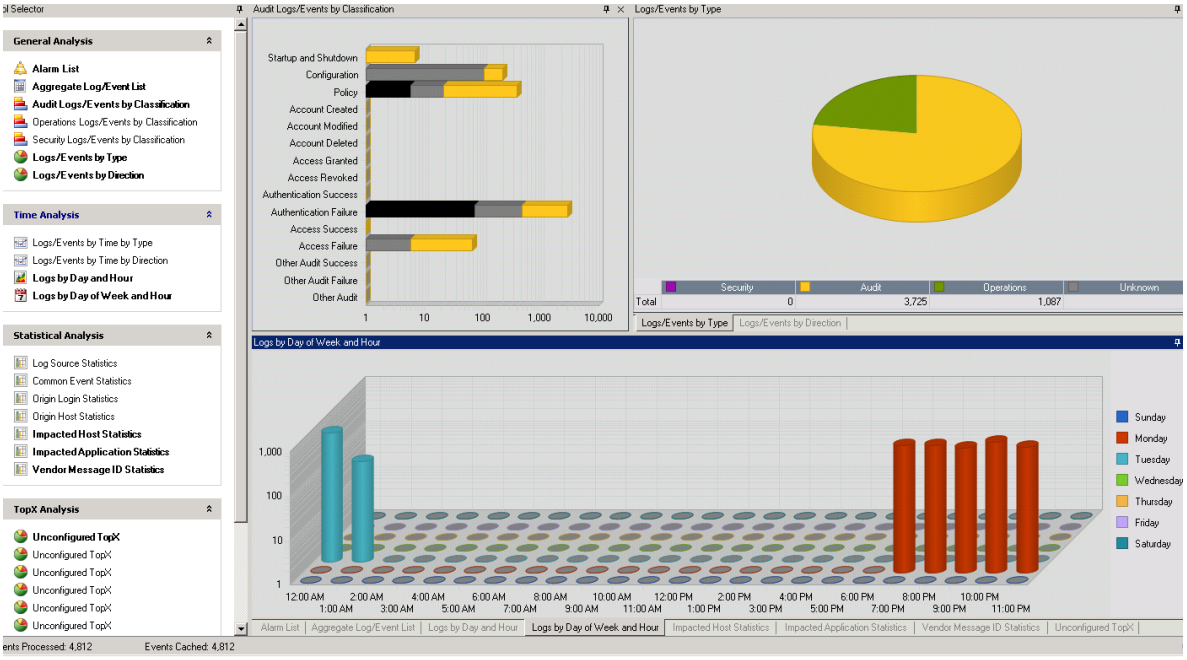



*Figura A21. Dashboard principal de un SIEM. Obtenida del Software SIEM 1.*

La Figura A22 ilustra cómo es que las notificaciones generadas por el SIEM son recibidas vía correo electrónico.

ALARM ID: 67338
ALARM DATE: 1/17/2017 11:27:55 AM(GMT-06:00) Guadalajara, Mexico City, Monterrey - Old
FIRST EVENT DATE: 1/17/2017 11:27:33 AM(GMT-06:00) Guadalajara, Mexico City, Monterrey - Old
LAST EVENT DATE: 1/17/2017 11:27:34 AM(GMT-06:00) Guadalajara, Mexico City, Monterrey - Old
EVENT COUNT: 35
DIRECTION: Local, Unknown
CLASSIFICATION: Authentication Failure
COMMON EVENT: User Logon Failure : Bad Username
RISK BASED PRIORITY (RBP):3.00
ORIGIN HOST:
IMPACTED HOST:

*Figura A22. Notificación de evento en un SIEM vía correo electrónico. Obtenida del Software SIEM 1.*

A partir de la alerta recibida es posible realizar una búsqueda para obtener mayor detalle del evento correspondiente. Los resultados de la búsqueda se ejemplifican en las Figuras A23 y A24.

