**Ingeniería en computación**



*Proyecto Integrador*

**Implementación de una solución para la gestión de eventos de seguridad de la información de una red de datos**

*Autores*

Sergio David Figueroa y Federico Nicolás Sepúlveda

*Director*

Mgter. Ing. Miguel Ángel Solinas

*Codirector*

*Dr. Fernando Menzaque*

# 

# Resumen

# Índice

[**Resumen**](#_kol2h6qgysv9) **3**

[**Índice**](#_klumoiel3imn) **3**

[**Índice de figuras**](#_q58k15c0fr3x) **5**

[**Índice de tablas**](#_7129zk3d87tq) **5**

[**Agradecimientos**](#_kbys14dyjqjf) **5**

[**Glosario**](#_clves114mmg4) **5**

[**Introducción**](#_msgxh4ei5l0s) **9**

[**Objetivo General**](#_78o1ww6a21kk) **10**

[Motivación](#_6in6ygfnp5ic) **10**

[**Descripción de Requerimientos**](#_6rai3ouvzmmy) **11**

[Requerimientos funcionales](#_y1qkb8o6l61l) 11

[Requerimientos no funcionales](#_m534rw324oov) 14

[**Marco Teórico**](#_xi0vbpfqj0fi) **15**

[Funciones y objetivos de un SIEM](#_j7bful4hljqi) 16

[Descripción del CSIRT y el rol del SIEM](#_wfyoyiexujrx) 18

[Incidentes de seguridad informática y el CSIRT](#_ybfg79jchlu1) 18

[Tipos de CSIRT](#_d18oh0f5jpik) 19

[SIEM dentro de un CSIRT](#_4mnu07zxs9y) 21

[Figura 2: Procesos de acción de un SIEM](#_i1jwb047kfjj) 23

[Estado del arte de los CSIRT en el mundo](#_sz22zkl49flf) 24

[Realidad de la Región y casos de uso](#_ya55npsxldf1) 28

[Estado de la ciberseguridad en Argentina](#_yfm8mk50o7e7) 33

[Demanda de ciberseguridad en Argentina](#_q5byxa3cwh8b) 36

[Amenazas y vulnerabilidades a las que debe responder un SIEM](#_vd2n41i1153w) 38

[Respuesta y manejo de incidentes](#_fnx7g8mem8wf) 39

[Cyber Kill Chain](#_kt1oahpqsa0q) 40

[Modelo Diamante](#_zhxyl0s9qodv) 42

[Esquema VERIS](#_lusa52ksqyyo) 44

[Comunidad a la que sirve el SIEM dentro de una Organización](#_iarwwbovvvid) 45

[Sistemas de monitoreo](#_hyxxsklvjvvv) 47

[Sistemas IDS: HIDS y NIDS](#_mp11hxs1x4yq) 49

[Infraestructura general de la red de una Organización](#_uvu0oic1fbe) 50

[**Iteración 1: “Análisis de herramientas disponibles”**](#_1g7acs2pbmlv) **51**

[Soluciones comerciales](#_qfy2fmcg4w6m) 52

[Soluciones gratuitas y de código abierto](#_6o7syte386lv) 56

[**Iteración 2: “Elección de las herramientas y arquitectura de red”**](#_e28gj5wmjpka) **59**

[Security Onion como sistema de gestión de eventos](#_6xxk90feqwsh) 59

[Arquitectura del sistema de gestión de eventos](#_d68wg7y9u8vq) 60

[Arquitectura de alto nivel](#_5tjrs2d54xrk) 60

[Arquitectura de despliegue](#_u3jf3sp8ta81) 61

[Tipo de Nodos](#_kn9i2cd2rftp) 61

[Tipos de Arquitectura](#_86kyhzv16i7a) 64

[Elastic, ElastAlert, TheHive y Cortex](#_eg8ed8fgbvvq) 67

[Recibiendo, procesando y visualizando eventos: La pila Elastic](#_g14uofnzjar) 67

[Analizando y clasificando eventos: ElastAlert](#_pqzcyedw8mey) 71

[El panel de control general: TheHive y Cortex](#_lq03o39atr0w) 72

[Automatizando acciones: TheHiveHooks](#_y03qr0todr02) 81

[Integración con los sistemas de detección](#_bto1am9p5t5z) 83

[Suricata, Snort y Ossec](#_5el7xg6aq71u) 84

[Arquitectura del despliegue](#_juvwd52ve8ho) 85

[**Iteración 3: “Configuración y despliegue en un ambiente de prueba”**](#_xdnrscy4e329) **86**

[Configuración del ambiente de prueba](#_5b96qatzvv33) 86

[Configuración del entorno de virtualización](#_vbv9ozuusue0) 87

[Definición y configuración de las redes a observar](#_4gy5pwndbx0t) 88

[Configuración inicial del sistema base](#_pr1m3xgke3pt) 90

[Instalación y configuración de Security Onion](#_dhdn30qeke8m) 90

[Instalación y configuración de TheHive - Cortex](#_5m89g5riahoi) 92

[Automatización de acciones](#_3p0estdaov1m) 94

[**Iteración 4: “Reportes de incidentes y acciones automáticas”**](#_a0fkq9pxl854) **95**

[Análisis de prioridades de los incidentes](#_csgr7xq0owzd) 96

[Automatización de acciones](#_d4bzhip9yjkb) 98

[**Iteración 5: “Testing y corrección para puesta a prueba”**](#_eojcxztr0qz5) **100**

[Test de detección de ataques varios](#_sozhocrqz06a) 100

[Test de reportes de incidentes](#_143fjw3fk3os) 100

[Test de acciones automáticas](#_qu0xa8uwm63h) 100

[**Conclusión**](#_e2lxx5wud3th) **100**

[**Futuros trabajos**](#_eomtxgzcuip2) **100**

[**Bibliografía**](#_jok3ar6e8r1a) **100**

[**Anexos**](#_mm3s3xi5bc29) **100**

# Índice de figuras

[Figura 2](#_i1jwb047kfjj)

# Índice de tablas

# Agradecimientos

# Glosario

CCNA: acrónimo en inglés de Cisco Certified Network Associate, un certificado de validación profesional emitido por la corporación Cisco para técnicos que operan sus productos.

CERT: siglas en inglés de Computer Emergency Response Team, en español equipo de respuesta a incidentes de computadoras. Término registrado comercialmente por la universidad estadounidense de Carnegie Mellon.

CICTE: siglas del Comite Interamericano contra el Terrorismo, entidad dependiente de la OEA.

CPU: siglas en inglés de Central Processing Unit, en español Unidad de Procesamiento Central.

Creative Commons:

CSIRT: siglas en inglés de Computer Security Incident Response Team, en español equipo de respuesta a incidentes de seguridad de computación. Es el equipo de profesionales, sistemas y toda la infraestructura (hardware y software) de detección y respuesta a incidentes de ciberseguridad de una organización.

DDoS: siglas en inglés de Denied Distribution Of Service, en español denegación distribuida de servicio.

DNS: siglas en inglés de Domain Name Service, en español Servicio de Nombres de Dominio, es un protocolo de red de la capa de aplicación.

Dirección MAC: siglas en inglés de Media Access Control, en español control de acceso a medios, es un conjunto de bytes que constituyen la dirección física (única) que identifica a un dispositivo conectado a una red.

EMCFFAA: Estado Mayor Conjunto de las Fuerzas Armadas Argentinas.

Firewall:

GNU: acrónimo recursivo en inglés de “GNU is Not Unix”, en español GNU No es Unix.

GPL: siglas en inglés de General Public Licence, en español licencia pública general, es un tipo de licencia GNU.

GUI: siglas en inglés de Graphical User Interface, en español Interfaz gráfica de Usuario.

HIDS: siglas en inglés de Host Intrusion Detection System, en español sistema de detección de intrusiones en un host o punto final.

IDS: siglas en inglés de Intrusion Detection System, en español sistema de detección de intrusiones. Es un componente de software destinado al procesamiento de firmas basadas en la información recolectada del tráfico de red, mediante una sonda colocada en un enlace de la infraestructura de comunicaciones de datos. Los IDS son un componente vital de un CSIRT debido a que realizan la identificación a priori de eventos en el tráfico de datos y su clasificación como un incidente.

InfoSec:

IPV4 e IVP6: siglas en inglés de los protocolos de Internet versiones 4 y 6, respectivamente.

IPS: siglas en inglés de Intrusion Protection System, en español sistema de protección de intrusiones.

LACNIC: siglas del Registro de Direcciones de Internet de América Latina y el Caribe, organización no gubernamental establecida en Uruguay.

Licencia GFDL:

Licencia AGPL:

Licencia APACHE:

Licencia BSD: siglas en inglés de Berkeley Software Distribution, licencia de software libre desarrollada en dicha universidad homónima de Estados Unidos.

Linux: núcleo de código (kernel) abierto de familias del mismo nombre de sistemas operativos de software libre.

Lockheed Martin:

Log: equivalente en inglés a “registro” en español. Término utilizado específicamente para registros de datos con un formato definido.

Malware:

MIT: siglas en inglés de Massachusetts Institute of Technology, universidad de los Estados Unidos cuyo nombre es usado para un tipo de licencia de código libre desarrollada en esa universidad.

MSSP: siglas en inglés de managed security service provider, en español proveedores de servicios de seguridad gestionados. Empresas que prestan servicios de seguridad informática a organizaciones.

NIDS: siglas en inglés de Network Intrusion Detection System, en español sistema de detección de intrusiones a nivel de red.

NIPS: siglas en inglés de Network Intrusion Protection System, en español sistema de protección de intrusiones a nivel de red.

NSM: siglas en inglés de Network Security Monitoring, en español monitoreo de seguridad de redes.

OEA: Organización de Estados Americanos.

RAM: siglas en inglés de Random Access Memory, en español memoria de acceso aleatorio.

Ransomware:

SaaS: siglas en inglés de Software as a Service, en español software como servicio, es un modelo de negocio de software a demanda.

SEM:

SIM:

SIEM:

SOC: siglas en inglés de Security Operations Center, en español centro de operaciones de seguridad de red.

SYN: bit usado en el protocolo TCP para indicar la sincronización del número de secuencia al comienzo de una comunicación utilizando el protocolo antes mencionado.

TCP: siglas en inglés de Transmission Control Protocol, en español protocolo de control de transmisión. Uno de los protocolos fundamentales en la comunicación de datos.

VPN: siglas en inglés de Virtual Private Network, en español red privada local

# Introducción

Este proyecto consiste en la implementación de un Sistema de Administración de Eventos y Seguridad de la Información (SIEM, por sus siglas en inglés) para la Universidad Nacional de Córdoba. Un SIEM consiste en varias herramientas como bases de datos, filtros para normalizar la información, tablero para visualizar los datos y generador de alertas entre otras. Por otro lado tenemos el monitoreo de la red en tiempo real que utiliza un Sistema de Detección de Intrusiones (IDS, por sus siglas en inglés). Este último envía los datos ya procesados al SIEM para que los almacene en la base de datos.

Además como se pretende que el SIEM funcione dentro de un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) se necesita integrar un gestor de incidentes. Este último sirve para tener un registro de los incidentes ocurridos, permite administrar las tareas del equipo de analistas, compartir y solicitar información con otros CSIRT entre otras funciones.

# Objetivo General

El objetivo de esta tesis es el desarrollo e implantación de un sistema SIEM dentro del proyecto general de la creación del CSIRT de la Universidad Nacional de Córdoba, con el fin de otorgar al mencionado centro de respuesta, el instrumento capaz de obtener, analizar y presentar datos sobre las amenazas detectadas por los demás subsistemas del CSIRT.

# Motivación

La tecnología y la digitalización de la información convierten a los datos en un activo muy importante de las organizaciones y de los individuos en general. Es fundamental saber cómo proteger los datos para evitar ser víctima de un ciberdelito o parte involuntaria de una ciber operación a gran escala. A pesar de que actualmente las técnicas de seguridad hacia los datos y la infraestructura de redes están en auge, las herramientas de seguridad como firewalls, IDS y otras que permiten prevenir ataques informáticos no son suficientes para mitigar y tener un seguimiento de actividades maliciosas o potencialmente maliciosas para lograr fortalecer la infraestructura y prevenir futuros incidentes. Resulta necesario contar con un sistema global que permita integrar un variado conjunto de utilidades que brindan soluciones puntuales y específicas, para crear una defensa inteligente y eficiente de los activos de información de una organización.

Actualmente la infraestructura de red y los sistemas asociados conviven en un ambiente de *saturación de la información* que implica un alto costo de procesamiento y ponen a prueba permanentemente a los sistemas encargados de la optimización de los recursos de hardware y software con los que cuenta la infraestructura, tales como uso de CPU y memorias RAM de routers, switches y servidores, el almacenamiento secundario donde el desafío de retener un ingente volumen de datos generados por el exponencial y siempre creciente tráfico de la red amenaza constantemente con el colapso de los medios disponibles sin importar su capacidad de almacenamiento, entre otros problemas, configuran una avalancha constante de información que sería imposible de analizar siquiera una parte de ella en un momento determinado utilizando métodos que impliquen el procesamiento en bruto. En esta situación, sería imposible distinguir un evento puntual y nocivo dentro de esta cantidad gigantesca de información que se genera permanentemente en la red, de un evento normal o de tráfico legítimo y en caso de identificar un potencial incidente, este tendría unas probabilidades muy altas de ser un falso positivo. Esto último es característico de los sistemas basados en el análisis de firmas, como los IDS, IPS o antivirus. Es necesario diseñar, desarrollar, implementar, configurar y probar un sistema capaz de orquestar un gran abanico de herramientas diseñadas cada una con un objetivo puntual, combinando las capacidades de todos sus subsistemas para identificar eficientemente las amenazas reales y responder en consecuencia, minimizando los falsos positivos y daños colaterales.