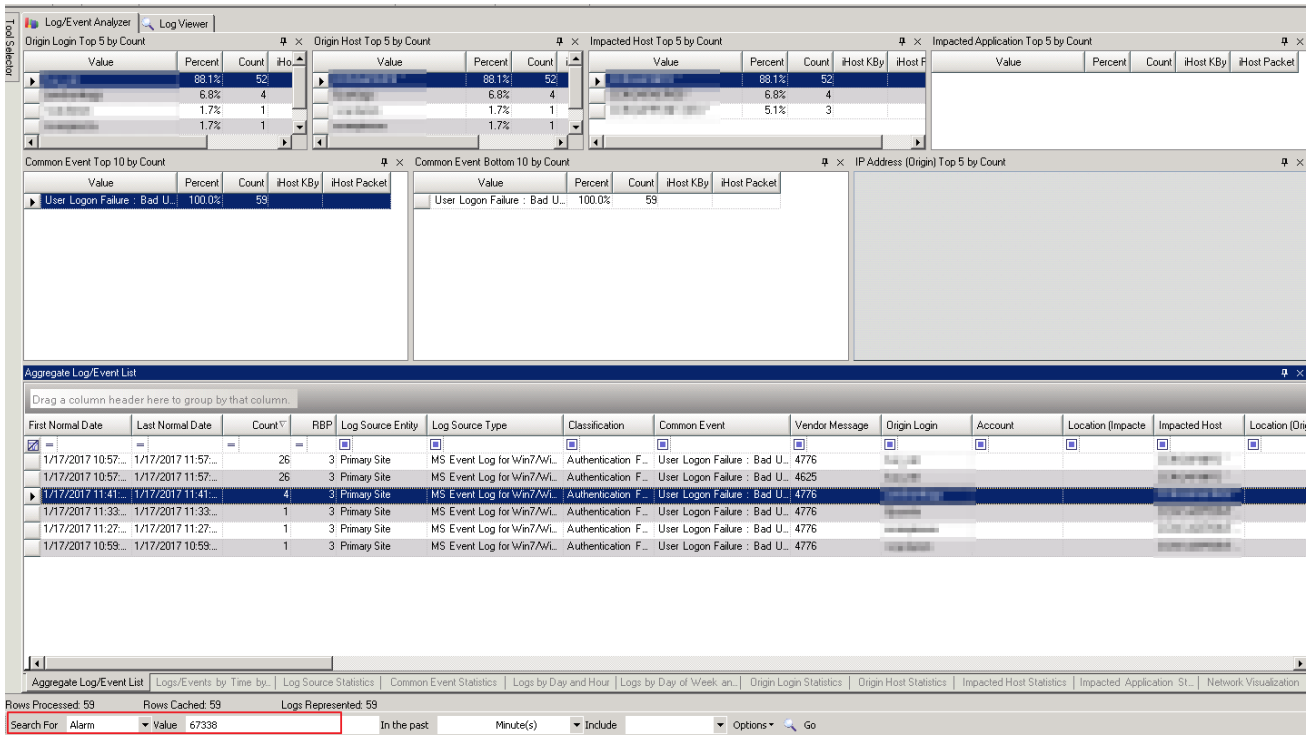



*Figura A23. Búsqueda de evento. Obtenida del Software SIEM 1*

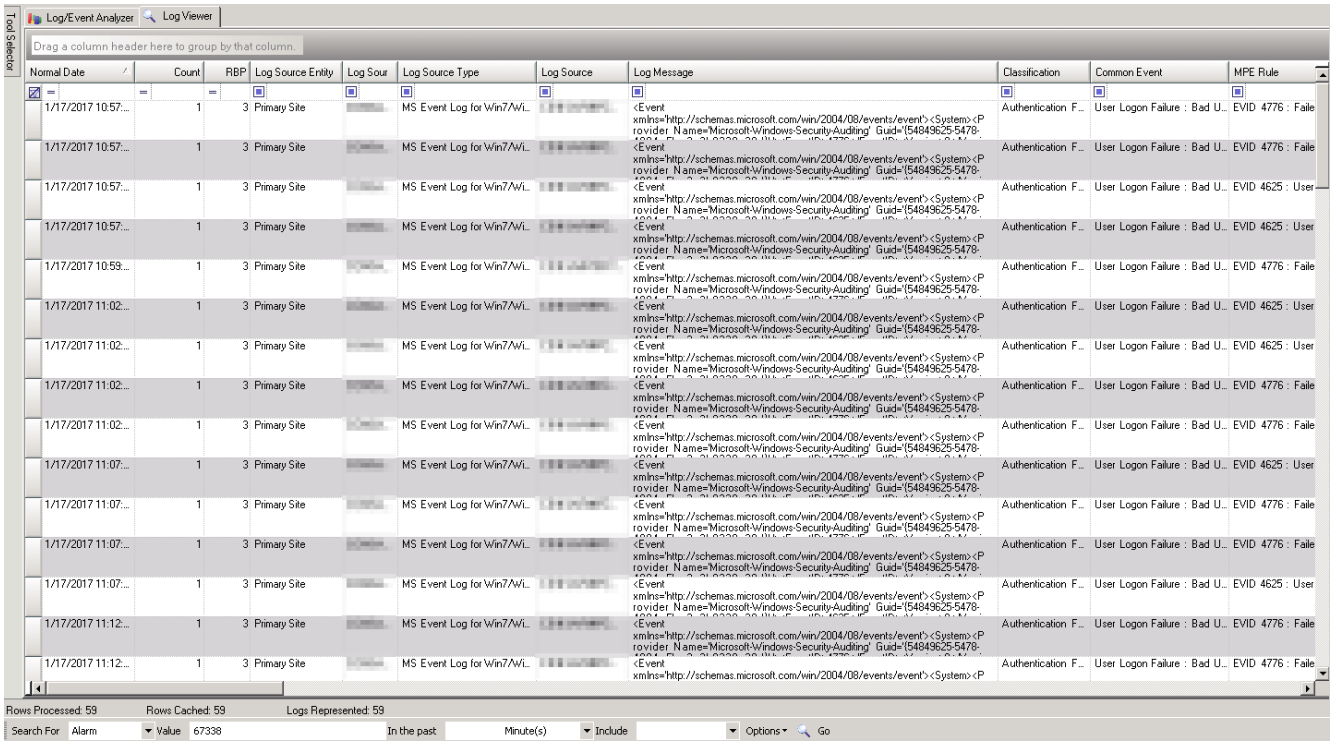



*Figura A24. Detalles del evento. Obtenida del Software SIEM 1.*

Finalmente, es posible generar informes estadísticos de diferentes tipos (Figura A25), para identificar tendencias y tener un mayor panorama de lo que ocurre en los sistemas.