# Descripción de Requerimientos

## Requerimientos funcionales

* Envío de alertas sobre eventos destacables mediante servicios específicos: es necesario configurar servicios idealmente ya utilizados por la organización para enviar notificaciones sobre las detecciones de anomalías o potenciales incidentes por parte del sistema, para que los responsables del CSIRT y los departamentos que lo requieran, puedan tener conocimiento sobre las actividades detectadas y dar una respuesta adecuada.
* Analizar en busca puntos críticos de la red con mayor detalle al que se posee actualmente: es necesario que el nuevo sistema permita identificar los puntos críticos de la red y sus vulnerabilidades, así como el aporte de información sobre ellos que actualmente no es posible recoger con los medios de relevamiento y análisis de tráfico disponibles.
* Implementación de un sistema de notificaciones y pedidos para el manejo de incidentes: es necesario implementar un sistema de pedidos, o en su defecto adaptar el que la organización posea, para notificar al área responsable de la infraestructura o activo comprometido y que esta sea capaz de tomar las decisiones que considere apropiadas; tanto para mitigar las posibles consecuencias de un ataque como para fortalecer los activos. También será útil para constituir un registro sobre los pedidos realizados, obteniendo de esta manera un historial auditable.
* Automatización de respuestas a incidentes de seguridad: una vez detectado un evento y confirmado su clasificación como hostil, es necesario responder de la manera más rápida y eficiente posible. Además, muchos ataques consisten en una multitud de eventos que si dependieran de una respuesta individual a cada uno de ellos y realizada por un operador humano, sería imposible defenderse del tipo de ataques que consisten en miles de eventos lanzados al mismo tiempo, por ejemplo un intento de DDoS. Por otro lado, existen incidentes que se repiten periódicamente, como los de reconocimiento, en los cuales se puede aprovechar su naturaleza altamente repetitiva para desarrollar una respuesta automatizada y no distraer la atención de los operadores del sistema, permitiendo que estos se centren en tareas de mayor valor.
* Correlación de eventos: luego de detectar y eventualmente responder a incidentes, es importante contar con la capacidad de revisar las bases de datos y comparar los eventos actuales con los registros de incidentes del pasado, para establecer posibles correlaciones de firmas, tipo, objetivos u otros parámetros en tiempo real. Disponer de esta información es de gran importancia, ya que permite tener una visión y comprensión más profunda de la situación, lo que permitirá dar una respuesta mucho más efectiva.
* Visualización de los eventos en un tablero de mando: un aspecto fundamental de un sistema SIEM es la capacidad de integrar la información que envían los distintos sensores que están monitoreando y procesando tanto el tráfico en cualquier punto de la red (NIDS) como en los hosts (HIDS), de una manera concentrada, filtrada y ordenada para que los analistas puedan tener una visión clara y global de lo que está ocurriendo en todo momento, con la posibilidad de tener a disposición todos los detalles necesarios de los eventos que sean de interés. Además, debe ser posible tomar las decisiones haciendo uso de otros subsistemas del CSIRT, con sus respectivas acciones, desde el mismo tablero de mando.
* Normalizar eventos: el sistema debe ser capaz de filtrar los eventos provistos por los distintos sensores y normalizar la información para su posterior tratamiento, presentación y almacenamiento en las bases de datos respectivas.
* Almacenar eventos en una base de datos: el sistema debe almacenar la información normalizada de los eventos que procesa el SIEM, en una base de datos distribuida para posteriormente utilizar los registros en la correlación a demanda con otros eventos y proveer la capacidad de facilitar auditorías e investigaciones según sea requerido.
* Soporte para múltiples usuarios: el SIEM y sus subsistemas podrán ser operados por múltiples usuarios y con distintos niveles de privilegios, se trate de personal del SIEM, de otras áreas del CSIRT como de miembros de otras unidades de la organización que requieran tener acceso a registros puntuales.
* Recolectar registros: Es un requerimiento fundamental que el sistema pueda almacenar los registros de todos los eventos o incidentes que sean necesarios y oportunamente seleccionados para su almacenamiento en las bases de datos

## Requerimientos no funcionales

* Escalabilidad de la solución: el desarrollo propuesto para el SIEM debe tener una arquitectura tal que permita escalar o redimensionar el sistema de acuerdo a la evolución de la infraestructura sobre la cual debe estar desplegado. Para ello, debe considerarse un diseño basado en componentes, modular y en contenedores, para desplegar inmediatamente en una nube propia de ser necesario. Es necesario que la solución desarrollada admita en un primer momento, la capacidad de monitorear enlaces de 1 Gbps de ancho de banda.
* Trazado de los diagramas topológicos de la red de la organización: es necesario realizar un relevamiento de las conexiones de la infraestructura de red interna de la organización central, las de sus dependencias y la red entre las unidades geográficamente distribuidas si las hubiera. Deben incluirse la topología de las conexiones de salida a Internet.
* Manipulación de las bases de datos resultantes para su agregación bajo demanda: es necesario adecuar la estructura de las bases de datos de manera que se encuentre de la manera más optimizada posible para recibir los logs y toda la información relacionada a los eventos. Las bases de datos deben cumplir condiciones de alta disponibilidad, particionado automático y diferentes niveles de persistencia en disco.
* Utilización de software libre: la solución propuesta debe contemplar el uso, configuración y desarrollo de software libre, cuyo código fuente pueda ser estudiado, modificado y utilizado libremente por la comunidad. Puede implementar licencias GPL, AGPL, BSD, Apache, GFDL, MIT y Creative Commons, según sea el caso de cada uno de los sistemas, subsistemas y componentes individuales.
* Uso de un sistema operativo de código abierto: es necesario que el sistema implementado se ejecute sobre un sistema operativo de código abierto, pertenecientes a las familias Linux o BSD.
* Instalación automatizada: desarrollar una secuencia de comandos que permita al sistema poder desplegarse de manera totalmente automatizada y sistemática en todos los servidores destinados por la organización. Para ello, se deben emplear lenguajes y metodologías que permitan el desarrollo de un proceso de instalación autónomo, la secuenciación de tareas para lograr una secuencia de etapas confiable, predecible y segura; transparentar el proceso de instalación y configuración inicial, minimizando el número de parámetros necesarios a configurar cuando el sistema entre en servicio. Además, el mecanismo empleado no debe contar con agentes para evitar la explotación de posibles vulnerabilidades en el proceso o requerir eventuales actualizaciones. Las técnicas y tecnologías empleadas deben permitir la orquestación de todas las configuraciones y mantenimiento que requiera el sistema y sus componentes, así como la entrega continua de mejoras y actualizaciones.
* Inventariar y clasificar los activos de la organización: es necesario investigar y realizar un relevamiento de los activos con los que cuentan las infraestructuras de red y de datos a fin de clasificarlos para poder organizar una estrategia que permita el despliegue y el uso más eficiente de los recursos del SIEM y del CSIRT en su conjunto, para garantizar el monitoreo más amplio posible, eliminar puntos oscuros o desprotegidos y obtener el proceso de respuesta más eficiente a eventos de seguridad de la información.

# Marco Teórico

El proceso de monitoreo de la seguridad de una red de datos compleja requiere recopilar diferentes tipos de datos para detectar, verificar y contener exploits. Luego, la tarea principal del analista de seguridad cibernética es verificar acciones de explotación exitosa o intentos fallidos. Para ello se requieren tecnologías SIEM (*Security Information and Event Management*) que proporcionan informes en tiempo real y análisis de eventos de seguridad a largo plazo, como se muestra en la siguiente figura:

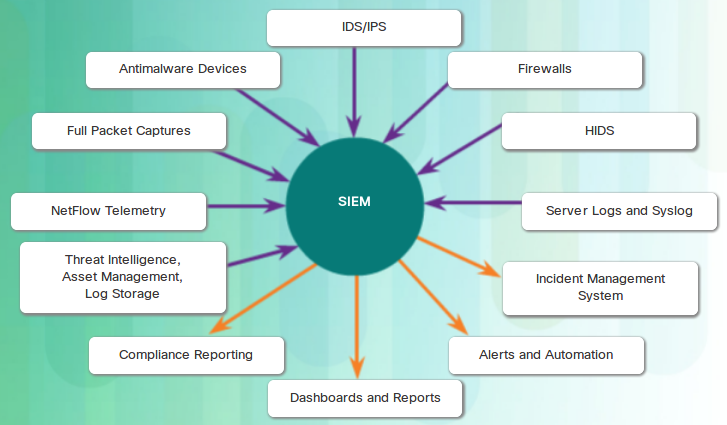


Figura 1. CCNA Cybersecurity Operations, Capitulo 11.2.2.6

*SIEM and Log Collection*

## Funciones y objetivos de un SIEM

Un SIEM combina por un lado las funciones esenciales de gestión de eventos de seguridad con las herramientas para la administración de información de seguridad, con el fin de proporcionar una vista completa de la red de la organización, utilizando las siguientes funciones:

* Recolección de logs: estos registros de eventos con origen en diferentes partes de la organización brindan información forense importante y ayudan a abordar, por ejemplo, requerimientos de informes de auditoría interna y/o externa.
* Normalización: el objetivo es asignar mensajes de logs de diferentes sistemas a un modelo de datos común, lo que permite a la organización analizar y correlacionar eventos, incluso cuando inicialmente se registran en diferentes formatos.
* Correlación: lo que se pretende es vincular registros y eventos de sistemas o aplicaciones dispares, acelerando la detección y reacción a las amenazas de seguridad.
* Agregación: aquí el objetivo es reducir el volumen de datos de eventos al consolidar, por ejemplo, registros de eventos duplicados.
* Informes: presentar los datos de eventos agregados y correlacionados para la supervisión en tiempo real y la generación de resúmenes a largo plazo, incluidos los tableros gráficos interactivos.
* Cumplimiento de auditorías: permite generar informes para cumplir con los requerimientos de regulaciones de cumplimiento, por ejemplo expresadas en políticas de seguridad o auditorías.

SIEM proporciona detalles sobre la fuente de actividad sospechosa:

* Información del usuario como su nombre, estado de autenticación, ubicación.
* Información del dispositivo, como fabricante, modelo, versión del sistema operativo, dirección MAC, método de conexión de red y ubicación.
* Información de postura tal como si el dispositivo cumple con la política de seguridad, si tiene archivos actualizados de antivirus y si se actualizó con los últimos parches del sistema operativo.

Con esta información, los analistas de seguridad de red pueden evaluar de forma rápida y precisa la importancia de cualquier evento de seguridad y responder a las siguientes preguntas críticas:

* ¿ Quién está asociado con este evento ?
* ¿ Tiene el usuario acceso a otros recursos sensibles ?
* ¿ Representa este evento un potencial no cumplimiento de algún aspecto de seguridad ?
* ¿ Se trata de un usuario importante con acceso a propiedad intelectual o información sensible?
* ¿ Está el usuario autorizado para acceder a aquel recurso ?
* ¿ Qué tipo de dispositivo está siendo usado ?

## Descripción del CSIRT y el rol del SIEM

### Incidentes de seguridad informática y el CSIRT

Un incidente de seguridad informática se puede definir de manera diferente en todas las organizaciones. En general, un incidente de seguridad informática es cualquier acto malicioso o sospechoso que viole una política de seguridad o cualquier evento que amenace la seguridad, confidencialidad, integridad o disponibilidad de los activos, sistemas de información o red de datos de una organización. Aunque esta definición puede considerarse vaga, estos son algunos incidentes comunes de seguridad informática:

* Código malicioso
* Negación de servicio
* Entrada no autorizada
* Robo de dispositivos
* Escaneos o sondas maliciosas
* Violación de la seguridad
* Infracción de cualquier elemento de la política de seguridad.

Cuando ocurre un incidente de seguridad, una organización necesita una forma de responder. Un CSIRT es un grupo interno que se encuentra comúnmente dentro de una organización que proporciona servicios y funciones para proteger los activos de esa organización. Este no solo responde necesariamente a incidentes que ya han sucedido. Un CSIRT también puede proporcionar servicios y funciones proactivos, como pruebas de penetración, detección de intrusiones o incluso capacitación en conciencia de seguridad. Estos tipos de servicios pueden ayudar a prevenir incidentes, pero también aumentan el tiempo de respuesta y mitigan los daños. En el caso de que un incidente de seguridad deba ser contenido y mitigado, el CSIRT coordina y supervisa estos esfuerzos.[1]

### Tipos de CSIRT

Es posible implementar un CSIRT en un conjunto muy diverso de organizaciones, lo que implica que el concepto puede extenderse y adaptarse según las demandas de las organizaciones. Por ejemplo, en grandes instituciones o corporaciones, un CSIRT típicamente estará centrado en investigar incidentes de seguridad, dejando la tarea de implementación de políticas de seguridad y monitoreo de incidentes (InfoSec) a un equipo dedicado a tal efecto. Por otro lado, en el caso de pequeñas empresas u entidades con pocos recursos, los CSIRT también son responsables de las funciones de Infosec, sus procesos, herramientas y políticas.   
 De esta manera, una posible clasificación de tipos de CSIRT según la organización que lo aloja, sería la siguiente:

Según su área de cobertura:

* CSIRT interno: proporciona manejo de incidentes para la organización en la que residen, por ejemplo estas pueden ser hospitales, bancos, universidades o diversas empresas. Este tipo de organizaciones son capaces de tener un CSIRT interno para el monitoreo de su propia infraestructura y servicios.
* CSIRT nacional: proporciona manejo de incidentes para redes nacionales y aquellos que afecten los intereses o activos vitales de un determinado país. Actúan al más alto nivel, tienen acceso a la infraestructura crítica tanto pública como privada y pueden estar compuestos por personal de las fuerzas de seguridad y / o fuerzas armadas.

Según su responsabilidad:

* Centros de coordinación : coordina el manejo de incidentes en múltiples CSIRT. Un ejemplo es el US-CERT. Según su definición, el US-CERT depende del gobierno de Estados Unidos y responde a incidentes importantes, analiza amenazas e intercambia información con otros expertos en seguridad cibernética y aliados de todo el mundo.
* Centros de análisis: utiliza datos de muchas fuentes para determinar las tendencias de actividad de incidentes. Las tendencias ayudan a predecir futuros incidentes y brindan alertas tempranas para prevenir y mitigar los daños lo más rápido posible. La comunidad VERIS es un ejemplo de un centro de análisis, que se encarga de estandarizar y normalizar un lenguaje para describir incidentes de ciberseguridad de manera que se pueda interpretar fácilmente al momento de compartir la información sobre un incidente.

Según su especialidad:

* Proveedores de servicios de seguridad gestionados (MSSP por sus siglas en inglés): brindan manejo de incidentes a otras organizaciones como un servicio de pago. Cisco, Symantec, Verizon e IBM son ejemplos de proveedores de servicios de seguridad administrados. Se trata de centros implantados en la organización cliente, de tal manera que estas no deben preocuparse de todas las fases que son necesarias para la creación de un CSIRT propio, tales como el diseño, planificación, implementación o mantenimiento. Los MSSP ofrecen distintos modelos de negocios según el caso, que van desde monitorear la infraestructura del cliente mediante servicios que corren en la nube de los proveedores (modelo de software como servicio o SaaS por sus siglas en inglés) hasta la implementación de soluciones mucho más costosas de hardware y software en el sitio del cliente (similar a modelos de soluciones llave en mano). En este último caso, los MSSP pueden incluso proveer personal que opere y / o integre las soluciones en el sitio del cliente, pudiendo actuar como un CSIRT interno de la organización.

### SIEM dentro de un CSIRT

El término SIEM fue acuñado en 2005 por los analistas Amrit Williams y Mark Nicolett de la compañía estadounidense Gartner, una empresa especializada en investigación y consultoría de incidentes de seguridad, unificando los acrónimos en inglés SIM (security information management) y SEM (security events management) para describir metodologías muy similares pero ligeramente diferentes de ciberseguridad. Esta superposición de tareas hizo evidente que un nuevo término podría englobar ambos conjuntos de funciones, con el fin de disponer de un único acrónimo que pudiese identificar a una plataforma capaz de resolver los objetivos de los sistemas predecesores.   
 Los sistemas SIM tenían como objetivo el proceso de recolectar, monitorear y analizar datos relacionados a incidentes de seguridad de la información con datos provenientes de registros (logs) generados automáticamente por los sistemas de computación.  
 En cuanto a los sistemas SEM, tenían a su cargo el proceso de centralizar los registros provenientes de distintas fuentes, tales como sistemas, puntos finales, aplicaciones o servicios, para mejorar las detecciones de eventos y la administración de estos últimos mediante un proceso de respuesta a incidentes estandard o implementado bajo un protocolo secuencial.  
 De esta manera, el nuevo acrónimo SIEM significa Administración de Eventos de Seguridad de la Información, por sus siglas en inglés. Como plataforma que combina las funciones de los sistemas anteriormente descritos, sus capacidades comprenden la siguiente lista de tareas:

* Recolectar, analizar y presentar de manera eficiente datos relacionados a la seguridad.
* Análisis en tiempo real de eventos de seguridad
* Generar reportes y almacenar datos relacionados a la seguridad
* Administración de niveles y tipos de acceso e identidad.
* Auditoría de registros
* Respuesta a incidentes y operaciones de seguridad.

|  |
| --- |
|  |
| *Figura 2: Procesos de acción de un SIEM* |

A medida que los sistemas de conexión se vuelven cada vez más complejos y deben soportar redes cada vez más heterogéneas con una creciente diversidad de dispositivos y servicios que a su vez incrementan las demandas de confiabilidad y disponibilidad de los activos de las organizaciones, también se multiplicaron las amenazas que intentan descubrir y explotar las posibles vulnerabilidades en todos los puntos de la infraestructura. Por esta razón, en simultáneo se está desarrollando un conjunto cada vez más numeroso y especializado de herramientas que intentan cubrir los permanentemente planos emergentes de análisis.   
 La situación descripta anteriormente se ejemplifica con los sistemas actualmente disponibles para monitoreo de puntos finales (HIDS), firewalls, monitoreo de activos de infraestructura de red como switches y routers, detección de malware en aplicaciones, detección y prevención de intrusiones en la red (NIDS y NIPS), alertas de pérdida de información, monitoreo de intentos de acceso a recursos y usuarios, vigilancia de archivos, nombres de usuario y hosts, etc.

En consecuencia, podemos observar que en un CSIRT existe una multitud de herramientas con un objetivo específico, que generan mensajes y alertas de distinto tipo de acuerdo a su misión puntual y es necesario un sistema capaz de procesar, filtrar, normalizar, presentar y almacenar toda esta información. Este es el objetivo del SIEM dentro del CSIRT y allí radica su importancia, ya que es necesario poder contar con un sistema que permita controlar a toda la orquesta de subsistemas que componen el área de monitoreo de un CSIRT.

|  |
| --- |
|  |
| *Figura 3: Capacidades Críticas de un SIEM* |

## Estado del arte de los CSIRT en el mundo

Existen diversos tipos de CSIRT funcionando actualmente alrededor del mundo, de una naturaleza pública o privada, con distinta área de cobertura ya sean puntuales (internos de una organización), regionales o nacionales y diferentes funciones principales, desde la búsqueda de vulnerabilidades, pasando por la investigación de amenazas, protección y monitoreo de infraestructura y activos críticos hasta la formulación de políticas públicas y educación ciudadana.   
 Los CSIRT privados generalmente son provistos por empresas especializadas, la mayoría provenientes de la industria de las telecomunicaciones que han derivado esfuerzos para cubrir un sector de mercado que es a su vez, un emergente de su sector industrial original. Es por esta razón, que las corporaciones han aprovechado su propio conocimiento de las infraestructuras que ellas proveen, para desarrollar soluciones a medida que se integran de forma nativa en sus productos ya existentes, tratando de esta manera de constituir un ecosistema de productos que se complementan entre sí y que en la mayoría de los casos representan soluciones propietarias y cerradas. Algunos casos son las corporaciones estadounidenses Cisco, AT & T e IBM, las europeas SAP cybersecurity, Siemens CERT, Airbus CyberSecurity and CSIRT y ElevenPaths, las empresas chinas Huawei, Alibaba y Tencent, las compañías rusas R-Vision y BI.Zone, entre otras.  
 Por otro lado, los CSIRT estatales son aquellos centros de respuesta a incidentes que tuvieron como origen una necesidad de los gobiernos de controlar y proteger sus intereses en el ciberespacio, tales como el monitoreo de la actividad en sus infraestructuras críticas de red: puntos de interconexión a la red global, servidores DNS nacionales, sistemas autónomos y todos los activos estratégicos que están conectados a las anteriores; centrales nucleares, hidroeléctricas, bases militares, puertos, sistemas de radares, universidades, sistemas de comunicación interna entre los diversos actores del Estado, etc.

El crecimiento de la demanda en la cantidad y calidad de las conexiones, asociadas con la expansión de los servicios públicos prestados en línea, el comercio electrónico y la consolidación de las comunicaciones digitales en todas sus formas como canal omnipotente de vinculación social de las sociedades contemporáneas, implicó el traslado de todas las consecuencias de la actividad humana al mundo digital. Es por ello que los CSIRT gubernamentales cobraron una importancia capital como instrumento de los Estados para su presencia y acción en internet.

Actividades como el comercio en línea y la banca digital han experimentado un crecimiento exponencial en la última década, trayendo aparejados el incremento de actividades ilícitas tales como estafas, fraudes, robo de identidades y cuentas bancarias. La irrupción de las redes sociales implicó el crecimiento de extorsiones, la organización de grupos criminales dispersos por áreas geográficas sin límite, el comercio de productos ilicitos, el terrorismo y una larga lista de acciones vinculadas a la naturaleza de las interacciones humanas. Los servicios digitales de procesamiento y almacenamiento de información en la nube se transformaron en la columna vertebral de las organizaciones que vieron volcada su actividad al mundo digital, generando en el proceso un sinnúmero de oportunidades para eventuales atacantes que buscan detectar y explotar las vulnerabilidades de los sistemas en los cuales descansa la infraestructura de estas organizaciones, con fines tan variados como obtener dinero a cambio de un rescate o sembrar el caos en intentos de activismo que derivan en ciberterrorismo.

El caso del hackeo a la infraestructura del sistema nacional de salud britanico con el ransomware Wannacry en mayo del 2017 es un ejemplo de un ciberataque que afectó a la atención y a la disponibilidad de los servicios de muchos hospitales y centros de salud, además de comprometer la información sensible de miles de pacientes. Otro ejemplo lo constituye el ataque de diciembre de 2015 a la red eléctrica de Ucrania por un grupo de hackers rusos que provocó un apagón masivo en todo el país durante varias horas, implicando pérdidas económicas cuantiosas y el desconcierto de la población. Por otro lado, el sabotaje de las centrifugadoras de uranio de Irán en el 2010 mediante el empleo del malware Stuxnet por parte de las agencias de inteligencias de Israel y Estados Unidos en combinación con una sofisticada operación de espionaje son ejemplos de distintos tipos de ataques a infraestructuras y activos críticos de un país, donde las amenazas pueden provenir de un espectro muy amplio de actores, desde simples individuos o grupos activistas movilizados por una causa, grupos organizados con fines de ciberterrorismo u otras formas de ciberdelito, hasta los intrincados y en ocasiones devastadores, ataques perpetrados por actores estatales de otro país.

Todo lo expuesto llevó al establecimiento de CSIRTs, centros de investigación, comandos especializados en ciberseguridad a cargo de fuerzas policiales y militares, incluso la creación de legislación específica sobre la materia e innovación de la ya vigente por parte de muchos países en lo que ya es considerado un asunto de la seguridad nacional. De esta manera, la Unión Europea dispuso la constitución, en el año 2004, de la Agencia para la Ciberseguridad de la Unión Europea (ENISA), dedicada a lograr un alto nivel de ciberseguridad común entre los países miembros de la Unión, contribuir a la definición de las políticas de ciberseguridad, mejorar la confiabilidad de los dispositivos de internet de las cosas (IoT por sus siglas en inglés), inducir a servicios y procesos a la implementación de esquemas de certificación en buenas prácticas de ciberseguridad y cooperar con los Estados miembros. En 2016, con la aprobación de la directiva NIS, en su artículo 12, se creó la Red de CSIRT de la Unión Europea. La agencia ENISA coordina esta red, compuesta por los centros nacionales y regionales de los países miembros, contando a treinta y nueve CSIRT en la red en 2020, aunque según la misma organización, en Europa hay 555 centros de respuesta a incidentes de ciberseguridad que pertenecen a fuerzas armadas, ad hoc de organizaciones auxiliares de la justicia, empresas privadas de servicios o internos de corporaciones industriales.

En los Estados Unidos de América, el US-CERT es un CSIRT responsable de coordinar la red del Sistema de Ciber Concientización Nacional (NCAS), el cual es el sistema nacional de ciberseguridad integrado, encargado de identificar, analizar y priorizar vulnerabilidades y amenazas emergentes. El objetivo del sistema es proveer a los ciudadanos de ese país de información sobre actualizaciones y recomendaciones de seguridad de manera gratuita para que estos puedan implementarlas en sus sistemas.

Durante el año 2020, el US-CERT identifico y alertó sobre las amenazas respecto a las actividades de Corea del Norte (programa HIDDEN COBRA), vulnerabilidades sobre el bootloader del sistema GRUB2, actividad maliciosa proveniente de actores estatales de China, intentos de intrusión en dispositivos IoT relacionados a infraestructuras críticas por parte de Rusia y un largo etcétera. El US-CERT depende del departamento de seguridad nacional (DHS por sus siglas en inglés); EEUU también dispone de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA), diversos centros militares y de investigación en universidades.

De manera similar a Estados Unidos y Europa, en muchos países del mundo existen CSIRTs gubernamentales y / o privados, tales como el Centro de Respuesta a Emergencias de Computación de China (CNCERT), el Centro Nacional de Ciberseguridad del Reino Unido (NSCS), el CERT-Bund de Alemania, el RU-CERT de la Federación Rusa, JPCERT de Japón, el Centro de Ciberseguridad Australiano (ACSC), el BruCERT de Bangladesh, KN-CERT de la República de Corea, el Centro de Coordinación de Respuesta a Incidentes de Seguridad de la Infraestructura de Internet de Indonesia (ID-SIRTII/CC), el MonCIRT de Mongolia, VNCERT de Vietnam, CERT.br de Brasil, CSIRT de Chile, colCERT de Colombia, CSIRTS.MX de Mexico, entre otros.

Es importante destacar que la mayoría de los CSIRTS / CERTS nacionales forman parte de redes y organizaciones internacionales con el objetivo de compartir información y coordinar acciones ante amenazas en el ciberespacio internacional o regional, tales como la mencionada ENISA, la red de CERTs de Asia Pacífico (APCERT) o la red global FIRST. En cuanto a los CSIRTS de América Latina en general y los de nuestro país en particular, serán objeto de un análisis detallado en las subsecciones siguientes.

### Realidad de la Región y casos de uso

Con el advenimiento de la internet comercial en todo el mundo a inicios de la década de 1990, nuestra región comenzó a incorporar sus primeros centros de respuesta a emergencias de computación en 1997, cuando inició sus operaciones en Brasil el primer centro de América Latina: el “CERT.br”. Dos años después, se crearía en nuestro país el “arCERT”, siendo el primero de su tipo en Argentina y el segundo en la región. Chile (2001), Uruguay (2008), Paraguay (2012) son algunos de los casos de la región en los que se han implantado CSIRT nacionales, pudiéndose observar la disparidad temporal en la adopción de políticas y acciones en el ámbito de la ciberseguridad en América Latina. Esto se puede apreciar con más claridad si comparamos la situación respecto de las decisiones en otros países del mundo: teniendo en cuenta que el primer CERT fue creado en EEUU por un proyecto conjunto entre la agencia de investigación para la defensa DARPA y la universidad de Carnegie Mellon en 1988, la red FIRST a inicios de la década siguiente y el establecimiento de CSIRT en países como Japón en 1996, podemos considerar que las iniciativas de Brasil y Argentina fueron contemporáneas a la de otras potencias tecnológicamente avanzadas del mundo. Sin embargo, la adopción en el resto de América Latina se extiende gradual y paulatinamente a lo largo de las dos décadas siguientes.

|  |
| --- |
|  |
| *Figura N. Fuente Ministerio de modernización* |

El caso más paradigmático de nuestra región lo constituye Brasil: el país más grande, poblado e industrializado de sudamérica fue pionero en la introducción de políticas de seguridad informática y en reconocer en su momento el impacto que las redes de internet tendrían en el futuro. Actualmente dispone de 33 centros dedicados a la vigilancia y detección de amenazas en el ciberespacio, entre los que se encuentran, además del anteriormente mencionado “CSIRT.br”, el “CTIR.FAB” de la Fuerza Aérea Brasileña, “CSIRT USP” de la Universidad de San Pablo, el “CSIRT Petrobras” de la corporación petrolera homónima, el “CCTIR/EB” del Ejercito Brasileño, el “CSIRT.globo” que atiende la red de la compañía de televisión Globo TV y el “CTIR gov” encargado de la red del gobierno federal, entre otros.