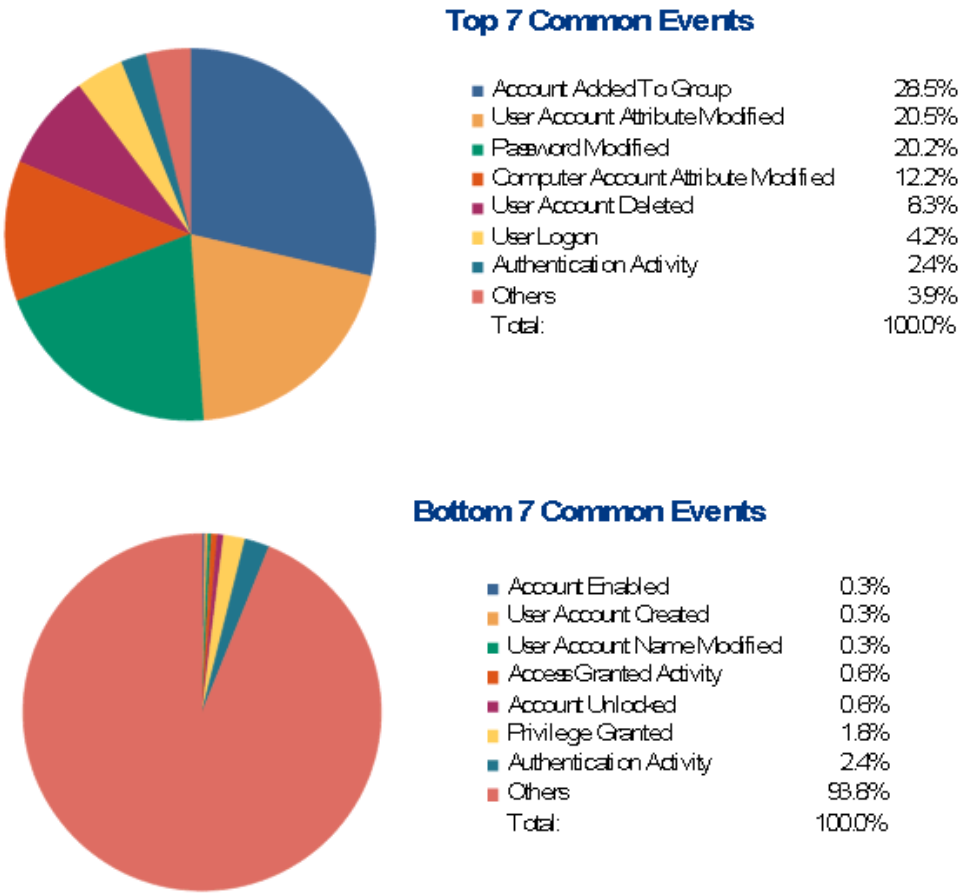



*Figura A25. Informes estadísticos generados por el SIEM. Obtenida del Software SIEM 1.*

### Anti-Denegación de Servicio Distribuido (Anti-DDoS)

En la actualidad los ataques *Distributed Denial of Service* (DDoS) son de los más utilizados debido a lo relativamente sencillo que resulta para un usuario realizarlo, incluso sin tener los suficientes conocimientos sobre TI. De hecho, existen sitios web en los que es posible rentar una *botnet* con el fin de realizar ataques DDoS a una víctima particular (Reyes, 2011). Este tipo de ataque resulta especialmente perjudicial para aquellas instituciones cuyo principal ingreso se basa en la disponibilidad de sus sitios web, por ejemplo los sitios de publicidad y ventas por internet; si los clientes no tienen acceso a sus sitios representaría pérdidas monetarias importantes. Sin embargo, no solo el sector privado se ve afectado por este tipo de ataques ya que existen los denominados “grupos Hacktivistas” quienes

generalmente encabezan estos ataques invitando al pueblo a unirse como una muestra de protesta o descontento social y en estos casos las principales víctimas son del sector gubernamental (Ruíz, 2012).

Ahora que se tiene un mayor contexto de las consecuencias que conlleva un ataque DDoS, procederé a definir en qué consisten dichos ataques, sus características y técnicas de mitigación.

Un ataque *Distributed Denial of Service* (DDoS) es una variante del ataque *Denial of Service* (DoS) cuyo principal objetivo es inhabilitar un servidor, un servicio o una infraestructura sobrecargando el ancho de banda del servidor o acaparando sus recursos hasta agotarlos, dando como resultado que éstos sea inaccesibles para usuarios legítimos (OVH, 2017). La diferencia entre uno y otro es como su nombre lo indica, que el primero es un ataque de denegación de servicio distribuido, es decir, que el flujo de tráfico para realizar el ataque es generado desde múltiples puntos de conexión.

Esto puede lograrse de diferentes maneras como pueden ser que un numeroso grupo de personas se organicen para hacer peticiones legítimas a algún objetivo para generar un excesivo flujo de tráfico, también existen herramientas diseñadas para generar peticiones masivas hacia un objetivo específico y la técnica más común es usar las ya mencionadas *botnets*. Una *botnet* es una red de computadoras infectadas con malware conocidas como “máquinas zombis” o *bots* y que son controladas remotamente por un atacante con fines maliciosos como envió masivo de spam, robo de información y ataques DDoS. Todo esto se logra sin que los equipos víctima se enteren que forman parte de la *botnet*, por lo que el atacante central es capaz de tener a su disposición cientos o miles de equipos en espera de una orden para comenzar un ataque a gran escala (Reyes, 2011).