A nivel regional existen varias organizaciones dedicadas a la promoción, formación, investigación e implementación de políticas y recursos de ciberseguridad, de las cuales LACNIC y la OEA ocupan un lugar destacado.

La Organización de los Estados Americanos (OEA) constituye el principal foro político de la región y fuente de la cual emergen muchas de las políticas que se implementan transversalmente en el continente, específicamente desde 2004 cuando en la IV conferencia de la CICTE (Comite Interamericano contra el Terrorismo, dependiente de la OEA) realizada el 29 de enero de ese año en Montevideo, Uruguay, se propuso por primera vez el marco para la creacion de una red interamericana de CSIRT de vigilancia y alerta. Este propuesta contemplaba el desarrollo de una red de puntos nacionales de contacto entre los CSIRT con responsabilidad nacional (“CSIRT Nacional”) de los Estados miembros de la OEA, que “funcionará las 24 horas del día, los siete días de la semana, capaz de responder apropiada y rápidamente a las crisis, incidentes y amenazas relacionadas a la ciberseguridad”. Se especificaba que la colaboración en esta red debería ser capaz de:

* realizar diagnosticos rapidos y precisos de un problema
* difundir rápidamente alertas de ataques reales sucediendo en la comunidad internacional;
* difundir rápidamente alertas de vulnerabilidades detectadas en la comunidad internacional;
* alertar a la comunidad mundial de actividades sospechosas y apoyar colaboraciones que investiguen y diagnostiquen esas actividades;
* proveer información para las estrategias de mitigacion y remediacion que combatan los ataques y amenazas; y
* minimizar la duplicación de los esfuerzos de análisis entre los equipos

El documento afirma que “la colaboración ayuda a equilibrar el conocimiento técnico que existe entre los equipos para limitar el daño y asegurar la operación continua de los servicios críticos". Para ello enuncia los principios que deben regir esta red panamericana de CSIRT:

* Indigena: El programa debe ser operado y controlado por entidades propias de cada nación participante, designadas por sus respectivos gobiernos.
* Sistémico: El sistema debe operar de forma multifacética, requiriendo una fuerza de trabajo entrenada y en alerta, compartir información regularmente en torno a las amenazas y vulnerabilidades actuales, re-evaluando e implementando constantemente las mejores prácticas y una apropiada interacción con los hacedores de las políticas públicas.
* En marcha: debido a la inherente evolución diaria de Internet, cualquier programa exitoso debe ser mantenido y actualizado regularmente. La seguridad de internet no se logrará con un arreglo de una única vez.
* Explicable: la “seguridad” en la “ciberseguridad”. Las reglas estrictas en aspectos tales como la manipulación de la información deben ser comprendidas y practicadas o los usuarios podrían dejar de confiar y los esfuerzos que hacen al sistema más seguro se verían disminuidos, lo que sería contraproducente.
* Construir sobre acuerdos existentes: hay un conjunto de entidades preexistentes en el hemisferio que proveen servicios de ciberseguridad en mayor o menor nivel. Cualquier sistema nuevo debería construirse sobre esas instituciones preexistentes para evitar la duplicación e incentivar la participación activa.

En cuanto a la identificación de las organizaciones existentes, el documento hace referencia a la necesidad de afiliación a algunos de los foros y redes reconocidas a nivel mundial de la época, tales como el foro global FIRST, la implementación de certificaciones como los del Centro de Coordinación CERT (CERT/CC) de la universidad Carnegie Mellon y las recomendaciones vertidas en libros como “State of the Practice of Computer Security Incident Response Teams”, “Creating a Computer Security Incident Response Team: A Process for Getting Started” y “Handbook for Computer Security Incident Response Teams (CSIRTs)” todos del mencionado CERT/CC. Adicionalmente se hace mención a un programa del departamento de defensa de Estados Unidos de certificación y acreditación de proveedores de servicios para la red de computadoras de defensa.

Finalmente, el informe presentado en la IV Reunión Regular del CICTE instaba a los países miembros a tomar un curso de acción que consistía en: conducir un censo para identificar los CSIRT existentes -junto a sus membresías y los servicios que proveen-, establecer un consenso mínimo de los servicios que todos los CSIRT miembros de la red deben ofrecer, redactar una resolución para enviarla a la Comisión de Seguridad Hemisférica (CSH, organismo dependiente de la OEA) y a la Asamblea General de las Naciones Unidas instando a los Estados miembros a crear sus CSIRT, implementar un consenso de servicios y estándares similares a las prácticas en Europa y Asia, así como establecer un sistema de asistencia técnica e intercambio de información para los CSIRT y asegurar el financiamiento para todo el programa.

Otro actor relevante para nuestra región es el Registro de Direcciones de Internet de América Latina y el Caribe (LACNIC), una organización internacional no gubernamental establecida en Uruguay en el año 2002, cuya función es “asignar y administrar los recursos de numeración de internet (IPv4 e IPv6), números autónomos y resolución inversa para la región” [N]. Además de administrar ciertos recursos críticos de la infraestructura de Internet de América Latina, esta organización promueve el desarrollo de internet en la región mediante políticas activas de cooperación entre los países y organizaciones miembros (unas 10000 aproximadamente) en 33 territorios de nuestro subcontinente. LACNIC declara entre sus objetivos apoyar y defender los intereses de la comunidad regional así como colaborar en la generación de las condiciones para que Internet sea un instrumento efectivo de inclusión social y desarrollo económico en América Latina y el Caribe.

En cuanto al desarrollo de las capacidades de ciberseguridad de la región, LACNIC llevó a cabo los programas WARP (Alertas, Recomendaciones y Punto de Reporte e Intermediación, por sus siglas en inglés), el proyecto Amparo para la formación de recursos humanos capacitados en ciberseguridad y el desarrollo del CSIRT LACNIC, el objetivo del cual lo constituye la infraestructura crítica de la organización y la cooperación con los CSIRT de los otras organizaciones miembros en lo concerniente al reporte de incidentes.

|  |
| --- |
|  |
| *Figura N. Fuente Ministerio de Modernización* |

### Estado de la ciberseguridad en Argentina

Los orígenes de la seguridad informática en nuestro país pueden rastrearse al decreto 856/98 y a la Resolución SFP (Secretaría de la Función Pública, organismo dependiente de la jefatura de gabinete de ministros) 81/99 -en los años 1998 y 1999, respectivamente- que establecen la reorganización de la Subsecretaría de Tecnologías Informáticas y el “Reglamento de Operación del ArCERT", donde se indican los requisitos y condiciones de operación de la Coordinación de Emergencia en Redes Teleinformáticas - ArCERT, y las Políticas de Seguridad del mismo.

El objetivo principal del ArCERTera coordinar y colaborar en los esfuerzos orientados a elevar los umbrales de seguridad en los recursos y en los sistemas de información en el ámbito de la Administración Pública Nacional (APN). Para esto se estableció una estrategia de coordinación, asesoramiento y capacitación hacia los organismos públicos en la gestión de la problemática de seguridad.

Sus funciones [N] eran:

1. Proveer un servicio especializado de asesoramiento en seguridad de redes.
2. Promover la coordinación entre los organismos de la Administración Pública Nacional para prevenir, detectar, manejar y recuperar incidentes de seguridad.
3. Centralizar los reportes sobre incidentes de seguridad ocurridos en la APN y facilitar el intercambio de información para afrontarlos.
4. Actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa.

En el marco de las funciones nombradas, el ArCERT realizaba actividades de investigación de amenazas y nuevas soluciones disponibles, divulgación de incidentes y soluciones así como capacitaciones de seguridad en redes y seminarios de actualización periódicos.

El año 2011 marcó el comienzo de un largo proceso de reestructuración de los organismos del Estado Nacional relativos a la ciberseguridad, que incluyó el reordenamiento de estructuras internas, la creación de nuevas dependencias y el reemplazo o absorción de unidades preexistentes por las de nueva formación. Ese mismo año, mediante la resolución JGM (Jefatura del Gabinete de Ministros) Nº 580/2011 se creó el Programa de Infraestructuras Criticas de Informacion y Ciberseguridad, que declaró como finalidad “Impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las Infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran”.

En el año 2013 y mediante el artículo 1º de la Disposición Nº 2/2013 de la Oficina Nacional de Tecnologías de Información, se creó el ICIC-CERT que reemplazó al ArCERT. Este nuevo CERT heredaba parte de las responsabilidades del original, a la par que otros artículos de la referida disposición creaban nuevos grupos de trabajo especializados que ampliaban las capacidades, funciones y responsabilidades concentradas originalmente en el ArCERT, tales como el grupo ICIC - GAP (Grupo de Acción Preventiva, art. 3º) con funciones similares a las encargadas al ArCERT pero enfocadas a monitorear “los servicios que el Sector Público Nacional brinda a través de la red de Internet y aquellos que se identifiquen como Infraestructura Crítica para la prevención de posibles fallas de Seguridad”, el grupo “ICIC - GICI” (Grupo de Infraestructuras Críticas de Información, art. 4º) especializado en el desarrollo y aplicación de nuevas tecnologías para el monitoreo, simulación y respuesta a incidentes en la red de infraestructuras críticas, establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad para la protección de este tipo de infraestructuras, coordinar la implementación de ejercicios de respuesta ante la eventualidad de un intento de vulneración de estos activos, entre otras. Finalmente, se creó el grupo de trabajo “ICIC - INTERNET SANO” (art. 7º) con el objetivo específico de ocuparse de las tareas de difusión y capacitación que anteriormente le correspondía al ArCERT. En cuanto al programa de infraestructuras críticas, podemos mencionar la adhesión de la Universidad Nacional de Córdoba, cuando el 15 de Julio de 2014, mediante la resolución 1221 firmada por el Rector Tamarit, en su artículo N°1 “Hacer lugar a lo solicitado a fS.1 por la Prosecretaría de Informática y, en consecuencia, adherir al "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad"...”

El Estado Nacional siguió actualizando sus políticas en los años siguientes, creando nuevos centros de respuesta a incidentes y actualizando la normativa vigente. Algunos de los ejemplos son la creación del Comando Conjunto de Ciberdefensa de las Fuerzas Armadas, el MING-CSIRT del ministerio de Seguridad de la Nación, la Dirección Nacional de Ciberseguridad y sus correspondientes unidades de gobierno.



Por otro lado, los Estados Provinciales, universidades y empresas también han desarrollado e implantado CSIRTs en sus organizaciones. Algunos ejemplos de esto son el BA-CSIRT de la Ciudad de Buenos Aires, el CSIRT-NQN del gobierno de la provincia de Neuquén, CERT UNLP de la Universidad Nacional de La Plata o el que dispone NIC Argentina destinado a la infraestructura crítica de DNS. En el caso de las empresas, podemos mencionar a los CSIRT de las redes bancarias Link y Banelco.

#### Demanda de ciberseguridad en Argentina

Nuestro país, de manera análoga a los demás países de la región, ha experimentado un flujo continuo y creciente de incidentes de ciberseguridad a lo largo de las últimas dos décadas, incrementando de manera exponencial año a año el número de incidentes de todo tipo que afectan a individuos, empresas, universidades, infraestructuras críticas y a los organismos de diferentes niveles del gobierno. Este incremento exponencial en la demanda ha encontrado una respuesta cuanto menos lineal del Estado Argentino. Un ejemplo lo constituye los 1590 millones de ataques que sufrió el sistema bancario argentino en el año 2019 o los 187 millones de ciberataques entre enero y marzo del 2020 con un incremento del 131% solo para el mes de marzo, según la plataforma “Fortinet Threat Intelligence Insider Latin America”.

|  |
| --- |
|  |
| *Figura [N]: Cantidad de intentos de intrusión según la amenaza. Abril - Junio de 2020. Los tres primeros corresponden al troyano de puertas traseras “DoublePulsar Backdoor”, negociación de cifrados SSL anónimos e intentos de ataque contra una vulnerabilidad de divulgación de información en el servidor SMB de Microsoft Windows. Fuente: Fortinet Threat Intelligence Insider Latin America* |

Informes del gobierno nacional desde el 2016 anticipan esta tendencia, en particular el ministerio de modernización indicó en un informe que el país había registrado 5400 millones de dólares en pérdidas atribuidas a incidentes de ciberseguridad.

|  |
| --- |
|  |
| Porcentaje de tipos de ataques contra organizaciones durante 2016. Fuente: Ministerio de Modernización en su publicación: “El panorama de la ciberseguridad en números”, 2016. |

Según datos del Instituto Nacional de Estadísticas y Censos (INDEC) del 2016, el Producto Bruto Interno (PBI) de Argentina fue de 544.500 millones de dólares americanos, por lo que comparando este valor con las pérdidas estimadas en el informe del entonces Ministerio de Modernización, se observa que el costo relacionado a incidentes de ciberseguridad constituyó, aproximadamente, el 1 % del total de PBI de ese año. Este costo, enorme tanto en relación a la producción nacional como en forma cuantitativa, resalta la necesidad cada vez más importante de desarrollar políticas públicas activas en forma de inversiones en la ampliación de las capacidades de análisis y respuesta a amenazas de ciberseguridad en los organismos del Estado y las infraestructuras críticas, la promoción de iniciativas privadas junto a la concientización de los riesgos existentes, el fomento de investigaciones académicas y la formación de recursos humanos capaces de afrontar estos desafíos, junto a una legislación adecuada y actualizada, para responder a los cada vez más demandantes amenazas y complejos escenarios que implica la creciente actividad en línea de industrias, organismos del Estado, comercio y desarrollo de la sociedad en Internet.

## Amenazas y vulnerabilidades a las que debe responder un SIEM

Existen un conjunto cada vez más amplio, diverso, en permanente crecimiento y evolución, de tipos de vulnerabilidades y ataques que pueden afectar a los activos de una organización. Aunque es importante comprender la naturaleza de cada uno de los ataques, es tanto o más valioso reconocer cuando los sistemas de información están siendo atacados. Responder a preguntas como “¿cómo saber cuando hay un ataque en desarrollo?”, “¿qué hay que observar?”, “¿Cuales son los rastros que dejó el atacante?”, “¿Qué información es necesaria para responder a un incidente de ciberseguridad?” y otros interrogantes, es la tarea clave que debe resolver un sistema SIEM al momento de conectarse con los demás sistemas del CSIRT y los activos de la organización a proteger. La importancia de responder de la manera más adecuada y precisa a los interrogantes anteriores permitirán disminuir el tiempo y el costo del inevitable ciclo de realimentación (definición de reglas, número de falsos positivos, refinamiento de las categorías de alertas y eventos, registros a guardar, etc), necesario hasta lograr un sistema estable, eficiente y eficaz.

El primer paso en el proceso de operaciones consiste en analizar los activos a monitorear para determinar las vulnerabilidades presentes. Estas pueden estar tanto a nivel de punto final (bases de datos vulnerables, cifrados con protocolos superados, versiones desactualizadas de software, configuraciones inadecuadas, etc) como de infraestructura (protocolos, configuraciones de routers, firewalls), que permitan identificar no solo los puntos débiles del estado actual de la organización, sino también la necesidad de contar con sistemas de seguridad que reporten al SIEM en puntos críticos, como escáneres de vulnerabilidades o sistemas de detección de intrusiones (IDS por sus siglas en inglés). Es importante destacar que en el caso de los IDS, estos constituyen elementos desplegables del CSIRT.

Dentro de las vulnerabilidades frecuentes encontramos a protocolos desactualizados o la falta de políticas claras que permiten la utilización de protocolos con vulnerabilidades conocidas; en estos casos los registros (en adelante “*logs*”) de los routers deberían ser enviados al SIEM y filtrados desde ahi, para identificar las posibles vulnerabilidades del empleo de protocolos desactualizados en la infraestructura. De una manera similar, se pueden crear vulnerabilidades en sistemas seguros si se cometen equivocaciones durante su configuración, pruebas o mantenimiento, debido a errores humanos durante el proceso aunque también es posible que estos problemas puedan ser originados intencionalmente por un atacante. Ejemplos de problemas de configuración los encontramos en firewalls desactivados en servidores o servicios de web server en sistemas donde no debería estar un web server. Todos estos casos pueden subsanarse mediante el uso de filtros y sistemas de administración de configuraciones en el SIEM que auditen permanentemente sistemas críticos y generen reportes cuando existan cambios en ciertos parámetros específicos o archivos que puedan comprometer la integridad, estabilidad y seguridad del sistema.

## Respuesta y manejo de incidentes

En ciberseguridad, los actores de amenazas siempre desarrollan nuevas técnicas. Por ello constantemente surgen nuevas amenazas que se deben detectar y contener, para restaurar los activos y la comunicación lo más rápido posible. Muchos atacantes usan extorsión, fraude y robo de identidad para obtener ganancias financieras. La necesidad de defenderse constantemente contra estos nuevos ataques llevó a la creación de varios modelos de respuesta a incidentes. Los modelos y procedimientos de respuesta y manejo de incidentes incluyen entre los más conocidos:

* Cyber Kill Chain
* Modelo Diamante
* Esquema VERIS

La utilización de estos modelos, procedimientos de respuesta y manejo de incidentes no son necesariamente excluyentes, sino que es una gran ventaja emplear estos procedimiento y modelos de manera conjunta. A continuación se realizará un repaso por estos tres modelos en más detalle.

### Cyber Kill Chain

La *Cyber Kill Chain* fue desarrollada por Lockheed Martin para identificar y prevenir las intrusiones cibernéticas. Se compone de siete pasos, que ayudan a los analistas a comprender las técnicas, herramientas y procedimientos de los actores de amenazas. Al responder a un incidente, el objetivo es detectar y detener el ataque tan pronto como sea posible en la progresión de la *Cyber Kill Chain*. Teniendo en cuenta los siete pasos, es deseable que si ocurre un ataque se detenga cuanto antes, haga el menos daño posible y el atacante aprenda menos de la red objetivo.

|  |
| --- |
|  |
| *Figura N - Cyber Kill Chain* |

La *Cyber Kill Chain* especifica los pasos que debe completar un atacante para lograr su objetivo. Para la *Cyber Kill Chain* son los siguientes:

1. **Reconocimiento:** Los atacantes inician por la investigación, identificación y selección de objetivos. Esta información la obtienen a partir de sitios web, redes sociales, listas de correo electrónico y en general cualquier actividad que permita identificar el tipo de información que pueda ser útil.
2. **Militarización:** El objetivo de este paso es utilizar la información del reconocimiento para desarrollar un arma contra objetivos específicos de la organización. Para desarrollarla el diseñador utilizará el conocimiento de las vulnerabilidades de los activos que se descubrieron y construirá una herramienta que puede aprovecharlas.
3. **Entrega:** Durante este paso, el arma construida se transmite al objetivo utilizando un vector de entrega. Esto puede ser a través del uso de un sitio web, dispositivos USB extraíbles o un archivo adjunto de correo electrónico. Si el arma no se entrega, el ataque no tendrá éxito. El actor de amenaza usará muchos y diferentes métodos para aumentar las probabilidades de entregar la carga útil.
4. **Explotación:** Una vez que se propaga la amenaza, el atacante espera que el código malicioso sea ejecutado y por lo tanto explotar la vulnerabilidad elegida. Los objetivos de explotación más comunes son las aplicaciones, las vulnerabilidades del sistema operativo y los usuarios.
5. **Instalación:** Este paso es donde el actor de amenaza establece una backdoor en el sistema para permitir el acceso continuo al objetivo. Para preservarla, es importante que el acceso remoto no genere algún tipo de aviso a los analistas o usuarios de ciberseguridad. El método de acceso debe sobrevivir a través de exploraciones antimalware y el reinicio de la computadora para que sea efectiva. Este acceso persistente también puede permitir comunicaciones automatizadas, especialmente efectivas cuando se necesitan múltiples canales de comunicación al comandar una botnet.
6. **Mando y Control:** Teniendo el control del sistema, el atacante establece los canales de comunicación que a distancia le van a permitir controlar el sistema vulnerado.
7. **Acciones sobre Objetivos:** El paso final de Cyber Kill Chain describe al actor de amenazas alcanzando su objetivo propuesto. Esto puede ser robo de datos, un ataque DDoS o utilizar la red comprometida para crear y enviar spam. En este punto, el actor de amenazas está profundamente arraigado en los sistemas de la organización, ocultando sus movimientos y cubriendo sus pistas. Es extremadamente difícil eliminar al actor de amenazas de la red.

Si se logra detener al atacante en cualquier etapa, la cadena de ataque se rompe. Romper la cadena significa que el defensor frustró exitosamente la intrusión del actor de la amenaza. Los actores de amenazas sólo tienen éxito si alcanzan el Paso 7.

### Modelo Diamante

El *Modelo Diamante* se compone de cuatro partes y representa un incidente o evento de seguridad. Un evento es una actividad limitada en el tiempo restringida a un paso específico, donde un adversario utiliza una capacidad sobre alguna infraestructura contra una víctima para lograr un resultado específico.

|  |
| --- |
|  |
| *Figura N - Modelo Diamante* |

Las cuatro características principales de un evento de intrusión:

* **Adversario:** Persona u organización responsable de la utilización de una determinada capacidad contra la víctima, para lograr su propósito. Con frecuencia es difícil conocer la identidad del adversario.
* **Capacidad:** Herramienta o técnica que usa el adversario para atacar a la víctima.
* **Infraestructura:** Comprende las estructuras físicas y/o lógicas de comunicación que los adversarios utilizan para establecer y mantener el mando y control sobre sus capacidades de la víctima.
* **Víctima:** Objetivo del ataque. Sin embargo, una víctima podría ser el objetivo inicialmente y luego usarse como parte de la infraestructura para lanzar otros ataques.

El adversario utiliza las capacidades que tiene sobre la infraestructura para atacar a la víctima. Cada línea en el modelo muestra cómo cada parte llegó a la otra.

Las meta-características amplían ligeramente el modelo para incluir otros elementos importantes, ellos son:

* **Marca de tiempo:** Fecha / hora de inicio y final del evento, lo que podría permitir el análisis de patrones de comportamiento del adversario, periodicidad o recurrencia de los ataques, etc.
* **Fase:** Es análogo a los pasos en la Cyber Kill Chain; la actividad maliciosa incluye dos o más pasos ejecutados en sucesión para lograr el resultado deseado.
* **Resultado:** Es la utilidad particular que el adversario persigue cuando ataca a la víctima. Los resultados pueden documentarse como uno o más de los siguientes aspectos: compromiso de la confidencialidad, compromiso de la integridad y disponibilidad comprometida.
* **Dirección:** Indica la dirección del evento a través del modelo de diamante. Resulta importante cuando se considera la posibilidad de adoptar medidas de mitigación, especialmente en los eventos basados en red. Las direcciones de eventos se pueden dar en Adversario-a-Infraestructura, Infraestructura-a-Víctima, Víctima-a-Infraestructura, e Infraestructura-a-Adversario.
* **Metodología:** Se utiliza para clasificar el tipo general de evento, como escaneo de puertos, phishing, ataque de entrega de contenido, inundación de SYN, etc.
* **Recursos:** Son el o los recursos externos utilizados por el adversario para el evento de intrusión, como software, conocimiento del adversario, información (por ejemplo, nombre de usuario / contraseñas) y activos para llevar a cabo el ataque (hardware, fondos, instalaciones, acceso a la red ). Esto se puede mapear con la información que se obtiene en la etapa de reconocimiento de *Cyber Kill Chain*.

### Esquema VERIS

El Vocabulario para el Registro de Eventos y el Intercambio de Incidentes (VERIS por sus siglas en inglés) es un conjunto de métricas diseñadas para crear una forma de describir los incidentes de seguridad de una manera estructurada y repetible. VERIS fue creado para compartir información de calidad sobre eventos de seguridad a la comunidad, de forma anónima. La Base de Datos de la Comunidad VERIS (VCDB por sus siglas en inglés) es una colección abierta y gratuita de incidentes de seguridad informados públicamente en formato VERIS. La VCDB es una ubicación central para que la comunidad de seguridad aprenda de la experiencia y ayude con la toma de decisiones, antes, durante y después de un incidente de seguridad.

Como se muestra en la figura siguiente, en el esquema VERIS, el riesgo se define como la intersección de cuatro áreas. El de Amenazas, Activos, Impacto y Control. La información de cada área ayuda a comprender el nivel de riesgo para la organización. VERIS ayuda a determinar estas áreas utilizando incidentes de seguridad reales para ayudar a evaluar la gestión de riesgos.

|  |
| --- |
|  |
| *Figura N - Esquema VERIS* |

## Comunidad a la que sirve el SIEM dentro de una Organización

El SIEM tiene como fin servir dentro del área de tecnología de información (IT, por sus siglas en inglés) de una organización, como parte del equipo de respuesta a incidentes de ciberseguridad (CSIRT).

La gestión de IT asegura que todos los recursos tecnológicos y los empleados asociados son utilizados correctamente y de una manera que proporciona valor para la organización.

El departamento de *tecnologías de información* es el área a cargo de la administración de las redes locales, regionales, metropolitana o global de datos de toda la organización y de sus enlaces con Internet; administra las conexiones a Internet, ofrece soporte técnico y asistencia realizando el mantenimiento continuo del equipamiento tecnológico. Es tarea del área de IT realizar el mantenimiento de los servidores que permiten las conexiones y la red interna de la comunidad, como también los servidores web y de correo electrónico. Analiza y evalúa la adquisición de nuevo equipamiento en función de las necesidades de los diferentes usuarios.

Es su función, además, realizar el mantenimiento y control del filtro de tráfico de la red. Está integrado por profesionales de informática y electrónica, especializados en el manejo de redes y en la administración de sistemas operativos.

Los servicios que se prestan desde esta área son:

* Internet: Acceso, Internet II y acceso a Journals y publicaciones.
* Infraestructura de red: mantenimiento, soporte técnico delineado y trazado de la red inalámbrica y / o fibra óptica de toda la organización.
* Alojamiento de sitios web.
* Soporte de Hardware y software
* Soporte Técnico: tanto para las dependencias del Área Central como a técnicos de las Unidades Distribuidas de una organización.
* Bases de Datos y backups de estas: En períodos regulares, determinados motores de bases de datos cuentan con un sistema de réplica asincrónica la cual garantiza la pronta puesta en producción de un servidor que haya sufrido un desperfecto. Se pueden aplicar distintas políticas de backup: por ejemplo dos tipos de backups, uno generado a primera hora del día, con backups incrementales y otro diario que es encriptado y descargado en cada unidad distribuida de la organización.
* VPN
* Servicios web:
  + Instalación de sistema de gestión de contenidos para plataformas web (CMS por sus siglas en inglés) como por ejemplo Wordpress, Drupal, etc. y su soporte.
  + ERP (software de planeamiento de recursos empresariales) como SAP y su infraestructura
  + OJS (Open Journals System): Sistema para la administración de revistas y publicaciones de la comunidad, si lo hubiera.
  + OCS (Open Conferences System): Sistema para la administración de conferencias.

## Sistemas de monitoreo

El sistema de monitoreo de red (NSM por sus sigla en Inglés) en una pieza fundamental para la recolección de datos en un SIEM. Es fundamental conocer previamente la arquitectura de la red que se quiere monitorear, de esta manera se puede conseguir una posición estratégica y tener una mejor perspectiva sobre lo que ocurre en la red.

Un esquema general para monitorear la red es como se ve en la figura siguiente.

|  |
| --- |
|  |
| *Figura 5. Esquema básico de conexión de un NSM* |

Para la detección, la cual consiste en el proceso de examinar los datos recopilados y generar alertas en función de los eventos observados y los datos inesperados, en general, esto se realiza a través de algún tipo de detección de firmas, anomalías o estadísticas. Esto da como resultado la generación de datos de alerta.

La detección suele ser una función del software, y algunos de los paquetes de software más populares son Snort IDS y Bro IDS desde una perspectiva de sistema de detección de intrusiones en la red (NIDS), y OSSEC, AIDE o McAfee HIPS desde una perspectiva de sistema de detección de intrusiones de host (HIDS).

El SIEM utiliza datos de red y de host para realizar la detección en función de eventos correlacionados.

### Sistemas IDS: HIDS y NIDS

Como se mencionó anteriormente los IDS se pueden clasificar en dos versiones según dónde apuntan a monitorear la red.

Los HIDS se encargan de monitorear un host en particular y en caso de detectar alguna anomalía dentro del mismo, como algún paquete de red sospechoso, envía un log al servidor de log centralizado, informando los sucedido. Este servidor puede ser parte del SIEM.