La Figura A26 muestra el esquema de cómo es que se lleva a cabo un ataque DDoS.

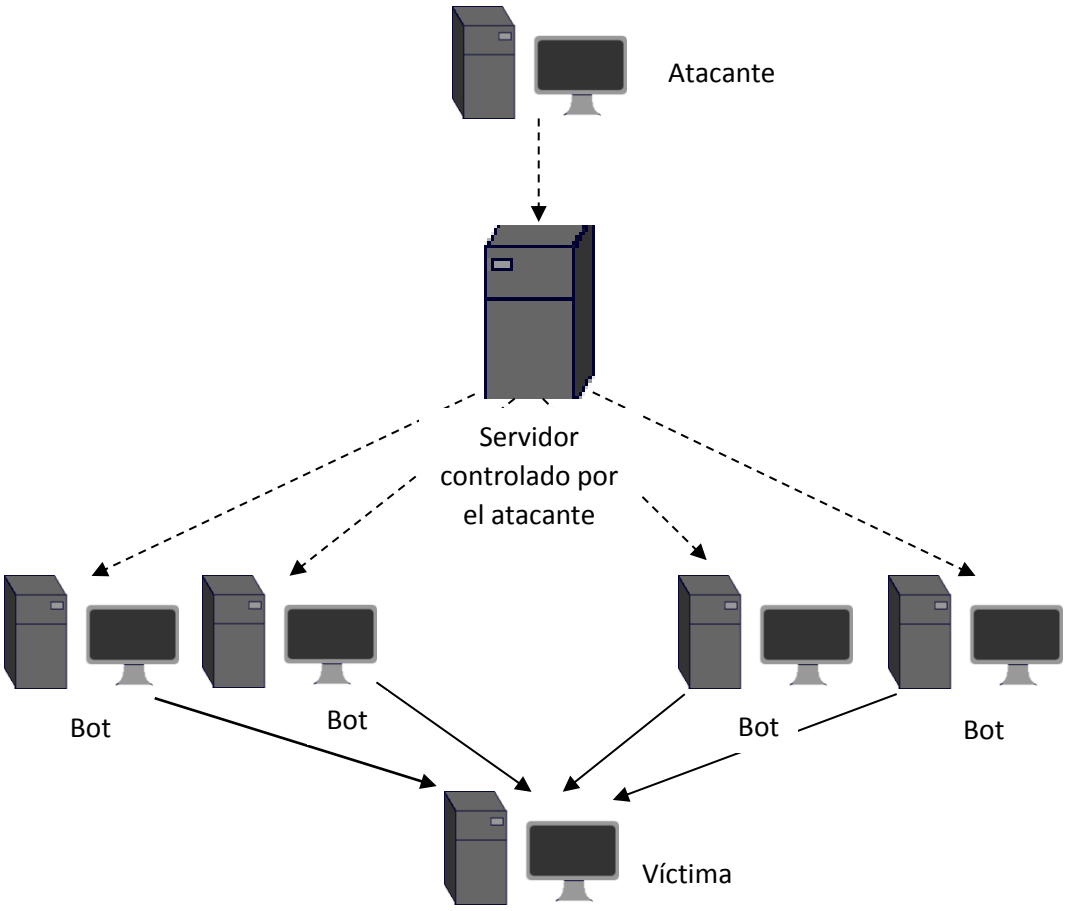



*Figura A26. Esquema de un ataque DDoS. Adaptada de* (Reyes, 2011)

Existen diferentes tipos de ataques DDoS y se pueden clasificar en 3 categorías: **los que afectan al ancho de banda** (SMURF, TCP SYN ACK *Reflection Flood*, UDP *Flood*, etc.) cuyo fin es saturar la capacidad de la red del servidor haciéndolo inalcanzable, **los que afectan los recursos** (ICMP *Echo Request Flood*, IP *Packet Fragment Attack*, IGMP *Flood* , etc.) que son aquellos que agotan los recursos del sistema impidiendo que pueda responder peticiones legítimas y por último los que **consisten en la explotación de fallos de software** (ping de la muerte) que aprovechan fallos en el software que pueden permitir tomar control del equipo o inhabilitarlo (OVH, 2017).

De todos los tipos existentes a continuación se describen los más comunes:

- **SYN Flood:** Es el más común de todos y se aprovecha del funcionamiento del protocolo TCP y su conexión de 3 pasos (*three way handshake*) que requiere una respuesta ACK para finalizar la comunicación la cual nunca llega, dejando así la conexión abierta y consumiendo recursos desproporcionadamente (Reyes, 2011).

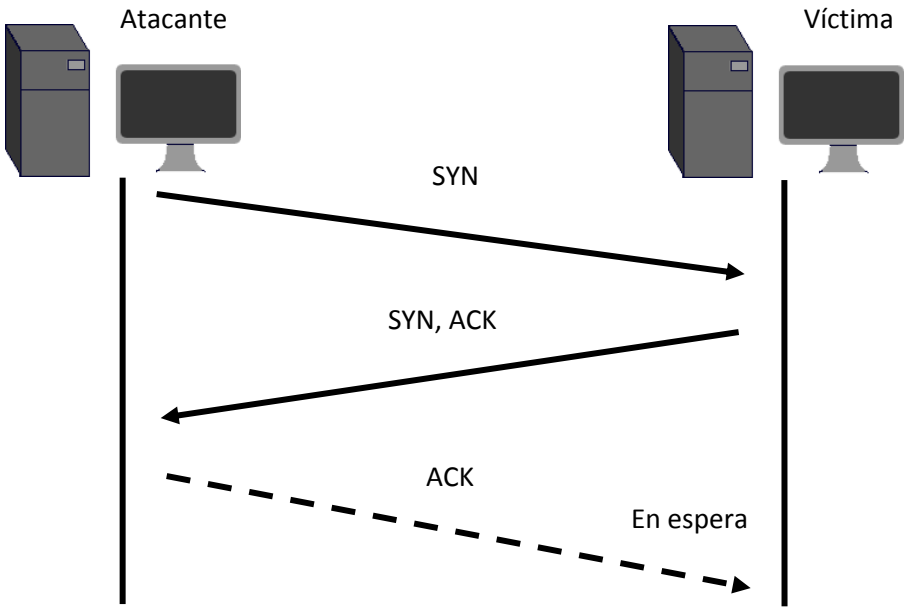



*Figura A27. Esquema de un ataque SYN Flood*. *Adaptada de* (Huawei, 2013)

- **Connection flood:** Aprovecha la dificultad de un servidor para atender un número excesivo de conexiones legítimas. El atacante envía *n* cantidad de peticiones las cuales el servidor atiende de manera adecuada, pero al ser tan grande el número de conexiones, éste comienza a tornarse lento, en cuanto caducan las conexiones el atacante vuelve a lanzar un gran número de peticiones, lo que da como consecuencia que usuarios legítimos no tengan acceso a los servicios brindados por la víctima del ataque (Reyes, 2011).
- **ICMP Flood:** El ataque de inundación de paquetes ICMP, también conocido como ping pong, consiste en saturar el servidor con “conexiones basura” las cuales impiden que las conexiones de clientes verdaderos se concreten. Pero ¿a qué nos referimos con conexiones basura?, pues bien, el atacante se vale del uso del protocolo ICMP enviando continuamente un número elevado de paquetes ICMP *echo request* (ping), a los cuales el servidor víctima responde con paquetes de tipo ICMP *echo reply* (pong) para indicarle que se encuentra disponible, sin embargo el atacante continúa enviando pings uno tras otro sin esperar la respuesta por parte del servidor, dando como resultado un alto consumo de recursos y generando una eventual pérdida del servicio (Reyes, 2011).

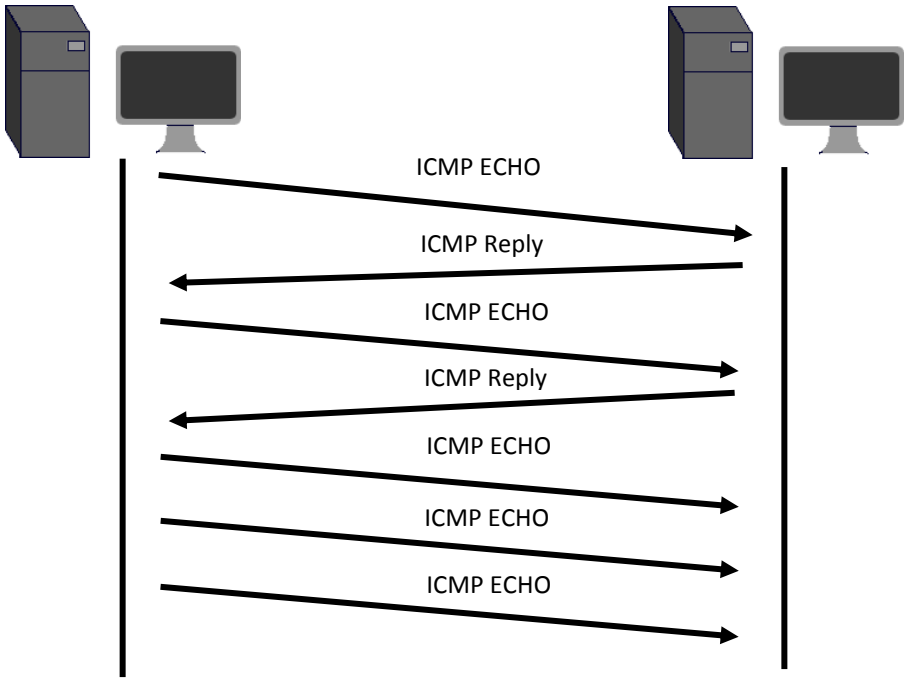



*Figura A28. Esquema de un ataque ICMP Flood. Adaptada de* (Huawei, 2013)

- **UDP Flood:** Usa el mismo principio que el ataque ICMP *Flood*, pero ahora empleando el protocolo UDP. De igual manera envía una enorme cantidad de paquetes UDP utilizando puertos aleatorios en cada uno causando que el equipo víctima compruebe ante cada petición a cada puerto, si hay alguna aplicación escuchando en destino; y en caso de no haberla responde con un paquete *Internet Control Message Protocol* (ICMP) de error de destino. Como se trata de un excesivo número de paquetes que el servidor debe comprobar, este proceso ocasiona que los recursos del servidor sean insuficientes, valiéndolo inaccesible (Reyes, 2011).