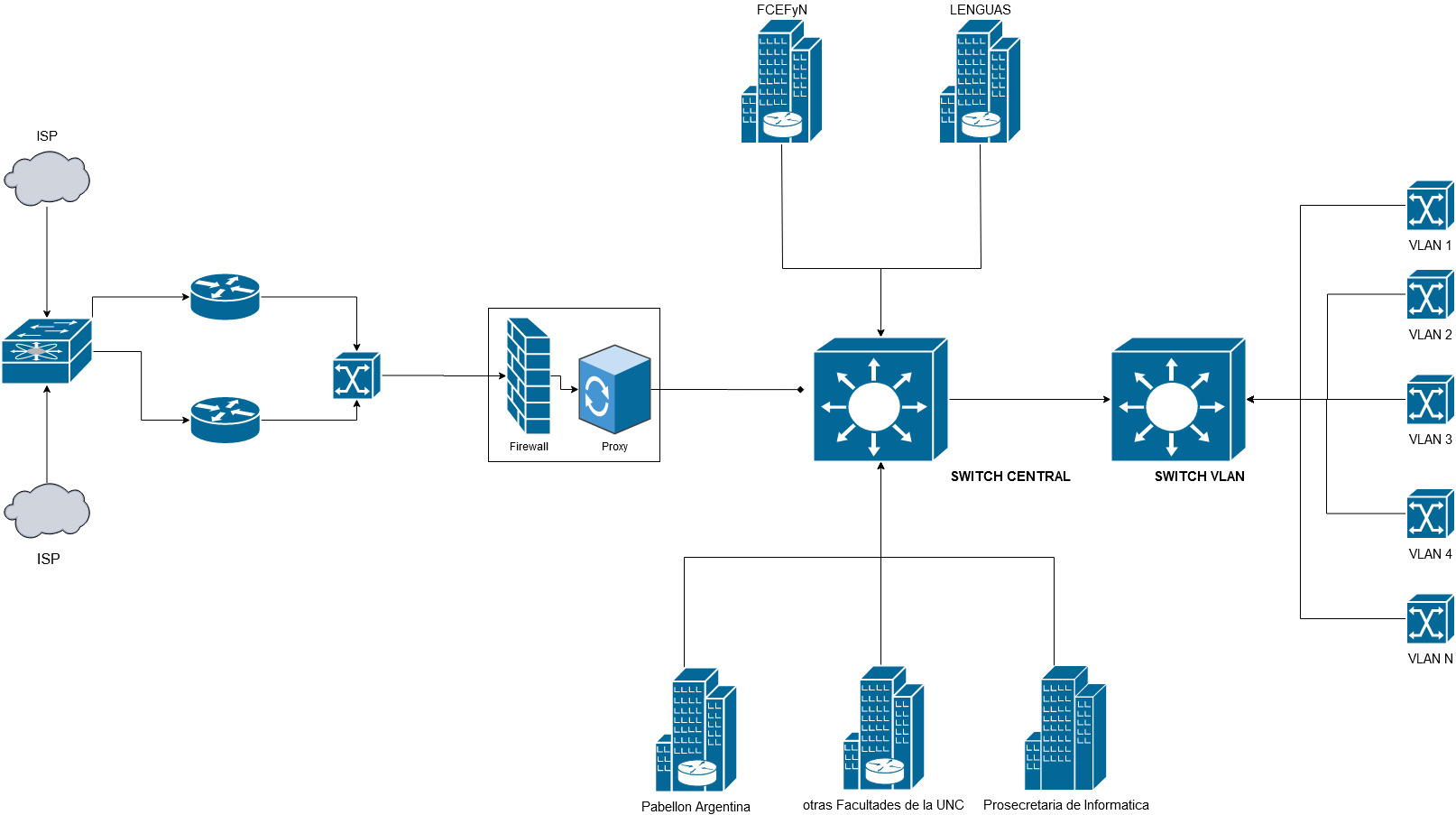
Por otro lado están los NIDS basado en la detección de actividad sospechosa a nivel de red, estos monitorean el flujo de la red en búsqueda de paquetes potencialmente maliciosos, a su vez al igual que el HIDS puede comunicar a un servidor dentro del SIEM, mediante logs, el evento detectado.

|  |
| --- |
|  |
| *Figura 6. Diferencias de monitoreo de datos entre un HIDS y un NIDS* |

## Infraestructura general de la red de una Organización

Generalmente las redes de las grandes organizaciones o de aquellas que están geográficamente distribuidas y cuentan con una infraestructura diversificada se las pueden describir como una topología estrella en la cual el sector de IT se encuentra en el centro y todas la sucursales, dependencias o unidades se conectan a esta ya sea para comunicarse internamente como para salir al exterior. Esta área cuenta con routers de borde que se conectan a distintos proveedores de servicios de Internet con conexiones redundantes para asegurar la conexión en caso de que se caiga uno de los enlaces. Por otro lado, la red global de estas corporaciones constituye un sistema autónomo, que incluso en ocasiones también podrían funcionar como proveedores de servicios de Internet.

Cada dependencia tiene asignada una red y una cantidad de host según el tamaño de la organización interna. Dentro de los establecimientos se segmenta la red mediante redes locales virtuales (VLAN), esta segmentación va a depender de las políticas internas, de las distintas áreas en las que se encuentre dividida y de los niveles de jerarquía que se empleen en la dependencia.



# Iteración 1: “Análisis de herramientas disponibles”

En los requerimientos no funcionales se mencionó que la implementación del SIEM debe realizarse con herramientas de software libre y gratuito. Sin embargo, en esta sección, se decidió analizar las principales soluciones que existen en el mercado, sean gratuitas, de software libre, de pago o código cerrado para tener una comparación más amplia y diversa.

Se realizó un relevamiento en sitios especializados y de referencia para el mercado mundial, con el objetivo de identificar las herramientas que actualmente dominan el mercado global de SIEM disponibles comercialmente. En el sitio web de Gartner se encontró un listado de los productos ordenados por valoración de los usuarios de dicha página. El resultado de los diez primeros productos junto a sus desarrolladores, es el siguiente:

|  |  |  |
| --- | --- | --- |
| 1) | QRadar SIEM | IBM |
| 2) | ManageEngine ADAudit Plus | ManageEngine |
| 3) | LogRhythm NextGen SIEM Platform | LogRhythm |
| 4) | LogPoint - SIEM | LogPoint |
| 5) | McAfee Enterprise Security Manager | McAfee |
| 6) | ArcSight Enterprise Security Manager (ESM) | Micro Focus |
| 7) | InsightIDR | Rapid7 |
| 8) | Elastic (ELK) Stack | Elastic |
| 9) | Splunk Enterprise | Splunk |
| 10) | Exabeam Security Management Platform | Exabeam |
| *Tabla N: Ranking Gartner de soluciones SIEM 2020* | | |

En base a toda lo información que se recolectó se procedió a clasificar las herramientas en base a su naturaleza: pagas o libres .

|  |  |
| --- | --- |
| **Soluciones Pagas** | **Soluciones Libres** |
| **Splunk** |  |
| **McAfee Enterprise Security Manager** |  |
| **AlienVault USM** | **Graylog** |
| **QRadar SIEM** | **Elastic (ELK) Stack** |
| **ManageEngine ADAudit Plus** | **AlienVault OSSIM** |
| **LogRhythm NextGen SIEM Platform** | **Security Onion** |
| **LogPoint - SIEM** | **Sweet Security** |
| **ArcSight Enterprise Security Manager (ESM)** |  |
| **InsightIDR** |  |

## Soluciones comerciales

En nuestro análisis de las soluciones comerciales disponibles, se decidió describir la situación del mercado internacional en términos de uso según los principales sectores industriales, la distribución geográfica de sus usuarios a nivel global y un énfasis en América Latina.

Respecto de los sectores industriales que hacen uso de sistemas de ciberseguridad y generan demandas de nuevas soluciones, se observó que el sector financiero a nivel mundial es el que lidera el consumo de soluciones SIEM, con la mayoría de los desarrolladores teniendo como clientes principales a empresas y organizaciones de ese sector. Esto se explica dado el alto nivel de digitalización de la banca y los servicios financieros, que por su masividad y naturaleza son objetivos prioritarios para cualquier atacante en el ciberespacio.

Finalmente, se hizo una comparación segmentada por características entre los principales productos SIEM del mercado internacional en base a las revisiones de sus usuarios que fueron recogidas por medios especializados y de referencia como “Gartner” y “Markets & Markets”.

|  |
| --- |
|  |
| *Tabla N. Valoración de las características* |

En esta tabla comparativa se observó que FortiSIEM y ADAudit Plus, de las compañías Fortinet y ManageEngine respectivamente, son las soluciones mejor valoradas.

|  |
| --- |
| Gráfico |
| *Figura N* |

En las figuras N y N+1 se aprecia que el sector financiero es el principal demandante a nivel global, siendo las industrias manufactureras y de la salud las otras dos que se destacan con diferencia respecto al resto del universo de consumidores. Esto se debe a que la automatización de la industria primero y su evolución al actual modelo de “industrias 4.0”, con cadenas de producción, montaje y ensamble distribuidas geográficamente alrededor del globo, el uso masivo de sensores, redes y datos intrínsecos a cada fase de producción; produjo la necesidad de soluciones de ciberseguridad para evitar incidentes que pudieran afectar las líneas de producción, daños a la maquinaria e infraestructura y sobre todo evitar en la medida de lo posible el robo de información crítica o secretos industriales. De manera análoga al sector manufacturero, las clínicas, hospitales y centros de salud han sufrido el impacto de la digitalización de sus procesos tanto en el hardware médico, el almacenamiento y distribución de la información como en la protección de los sensibles datos privados de los pacientes y la estricta normativa que los regula.

Se pudo observar que hay un marcada distribución en los mercados segmentados geográficamente, como QRADAR, LogPoint y FortiSIEM concentrando su demanda en Europa, el Medio Oriente y África; mientras que Enterprise Security Manager, InsightIDR y AlienVault USM lo hacen en América del Norte y FortiSIEM en Latinoamérica. Sobre nuestra región, en la figura N+2 se observó que FortiSIEM acapara el 34 % del mercado, seguido de Enterprise Security Manager, ADAudit Plus y NextGen SIEM Platform con un 17, 14 y 13 % del mercado, respectivamente.

|  |
| --- |
| Gráfico |
| *Figura N+1* |

|  |
| --- |
| Gráfico |
| *Figura N+2* |

## Soluciones gratuitas y de código abierto

Para el análisis de soluciones libres se observó primeramente que no se cuenta con muchas variedad de productos que cubran esta necesidad, algunos inclusos como el proyecto *Sweet Security* no cuenta con soporte desde el año 2017. Luego se encontró las soluciones que son propietarias pero a su vez tienen su versión gratuita también, el inconveniente de estas versiones es que no pueden escalar en caso que se requiera por parte de la organización. Las limitaciones van desde la cantidad de logs que pueden procesar, hasta el límite de almacenamiento de los mismos.

Al igual que en el caso de las soluciones pagas, se realizó un análisis de cuáles son los sectores en la industria a nivel mundial donde predominan las soluciones gratuitas y se observó un uso más intensivo en las áreas de servicios, estos se puede deber a que las áreas de servicios generalmente, las manejan entes estatales en conjunto con instituciones privadas y prefieran modificar dichas soluciones para que se adapten a sus estructuras organizativas. En las figura N+3 se puede observar el porcentaje de adopción por área en la industria.

|  |
| --- |
| Gráfico |
| *Figura N+3* |

Por otro lado, se realizó el estudio de la región y el porcentaje de uso de las soluciones y se pudo notar que la pila ELK en mayor o menor medida se utiliza en todas las regiones, como se puede ver en la figura N+4

|  |
| --- |
| Gráfico |
| *Figura N+4* |

Otra conclusión que se puede destacar del gráfico es que en américa del norte y del sur la solución SIEM más utilizada es AlienVault, mientras que en Europa, Medio Oriente y África es Graylog y en Asia/Pasifico optan usar la pila ELK.

También se puede remarcar que en Latinoamérica el segundo producto más utilizado después de AlienVault es Security Onion.

Cabe mencionar que tanto Graylog como Security Onion utilizan componentes de la pila Elastic. En el caso de Graylog, utiliza de base de datos a Elasticsearch que pertenece a dicha pila. Distinto es el caso de Security Onion, el cual utiliza la pila completa de Elastic ya que se trata de una distribución de Linux basada en Ubuntu que cuenta con un suite de diversas herramientas dedicadas a la ciberseguridad.

# Iteración 2: “Elección de las herramientas y arquitectura de red”

Como se describió en los requerimientos, la naturaleza de código abierto y libre del sistema base resulta una característica excluyente en la elección de la plataforma sobre la que desarrollamos la solución SIEM, así como los componentes integrantes de la suite elegida. Es por esta razón que elegimos Security Onion como plataforma base para el desarrollo del proyecto integrador, teniendo en cuenta sus características y herramientas durante la comparación con otras alternativas libres.

## Security Onion como sistema de gestión de eventos

|  |
| --- |
|  |
| Figura N: logo de Security Onion |

Nuestra elección de Security Onion como plataforma estuvo basada en sus características destacables respecto de otras soluciones, como el soporte de una amplia y activa comunidad, el desarrollo continuo de mejoras, actualizaciones y correcciones, su capacidad polimórfica y funcional de actuar como IDS, plataforma SIEM o cluster de almacenamiento; esto deriva en la posibilidad de desarrollar distintas arquitecturas de una manera fácil y asistida para el despliegue y la consiguiente optimización de los recursos de hardware y de red.

Otras de las propiedades sobresalientes es la capacidad de integración directa con un conjunto casi universal de los sistemas IDS disponibles, tanto libres como privativos; esto se ve facilitado por un paquete de configuraciones iniciales predefinidas, su elevado nivel de automatización en el momento de instalar y poner a punto mediante scripts la infraestructura inicial del sistema; tales como el almacenamiento, normalización y gestión de logs (pila ELK), los sistemas IDS y los demás nodos de la arquitectura, junto a los sistemas de gestión de usuarios.

## Arquitectura del sistema de gestión de eventos

### Arquitectura de alto nivel

|  |
| --- |
|  |
| Figura N + 1: Security Onion: Arquitectura de alto nivel |

En la Figura N + 1 se observa la distribución y flujo de datos entre los componentes principales (la pila Elastic) y secundarios (Curator, ElastAlert, freqServer y domainStats) de Security Onion; junto a los sistemas de detección IDS como Bro, Snort, Suricata, Syslog, etc. Se distinguen las conexiones con los puntos de administración de los analistas del SIEM / CSIRT y los servicios web externos para el envío y recepción de alertas, notificaciones, análisis de tráfico, entre otros. Un punto a destacar es que la pila Elastic se encuentra desplegada en contenedores Docker.