Finalmente, es posible hablar ahora sobre algunas de las diferentes estrategias que pueden ser utilizadas para mitigar los ataques DDoS. Se puede comenzar por tomar en cuenta medidas preventivas y contar con equipos como balanceadores de carga que ayuden a proteger al servidor crítico, desviando la carga de trabajo a varios servidores en lugar de sólo a uno; utilizar herramientas que capturen e identifiquen el tráfico que represente un potencial ataque y realizar el análisis correspondiente (identificar direcciones maliciosas, tipo de flujo de tráfico, puertos empleados, etc.) y en base a los resultados, realizar los bloqueos necesarios a nivel de red (Reyes, 2011). Por último, existen proveedores de dispositivos inteligentes e infraestructura de contención de ataques DDoS, cuya principal función es identificar el tráfico con características maliciosas y absorberlo o filtrarlo, dejando pasar únicamente el

tráfico legítimo hacia el servidor principal, cabe resaltar que esta última es la opción más costosa pero también la más efectiva (OVH, 2017).

En el capítulo correspondiente al reporte de actividades se explica a detalle cuál es el proceso empleado por parte del SOC para el análisis de un ataque DDoS.

## Lista de figuras, tablas, diagramas y gráficas

## Glosario

- **ACK:** Es un campo contenido en un paquete o segmento TCP y funciona como un acuse de recibo, es decir, mediante una respuesta ACK el servidor le confirma al cliente que ha recibido su solicitud para iniciar la conexión (CCM, 2017).
- **Appliance:** Es el dispositivo físico (hardware) que contiene la aplicación (software) de las herramientas de seguridad, para poder realizar configuraciones y la administración de las mismas (Cestero, 2008).
- **Botnet:** Es una red de computadoras conformada por máquinas infectadas con malware que permiten a un atacante tomar el control remoto de las mismas para ser utilizadas con fines maliciosos como pueden ser envío masivo de spam, propagación de virus, ataques DDoS, etc. (Norton, 2016).
- **CVE:** Es un diccionario de vulnerabilidades que son públicamente conocidas y que proporciona información importante sobre las mismas, como pueden ser su descripción general, versiones vulnerables de software, así como recomendaciones de prevención (ElevenPaths, 2014).
- **Dashboard:** Es una interfaz gráfica de usuario que permite la visualización de todos los detalles del monitoreo de la herramienta de seguridad, así como su administración y configuración.
- **DDoS:** Es el acrónimo de *Distributed Denial of Service* o "ataque de denegación de servicio distribuido", el cual consiste en enviar una gran cantidad de tráfico hacia un servidor desde múltiples puntos de conexión, con el fin de que deje de funcionar.
- **Dirección IP:** Es un conjunto de cuatro números del 0 al 255 separados por puntos que representan un identificador único que diferencia a un dispositivo dentro de un red (uServers, 2017).
- **DML:** Son las siglas de Data Manipulation Language o "lenguaje de manipulación de datos", el cual es un lenguaje utilizado en los gestores de bases de datos para realizar consultas y modificación de los datos contenidos en las DB, las operaciones que contempla el DML son Select (para realizar consultas), Insert (para agregar registros), Update (para modificar los valores de registros existentes en las tablas) y Delete (Para eliminar registros) (UAEH, 2017).
- **Falso positivo:** Es un evento que una herramienta de seguridad identifica como una posible actividad sospechosa, sin embargo el evento en sí no representa un incidente, ya que se trata de una actividad permitida.
- **ICMP:** Son las siglas del Protocolo de Mensajes de Control y Error de Internet, y su principal función es la de llevar un control en las comunicaciones, así como notificar si una comunicación entre los equipos de la red es exitosa o no, usando para ello mensajes de error, informando con

ellos a la fuente original para que evite o corrija el problema detectado (NEO, 2014).

- **Inline:** Es el proceso de respuesta implementado en las herramientas de seguridad que le permite actuar bajo demanda, es decir, al identificar una amenaza en el tráfico recibido, es capaz de ejecutar una acción de contención automáticamente.
- **Lista blanca:** Es una base de conocimiento donde se registra toda actividad que es permitida y que no representa una amenaza. Esta lista puede incluir registros de usuarios, tipo de tráfico, direcciones IP, etc.
- **Lista negra:** Contrario a la lista blanca, en la lista negra se registra toda la actividad que no es permitida y puede llegar a presentar afectaciones. También en las listas negras se registran las direcciones IP con mala reputación que han sido identificadas como maliciosas.
- **Malware:** Es todo aquel *software* o programa malicioso, cuyo principal objetivo es causar algún daño en un equipo de cómputo o en la información contenida en él (Ortega, 2009).
- **Match:** Se refiere al término utilizado cuando las características de cierto evento coinciden con las descritas en las reglas configuradas en la herramienta de seguridad, por lo que ésta última permitirá o denegará una acción según se haya configurado.
- **Parseo:** Es el término que se refiere a procesar los datos extraídos de las herramientas de seguridad, de tal manera que se conviertan en información útil para el usuario final. Para ello hay que realizar una depuración así como adecuaciones a los datos para que éstos se muestren en forma de tablas, gráficas, etc.
- **Ping:** Es el acrónimo de *Packet Internet Groper* o buscador de paquetes en redes y representa una herramienta de diagnóstico con la cual se puede verificar el estado de una conexión hacia un equipo remoto dentro de la misma red, en otras palabras, sirve para determinar si una dirección IP específica o host es accesible desde la red o no (Ramírez, 2016).
- **Plugin:** Los plugins, también conocidos como complementos, son programas que añaden funcionalidades específicas a un programa principal como es el caso de los navegadores web (Saberia, 2017).
- **Pruebas de penetración:** Son simulaciones de ataques informáticos empleando técnicas utilizadas por atacantes reales, con el fin de detectar vulnerabilidades y fallos en la seguridad del cliente, para posteriormente entregar un informe con los resultados encontrados. A las personas que realizan estas pruebas se les conoce como “hacker ético” (Guevara, 2012).
- **SOC:** Son las siglas de Security Operation Center o Centro de Operaciones de Seguridad, y es un centro de operaciones encargado del monitoreo y el análisis de actividad en la infraestructura de sus clientes en términos de seguridad informática. Sus principales funciones son la atención y mitigación de incidentes de seguridad en el menor tiempo posible.

- **Spam:** Es el término con el que se conoce al correo no deseado, generalmente proviene de remitentes desconocidos y es de carácter publicitario. Otra característica de este tipo de correo es que llega en grandes cantidades y puede ser utilizado para distribuir enlaces maliciosos o malware.
- **SYN:** Es un campo contenido en un paquete o segmento TCP y funciona como una solicitud inicial para establecer una conexión, es decir, mediante una solicitud SYN el cliente le pregunta al servidor si está disponible para iniciar una conexión (CCM, 2017).
- **TCP:** Son las siglas de *Transmission Control Protocol* o Protocolo de Control de Transmisión. Es un protocolo empleado en el modelo TCP/IP y permite que dos máquinas que están comunicadas controlen el estado de la transmisión y confirmen la buena recepción de datos, de esta manera los equipos involucrados pueden comenzar y finalizar la comunicación amablemente (CCM, 2017).
- **TI:** Es el acrónimo de Tecnologías de la Información.
- **Top:** Es un listado en el cual se registran los principales resultados o los más altos de un conteo. En el caso de un SOC pueden referirse a direcciones IP, ataques, horas de detección, etc.
- **UDP:** Son las siglas de *User Datagram Protocol* o Protocolo de Datagrama de Usuario. Es un protocolo no orientado a conexión, lo cual quiere decir que cuando una máquina envía paquetes a otra, el flujo es unidireccional y el destinatario recibirá los datos sin enviar una confirmación al emisor (CCM, 2017).
- **Vulnerabilidad:** Es un “punto débil” en un sistema, el cual puede permitir a un atacante aprovecharse de él para tener acceso o control del sistema vulnerable y realizar acciones ilícitas. Las vulnerabilidades pueden encontrarse tanto a nivel de hardware, software o sistema operativo (CodeJobs, 2012).

# Referencias


Ávila, D. A. (2016). *Enseñanza por competencias*. Obtenido de Anécdotas y reflexiones: https://aviladorador.wordpress.com/2016/12/13/ensenanza-por-competencias/#_ftn4

CCM. (Julio de 2017). *Diferencias entre los protocolos TCP y UDP*. Obtenido de CCM Website: http://es.ccm.net/faq/1559-diferencias-entre-los-protocolos-tcp-y-udp

CCM. (Julio de 2017). *Protocolo TCP*. Obtenido de CCM Website: http://es.ccm.net/contents/281-protocolo-tcp

Cestero, J. (25 de Septiembre de 2008). *Appliances de seguridad para la protección perimetral de la red empresarial*. Obtenido de PymesyAutonomos: https://www.pymesyautonomos.com/tecnologia/appliances-de-seguridad-para-la-proteccion-perimetral-de-la-red-empresarial

CISCO. (2005). *SERVICIOS CISCO PARA SISTEMA DE PREVEN CIÓN DE INTRUSIONES.* Obtenido de Cisco Website: http://www.cisco.com/c/dam/global/es_mx/products/servicios/docs/IPS_external_qa_clients_Spanish.pdf

CodeJobs. (7 de Septiembre de 2012). *Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?* Obtenido de CodeJobs: https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

Díaz, S. S. (Enero de 2013). *FIREWALL DE APLICACIÓN WEB - PARTE I*. Obtenido de Revista.Seguridad: https://revista.seguridad.unam.mx/node/2167

ElevenPaths. (3 de Enero de 2014). *Ocho siglas relacionadas con las vulnerabilidades*. Obtenido de Eleven Paths: http://blog.elevenpaths.com/2014/01/ocho-siglas-relacionadas-con-las.html

Foster, J. (2017). *IDS: Signature versus anomaly detection*. Obtenido de TechTarget: http://searchsecurity.techtarget.com/tip/IDS-Signature-versus-anomaly-detection