### Arquitectura de despliegue

Security Onion sigue un modelo cliente - servidor y admite múltiples arquitecturas de despliegue, recomendando tres modelos generales: monolítico, densamente distribuido y distribuido; donde el servidor central es también denominado ”nodo master” y los clientes pueden ser llamados “nodos Forward” o “sensores” según se trate de nodos con una versión de Security Onion especialmente configurada para cumplir una función de procesamiento de frontera o de sistemas IDS, respectivamente. En primer lugar se han detallado los tipos de nodos para posteriormente describir las distintas arquitecturas que los implementan.

#### Tipo de Nodos

Los tipos de nodos que componen las posibles arquitecturas son:

* Nodo Master: Este nodo ejecuta su propia copia de la base de datos Elasticsearch, con la que gestiona las búsquedas a través del cluster y estructurar los otros nodos en el momento de su despliegue. Lo anterior implica que puede realizar las configuraciones necesarias para los nodos de los tipos “densos” y los de almacenamiento, pero no los de sensores o Forward, por carecer estos últimos de elementos de una pila Elastic. Este nodo permite a un analista conectarse mediante un enlace de supervisión para realizar consultas de los datos.
  + Este nodo contiene los siguientes componentes:
    - Elasticsearch
    - Logstash
    - Kibana
    - Curator
    - ElastAlert
    - Redis
    - Wazuh / OSSEC
    - Sguild

Elasticsearch, Kibana y Logstash son componentes de la pila Elastic, que trataremos en la siguiente sección junto a ElastAlert. El objetivo de Curator y Redis es administrar y optimizar las bases de datos de los nodos de almacenamiento; Wazuh es un IDS y Security Onion lo utiliza para el monitoreo de sí mismo, configurando un sistema HIDS ad hoc propio, aunque es posible desplegarlo en otros nodos o puntos de interés. Sguild permite consultar eventos de una base de datos MySQL desde dentro de Security Onion y muestra los resultados en una GUI. Además, actúa como intermediario de otros componentes secundarios como Squert, del que detallaremos sus funciones y comportamiento en una sección posterior.

* Nodos Forward: este nodo cumple la función de procesar el tráfico y reenviar los resultados al nodo master. Los logs generados por Snort / Suricata y Bro son enviados mediante syslog al Logstash del nodo master utilizando un túnel ssh, donde finalmente son guardados en la base de datos Elasticsearch del nodo master, pudiendo éste optar a su vez por volver a enviar los logs hacia los nodos de almacenamiento. Los logs pueden ser consultados a través de una búsqueda en el cluster.
  + Los componentes de un nodo Forward son:
    - Zeek (sucesor de Bro)
    - Snort / Suricata
    - Netsniff-ng
    - Wazuh / OSSEC
    - Syslog-ng

Zeek, Snort / Suricata y Netsniff-ng son procesadores de tráfico (IDS), donde Snort y Suricata serán tratados en una sección posterior. Syslog-ng es utilizado para recolectar logs de los IDS y enviarlos al Logstash del master, donde serán procesados y tratados antes de ser escritos en Elasticsearch.

* Nodos Pesados: Es un nodo híbrido entre el nodo Forward y el nodo Master, que incluye todos los componentes del nodo Forward, además de una instancia completa de la pila Elastic. Los nodos pesados envían los resultados de las consultas de su instancia local de Elasticsearch a las solicitudes realizadas por el Elasticsearch del nodo master mediante un túnel de autossh.
  + Los componentes del nodo master son:
    - Elasticsearch
    - Logstash
    - Curator
    - Zeek
    - Snort / Suricata
    - Netsniff-ng
    - Wazuh / OSSEC
    - Syslog-ng (envía los logs a la instancia local de Logstash)

* Nodos de almacenamiento: su objetivo es extender las capacidades de almacenamiento y procesamiento del nodo master. Estos nodos despliegan una instancia local de la pila Elastic; de manera análoga a los nodos pesados, cuando se realiza una consulta por parte de la instancia Elasticsearch del nodo master, esta es procesada por la instancia local de la pila Elastic del nodo de almacenamiento y devuelta por un túnel autossh.
  + Los componentes del nodo de almacenamiento son:
    - Elasticsearch
    - Logstash
    - Curator
    - Wazuh / OSSEC

#### Tipos de Arquitectura

La versatilidad de disponer de múltiples arquitecturas permite adaptar la plataforma a las necesidades de la organización en la que se implante. A continuación, se describen cada una de las opciones posibles:

* Arquitectura monolítica: Consiste en un único servidor que ejecuta simultáneamente los componentes centrales o propios de un nodo master y los de un nodo sensor en conjunto con los componentes de la pila Elastic; es un modo híbrido y concentrado que no se recomienda para enlaces de red de alto rendimiento por los elevados requerimientos de hardware necesarios.   
  Este tipo de arquitectura se recomienda para propósitos de pruebas en laboratorio y en entornos de baja demanda de tráfico de red.

|  |
| --- |
|  |
| *Figura N + 2: Arquitectura monolítica de Security Onion* |

* Arquitectura densamente distribuida: consiste en uno o más nodos pesados conectados a un nodo master. Solo se recomienda en el caso de que no sea posible desplegar una arquitectura distribuida, ya que tiene las mismas deficiencias de rendimiento de la arquitectura monolítica y no es apropiado para entornos de producción y/o enlaces de red de alta velocidad.

|  |
| --- |
|  |
| *Figura N+3: Arquitectura densamente distribuida de Security Onion* |

* Arquitectura Distribuida: consiste en un servidor master, uno o más nodos Forward y uno o más nodos de almacenamiento. Es el tipo de despliegue recomendado en términos de eficiencia de requerimientos de hardware, balance de la carga y almacenamiento de datos y optimización general de los recursos disponibles en la organización.

|  |
| --- |
|  |
| Figura N+4: arquitectura distribuida de Security Onion |

### Elastic, ElastAlert, TheHive y Cortex

Security Onion incluye la pila Elastic, cuyos componentes son la base de datos Elasticsearch, Logstash quien se encarga de recibir, procesar, normalizar y agregar los datos resultantes a la base de datos; estos datos son visibles mediante Kibana. El proceso comienza cuando Logstash recibe los datos sin procesar provenientes de múltiples fuentes, son normalizados por este componente y enviados a Elasticsearch para su almacenamiento. Kibana permite consultar la base de datos mediante una interfaz gráfica de usuario y utilizar esa información para propósitos de análisis de amenazas.

ElastAlert es un framework que permite identificar y alertar sobre eventos anómalos o patrones de interés sobre los datos de Elasticsearch. También provee múltiples mecanismos para enviar alertas mediante distintas plataformas externas, tales como Slack, correo electrónico, JIRA, Telegram y muchos más. Tanto ElastAlert como los componentes de la pila Elastic están desplegados sobre contenedores Docker.

Es destacable que, aunque Security Onion cubre gran parte de los requerimientos de un SIEM, no posee los elementos que permiten completar un sistema de manejo y respuesta a incidentes; por esta razón y luego de una investigación sobre las alternativas posibles, se incluyó a TheHive y Cortex como complemento de Security Onion. TheHive permite la gestión de incidentes de manera detallada y la colaboración con otros CSIRT mediante el uso compartido de información sobre incidentes en tiempo real; mientras que Cortex hace posible la automatización de las respuestas y operaciones ante incidentes utilizando los datos enviados por TheHive.

### Recibiendo, procesando y visualizando eventos: La pila Elastic

Como se pudo observar en la *Figura 2* del marco teórico, luego de recolectar los datos provenientes de múltiples fuentes, es necesario normalizarlos y agregarlos a la base de datos; estas tareas son llevadas a cabo por los componentes de la pila Elastic, en este caso Logstash y Elasticsearch, respectivamente.

|  |
| --- |
|  |
| Figura N+5: Conexión de componentes Elastic |

Logstash es una tubería (en adelante “pipeline”) de procesamiento de datos gratuito y abierto del lado del servidor que ingesta datos de una multitud de fuentes, los transforma y luego los envía a su destino. Las fuentes de entrada admitidas por logstash son extremadamente amplias, como por ejemplo: syslog, STDIN, TCP, UDP, SNMP, IMAP, entre otras. Posteriormente, Logstash toma los datos sin estructura y los normaliza para crear conjunto ordenado mediante la identificación y conversión de la información a un formato común. Para realizar la tarea anterior, dispone de una gran variedad de filtros que facilitan el procesamiento general, independientemente de la fuente de datos. En este proyecto se utilizó a grok como filtro de las fuentes de información. Con los datos ya normalizados, es posible darles un formato específico para un destino en particular, ya que Logstash admite múltiples destinos para la etapa final del pipeline; desde una base de datos, archivos finales o servicios web. Security Onion, por defecto, almacena estos datos normalizados en un formato JSON en la misma pila Elastic, es decir la base de datos Elasticsearch.

Elasticsearch es una base de datos del tipo NoSQL distribuida y orientada al almacenamiento de documentos. Los datos normalizados provenientes de Logstash son documentos almacenados en índices en Elasticsearch. Cada índice está compuesto por uno o más shards (fragmento), por lo tanto un shard es un subconjunto de documentos, siendo el elemento básico de Elasticsearch y el que permite la escalabilidad del mismo. Un shard es también una instancia de un “índice de Lucene'', que indexa y almacena un documento en un segmento. Lucene es una librería desarrollada en Java para hacer búsquedas en una base de datos, constituyéndose en un motor de búsqueda que indexa y administra consultas en un conjunto de segmentos. La figura N+5 muestra la arquitectura de alto nivel del almacenamiento en Elasticsearch.

|  |
| --- |
|  |
| Figura N+6: Arquitectura de almacenamiento en Elasticsearch |

El índice y segmento correspondiente a un documento al momento de ser almacenado, corresponde a un identificador basado en el hash del contenido del propio documento a guardar. Elasticsearch dispone de una REST API con los métodos para administrar los documentos utilizando el identificador de estos. Otro aspecto a considerar en términos de rendimiento de Elasticsearch sobre el hardware de su host, es el tamaño de los shards. Estos se pueden definir en las configuraciones de Elasticsearch y su importancia radica en que un tamaño demasiado pequeño de los shards provocará un uso ineficiente del hardware, ya que estos deberán ser sometidos a un “merge” con una frecuencia mucho mayor a la habitual. Por el contrario, un tamaño demasiado grande de los shards demandarán tiempos demasiado largos de recuperación del cluster de Elasticsearch en caso de algún inconveniente.

Todos los datos almacenados en Elasticsearch pueden ser visualizados por Kibana, una interfaz gráfica perteneciente a la pila Elastic. Kibana permite visualizar los datos en gráficos circulares, de barras, histogramas, etc e interactuar con ellos; también es posible realizar análisis de ubicación cuando se disponen de los metadatos correspondientes mediante el complemento Elastic Maps, realizar análisis de series temporales de una manera rápida y sencilla, dispone de herramientas de inteligencia artificial, que mediante aprendizaje no supervisado permite detectar anomalías y patrones mediante las proyecciones sobre los datos. Otra de sus características es la posibilidad de realizar gráficos de correlación y entrecruzamiento, seleccionando campos de interés y filtros lógicos creados por el usuario. Es de destacar que para algunas de estas características es necesario la instalación de plugins complementarios y aunque en su inmensa mayoría son gratuitos, algunos pueden ser pagos ya que utilizan servicios web de la nube de los desarrolladores.

|  |
| --- |
|  |
| Figura N+7: Captura de pantalla de Kibana |

### Analizando y clasificando eventos: ElastAlert

A pesar de que Kibana permite consultar los datos almacenados en Elasticsearch y presentarlos de diversas maneras que resultan en una gran utilidad, carece de la capacidad de generar alertas cuando los datos coinciden con algun patron, especialmente cuando estos datos son escritos y consultados en tiempo real en la base de datos. Con este objetivo, la plataforma integra a ElastAlert, siendo un componente confiable, modular y simple de configurar. Su funcionamiento se basa en dos componentes principales: reglas y alertas; las primeras son utilizadas para comparar con los datos resultantes de las consultas que se hacen en forma constante a Elasticsearch, esta comparación consiste en hallar patrones o firmas definidas en las reglas dentro de los datos obtenidos de la consulta; si el resultado de la búsqueda es positivo, una alerta es disparada para notificar el evento.

Las alertas consisten en mensajes que permiten notificar a otro sistema con el objetivo de que este último realice una acción sobre las causas del evento que detectó la regla o bien informar a los analistas y/o responsables definidos. En cualquiera de los dos casos, las alertas pueden incluir toda la información recabada en un formato definido, tales como plantillas o cualquier arreglo configurado a tal fin.

Según la naturaleza de los eventos a clasificar, las reglas cuentan con un conjunto común de paradigmas de monitoreo, estos permiten identificar y generar alertas aprovechando las características de las anomalías al mismo tiempo que optimizan los recursos del resto del CSIRT en términos de hardware y atención de los analistas. Algunos de estos paradigmas se basan en el comportamiento, tales como la frecuencia que consiste en generar una alerta cuando se detectan N cantidad de eventos en un intervalo definido, el cambio de tasas de ocurrencia por arriba o abajo de un límite establecido como normal para un determinado tipo de eventos, cuando en los datos se encuentran presente campos que han sido previamente establecidos como parte de una lista blanca, negra u algún campo cuyo valor coincida con otros tipos de filtros, entre otros. Es posible definir y configurar tantas reglas como alertas sean necesarias.