Grance, T., Karen, K., & Kim, B. (Enero de 2004). *Recommendations of the National Institute.* Obtenido de New Mexico Tech Website: http://infohost.nmt.edu/~sfs/Regs/sp800-61.pdf

Guevara, A. (Enero de 2012). *HACKING ÉTICO: MITOS Y REALIDADES*. Obtenido de Revista.Seguridad: https://revista.seguridad.unam.mx/node/2118

Huawei. (5 de Septiembre de 2013). *Huawei*. Obtenido de Huawei website: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000009653&partNo=100152

IMPERVA. (2010). *La historia de IMPERVA.* Obtenido de IMPERVA Website: https://www.imperva.com/docs/Imperva_Company_Overview_ES_LATIN.pdf

IMPERVA. (2017). *Web Protection – Introduction*. Obtenido de IMPERVA INCAPSULA Website: https://docs.incapsula.com/Content/introducing-incapsula/website-protection.htm

IMPERVA. (2017). *Web Protection - WAF Settings*. Obtenido de IMPERVA INCAPSULA Web site: https://docs.incapsula.com/Content/management-console-and-settings/waf-settings.htm

Murillo, J. V. (Diciembre de 2011). *PRINCIPIOS BÁSICOS DE SEGURIDAD EN BASES DE DATOS*. Obtenido de Revista.Seguridad: https://revista.seguridad.unam.mx/node/2236

Nathans, D. (2015). *Designing and Building a Security Operations Center.* Waltham, Massachusetts, Estados Unidos: ELSEVIER.

NEO. (2014). *El protocolo ICMP*. Obtenido de NEO Website: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html

Norton. (2016). *¿Qué es una botnet?* Obtenido de Norton Website: https://mx.norton.com/botnet

Operador. (18 de Enero de 2013). *¿Que es un SIEM?, ¿que es Prelude SIEM?* Obtenido de SeguridadX: https://www.seguridadx.com/que-es-un-siem-que-es-prelude-siem/

Ortega, O. R. (Mayo de 2009). *CÓDIGOS MALICIOSOS*. Obtenido de Revista.Seguridad: https://revista.seguridad.unam.mx/node/2096

OVH. (2017). *Principio anti-DDoS*. Obtenido de OVH Website: https://www.ovh.com/us/es/anti-ddos/principio-anti-ddos.xml

Polanco, M. (24 de Junio de 2010). *Arquitectura de eventos de seguridad*. Obtenido de Magazcitum: http://www.magazcitum.com.mx/?p=419&utm_expid=16248718-0

Polanco, M. (21 de Junio de 2010). *Los acuerdos de niveles de servicio (SLA) no sirven… ¿o sí?* Obtenido de Magazcitum: http://www.magazcitum.com.mx/?p=217#.WVxqBPmGPIU

Ramírez, T. (21 de Mayo de 2016). *¿Qué es el comando Ping y cómo funciona?* Obtenido de Computer Hoy: http://computerhoy.com/noticias/internet/que-es-comando-ping-como-funciona-42607

Reyes, A. (Diciembre de 2011). *¿QUÉ ES Y CÓMO FUNCIONA UN ATAQUE DDOS?* Obtenido de Revista.Seguridad: https://revista.seguridad.unam.mx/node/2138

Romero, D. (23 de Diciembre de 2013). *Correlación de eventos*. Obtenido de Seguridad de la información | Redes: http://www.davidromerotrejo.com/2013/12/correlacion-de-eventos.html

Ruíz, J. A. (Mayo de 2012). *DDOS ACTUALIDAD, TAXONOMÍA Y CONTRAMEDIDAS*. Obtenido de Revista.Seguridad: https://revista.seguridad.unam.mx/node/2123

Saberia. (2017). *¿Qué es un plugin?* Obtenido de Saberia: http://www.saberia.com/que-es-un-plugin/

Santillán Arenas, J. U. (Mayo de 2011). *EVOLUCIÓN DE LOS SISTEMAS DE DETECCIÓN, PREVENCIÓN Y ANÁLISIS DE INCIDENTES*. Obtenido de Revista .Seguridad: https://revista.seguridad.unam.mx/node/2158

Snyder, J. (2017). *Do you need an IDS or IPS, or both?* Obtenido de TechTarget: http://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPS-or-both

Soluciones en seguridad S.A. (14 de Mayo de 2017). *Acerca de nosotros*. Obtenido de Soluciones en Seguridad S.A. Web site: http://www.Soluciones en Seguridad.com/#About

Soluciones en seguridad S.A. (s/f). Capacitación-Servicios. Ciudad de México, México.

Soluciones en seguridad S.A. (s/f). Descripción del modelo de operación del Security Operation Center. Ciudad de México, México.

SuccessFactors. (Septiembre de 2017). *Organigrama*. Obtenido de SuccessFactors Website: https://performancemanager8.successfactors.com/sf/start/#/companyCheck

UAEH. (2017). *Lenguaje de Manipulación de Datos (DML)*. Obtenido de UAEH Website: http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro14/53__lenguaje_de_manipulacion_de_datos_dml.html

uServers. (2017). *¿Qué es una dirección IP?* Obtenido de uServers: http://web.uservers.net/ayuda/soluciones/dominios/que-es-una-direccion-ip_NTk.html