### El panel de control general: TheHive y Cortex

Como se mencionó en las secciones anteriores, Security Onion requiere de otros elementos capaces de realizar la gestión integral de incidentes y sus respuestas, elementos que sean capaces de condensar y presentar información a los analistas del CSIRT encargados de monitorear y responder a las anomalías e incidentes detectados. TheHive es la herramienta que se eligió para esta tarea ya que es una plataforma de respuesta a incidentes de seguridad gratuita y de código abierto, cumpliendo así con uno de los requerimientos no funcionales del proyecto, referido al tipo de licencia y accesibilidad al código. Otra de las razones para la elección de esta plataforma en particular ha sido su escalabilidad y su integración con MISP, lo que permite compartir información sobre las amenazas detectadas con otros CSIRT de organizaciones aliadas. Las tres capacidades centrales son la elaboración de casos, la respuesta a estos y la anteriormente mencionada colaboración con otros SOC / CSIRT.

|  |
| --- |
|  |
| Figura N+8: Alertas recibidas en el panel de TheHive |

En cuanto a la elaboración de casos y tareas asociadas, estas se crean en base a las alertas recibidas (figura N+8), donde el primer paso consiste en la creación de un caso para luego asociar este a una o varias de las alertas presentes utilizando la plantilla disponible (figura N+9), posteriormente es posible agregar tareas asociadas al caso, las cuales se pueden asignar a distintos analistas; a continuación es posible sumar métricas y campos personalizados, reducir el tiempo de búsqueda y recopilación de datos así como automatizar algunas tareas de recopilación de antecedentes en el manejo de incidentes mediante el uso del tablero (dashboard) dinámico, tal como se observa en la figura N+10. En el proceso de creación del caso, thehive permite agregar cualquier otra información que se considere relevante, como etiquetas, archivos sospechosos de contener malware, etc a modo de evidencias.

|  |
| --- |
|  |
| Figura N+9: Plantilla para la creación de nuevos casos |

|  |
| --- |
|  |
| Figura N+10: Dashboard dinámico de TheHive |

Luego de la creación de un caso, es posible sumarle todos los “observables” que sean necesarios, donde los observables son todos aquellos campos que se pueden agregar de forma manual y que constituyen fuentes de información para analizar cada caso. Una vez configurado un caso, estos son examinados por scripts llamados “analyzers” que correlacionan y filtran los datos del caso contra los provistos por otras instancias MIPS u otras fuentes de información como la propia base de datos local, servicios de resolución DNS, plataformas como Shodan, VirusTotal, Google Cloud Visión, entre muchas otras. Los observables también se pueden obtener por datos de las alertas recibidas, los cuales son previamente configurados en ElastAlert. Como se mencionó anteriormente ElastAlert realiza consultas a Elasticsearch y con los resultados busca patrones de interés para realizar una notificación, obtenida esta última extrae datos que se consideran de interés para ser enviados a The Hive. Un ejemplo de esto puede ser un número de IP, tipo de protocolo, fecha que se generó el log, puerto de origen y/o destino. La alerta que llega a The Hive contiene todos estos datos, considerados observables.

Luego de que el caso fue creado o sobre la misma alerta, el analista puede dar curso a una respuesta mediante “responders” que son scripts en los cuales se encuentra la respuesta del CSIRT a la amenaza. Tanto los responders como los analyzers se encuentran bajo la responsabilidad de Cortex, el subsistema encargado de procesar los casos de TheHive. Al final de esta sección, se presentan los diagramas de casos de uso correspondientes a TheHive y Cortex.

|  |
| --- |
|  |
| Figura N+11: Algunos de los analyzers disponibles en Cortex |

|  |
| --- |
|  |
| Figura N+12: Ejemplos de responders utilizables en Cortex |

|  |
| --- |
|  |
| Figura N+13: Casos de uso de gestión de usuario y configuraciones de TheHive |

|  |
| --- |
|  |
| Figura N+14: Diagrama de casos de uso de alertas y casos |

|  |
| --- |
|  |
| Figura N+15: Casos de uso de gestión de usuario y configuraciones de Cortex |

|  |
| --- |
|  |
| Figura N+16: Casos de uso del tablero de Cortex |

### 

### Automatizando acciones: TheHiveHooks

Debido a que ciertos eventos tienen una elevada frecuencia de repetición y además su respuesta está perfectamente definida, sería de gran utilidad en estos tipos de ocasiones relevar a los analistas de la tarea que comprende tomar una alerta, elaborar un caso, ejecutar los analyzers y luego activar la respuesta correspondiente mediante los responders. Con este objetivo se implementó una automatización del proceso utilizando webhooks, que en el caso de TheHive se trata de una aplicación web (TheHiveHooks) que expone una REST API receptora de todos los cambios en TheHive y los envía hacia un punto final HTTP, donde un programa (en este caso Cortex) consume los datos recibidos. De esta manera, TheHive envía cada acción realizada en el (crear caso, actualizar caso, agregar tarea) vía los webhooks hacia el punto donde Cortex estará escuchando para actuar en consecuencia. Para esto fue necesario declarar la API mencionada anteriormente en el archivo de configuración *application.conf* de TheHive y luego desarrollar los *handlers* de los eventos para activar los responders apropiados.

La importancia de automatizar respuestas a ciertos tipos de incidentes no radica solo en optimizar el tiempo y la capacidad de atención de los analistas humanos en tanto en cuanto un recurso escaso y valioso, sino fundamentalmente en la capacidad de responder con eficacia y eficiencia a determinados arquetipos de ataques potencialmente devastadores como (por ejemplo) un DDoS, donde miles de eventos (incidentes) se producen en simultáneo y la capacidad humana de responder eficazmente a esta avalancha utilizando el protocolo descrito con anterioridad, es prácticamente nula. A continuación se presenta un diagrama simplificado de secuencia que involucra TheHiveHooks con TheHive y Cortex en la respuesta a un evento particular y la creación de un caso:

|  |
| --- |
|  |
| Figura N+17: Diagrama simplificado de secuencia del proceso de respuesta con TheHiveHooks y promover alertas a casos |

## Integración con los sistemas de detección

En secciones anteriores se mencionó que Security Onion cuenta con componentes para realizar tanto monitoreo de red (NIDS) como monitoreo de puntos finales (HIDS). Durante la configuración inicial del sistema se pueden especificar los NIDS a utilizar, para una configuración rápida de los sensores. Esto permite realizar una primera integración con el hardware disponible

### Suricata, Snort y Ossec

Suricata y Snort son motores de detección de amenazas en el tráfico de red. Ambos NIDS se basan en firmas o reglas para realizar la detección de amenazas, estas firmas son actualizadas constantemente conforme a la aparición de nuevos tipos de ataques, exploits y malware. Si bien estos NIDS son gratuitos y de código abierto Snort ofrece la versión paga, la cual cuenta con soporte para descargar las firmas actualizadas a la fecha. Por defecto Snort cuenta con las reglas básicas para la detección de amenazas bien conocidas.   
 Suricata, por otro lado, es desarrollado y mantenido por los colaboradores de la OISF, los cuales también dan soporte a las firmas ya que se actualizan las existentes y se agregan nuevas en forma permanente. Estas actualizaciones en las reglas son descargadas periódicamente mediante PulledPork, una utilidad que también es usada por Snort cuyo fin es descargar reglas y firmas desde distintos centros de investigación reconocidos en todo el mundo, como el SANS institute, Emerging Threats, entre otros.

A continuación se muestran las diferencias entre Snort y Suricata en una tabla comparativa:

|  |  |  |
| --- | --- | --- |
|  | Snort | Suricata |
| Desarrollador | CISCO | Open Information Security Foundation (OISF) |
| Lanzamiento | 1998 | 2009 |
| Lenguaje del código | C | C |
| Sistema operativo | Linux, Windows y Mac OS X | Linux, Windows y Mac OS X |
| Hilos | Monohilo | Soporte múltiples hilos |
| Soporte IPv6 | Si | Si |
| Reglas de Snort | Si | Si |
| Reglas de Emerging Threats | Si | Si |
| Formato de logs | unified2 | unified2 |
| Compatible con Aanval | Si | Si |

Por otro lado está Ossec (actualmente llamado Wazuh), que es un IDS orientado a hosts (HIDS). Al igual que los NIDS anteriores está basado en firmas para la detección de amenazas, además también es gratuito y de código abierto. Las reglas pueden descargarse del repositorio disponible en github.

## Arquitectura del despliegue

|  |
| --- |
|  |
| Figura N+18: Arquitectura de Despliegue |

En la imagen superior (Figura N+18) se muestra la arquitectura de despliegue del proyecto. La descripción, de izquierda a derecha, es: el proveedor ISP de conexión a internet y por consiguiente al exterior de la organización, el switch de capa 3 al que están conectadas las dependencias cuyos enlaces fueron seleccionados para ser monitoreados para este proyecto, los nodos Forward de Security Onion y un switch de la red interna del CSIRT. Se observa que los enlaces “Dependencia 1 - switch capa 3” y el de “switch capa 3 - nodo Forward de Security Onion Dependencia 1” tienen el mismo color; esto se debe a motivos de representar el hecho de que el switch capa 3 fue configurado para reenviar el tráfico entre el enlace de este y la dependencia 1 hacia el nodo Forward mencionado. Una situación análoga ocurre entre la Dependencia 2 y el nodo Security Onion Forward Dependencia 2.

El último eslabón de la conexión, el switch de capa 2, es el encargado de la red interna del CSIRT. A él se encuentran conectados las computadoras de los analistas y el nodo Master de Security Onion, los nodos Forward anteriormente mencionados y el servidor que aloja a TheHive y Cortex. Finalmente, los analistas pueden consultar y administrar los servidores correspondientes a los nodos Master y Forward de Security Onion así como al servidor que contiene a TheHive y Cortex.

# Iteración 3: “Configuración y despliegue en un ambiente de prueba”

En este proyecto se desarrolló sobre un ambiente de prueba primero y de producción después, sobre un servidor central y un sistema operativo de virtualización sobre el que se crearon un conjunto de máquinas virtuales, cada una alojando un servidor con nodos Forward, Master y el correspondiente a TheHive - Cortex. Se utilizó de guia los componentes, software y arquitectura de conexión entre ellos, mencionados en las iteraciones precedentes.

## Configuración del ambiente de prueba

El primer paso consistió en examinar los requisitos de hardware mínimos y recomendados por cada uno de los fabricantes de los sistemas y subsistemas elegidos, al mismo tiempo que se analizaron, por un lado, las demandas de tráfico de red en el ambiente de prueba y por el otro los requerimientos sobre los datos y capacidades que se esperan obtener del proyecto. Se procedió a realizar un diagrama topológico en la infraestructura objetivo, con esta información y los datos anteriormente mencionados, se procedió a realizar una estimación del hardware necesario para el servidor central que albergó las correspondientes máquinas virtuales de este proyecto.

Los requerimientos de hardware necesarios se incluyen a continuación discriminados según el tipo de nodo desplegado:

Nodo Master:

* Cantidad de CPU: 8 núcleos (vCPU), arquitectura X86-64 exclusivamente.
* RAM necesaria: a partir de 16 GB
* Almacenamiento: 1 Tb o lo necesario para cumplir la demanda de retención de logs.

Nodo Forward:

* Cantidad de CPU: 2 núcleos (vCPU) Para enlaces de 200 Mbps, por lo tanto para este proyecto fueron necesarios 10 vCPU (enlace de 1 Gbps). Arquitectura X86-64.
* RAM: desde 16 a 128 GB. En este proyecto utilizamos 32 GB.
* Disco: a partir de un tráfico de 50 Mbps se necesitan 540 GB debido principalmente a la acumulacion de pcaps. En este proyecto se utilizaron 200 GB ya que se contaba con restricciones de hardware disponible.

The Hive y Cortex:

* Cantidad de CPU: 8 núcleos (vCPU), arquitectura X86-64 exclusivamente.
* RAM: a partir de 8 GB
* Disco: a partir de 60 GB

Siguiendo el diagrama de la arquitectura de despliegue de la sección anterior, se optimizó al máximo el uso de los recursos del servidor disponible para permitir el despliegue de cuatro nodos: dos Forward y un Master de Security Onion, así como un cuarto conteniendo a TheHive y Cortex.

### Configuración del entorno de virtualización

Para el entorno de virtualización se utilizó VMWare, concretamente la suite vSphere HyperVisor v6.7.0 u3. Este sistema operativo basado en Unix permite gestionar los recursos de hardware disponibles, almacenar imágenes de distintos sistemas operativos y crear máquinas virtuales con estos últimos. Durante el proceso de creación de una máquina virtual, se selecciona el sistema operativo deseado y es posible asignar distintas cantidades de memoria principal, secundaria, cantidad de vCPU, número y tipo de enlaces de red, entre otros parámetros.

|  |
| --- |
|  |
| Figura N: Diagrama de una máquina virtual desde el punto de vista de un HyperVisor |

### Definición y configuración de las redes a observar

Se decidió monitorear dos dependencias en base a un análisis del ancho de banda de las dependencias existentes, por lo tanto se seleccionaron las que mayor volumen de tráfico registraban en función de un registro histórico y mediciones propias realizadas a lo largo de una semana. Las dependencias seleccionadas tenían un enlace con ancho de banda de 1 Gbps cada una, con velocidades promedio consideradas como la suma entre entrada y salida, entre 11,95 y 47,24 Mbps respectivamente; con picos poco frecuentes de 300 Mbps de tráfico, que no se contemplaron en los requisitos de hardware, por lo tanto habrá una posible pérdida de paquetes en estos casos. Se realizó un “port mirroring” de los puertos del switch capa 3 a los que están conectados estas dependencias y se los conecto con los respectivos enlaces de monitoreo de sendos nodos Forward de Security Onion.

Los gráficos a continuación muestran el volumen del tráfico medido en dos periodos de tiempo distintos: Durante un día (exceptuando las horas en las que la actividad era mínima) y a lo largo de una semana. Si bien estos registros que se presentan a continuación corresponden a una sola de las dependencias, la restante tenía un comportamiento análogo.

|  |
| --- |
|  |
| Figura N+1: Tráfico correspondiente a una dependencia, medido durante un día, obviando las horas donde este es casi nulo |

|  |
| --- |
|  |
| Figura N+2: Tráfico medido durante el periodo correspondiente a una semana |

## Configuración inicial del sistema base

Es posible instalar Security Onion en su versión 16.04 de dos maneras, sea mediante una ISO provista por los desarrolladores o bien mediante una serie de paquetes en una distribución Ubuntu. En este último caso será necesario contar con la distribución Ubuntu en su versión 16.04, ya que las distribuciones de Security Onion siguen a las distribuciones respectivas de Ubuntu; esto fue cierto hasta el año 2020 cuando se lanzaron nuevas versiones de Security Onion con soporte a otras distribuciones Linux: CentOS 7 y Ubuntu 18.04 y 20.04 aunque en el futuro se podrá desplegar en otros tipos de sistema Linux ya que desde la versión 2.x en adelante, el sistema se despliega en contenedores.

### Instalación y configuración de Security Onion

Como se mencionó en la sección anterior, existen dos maneras de instalar Security Onion: a partir de una imagen ISO o mediante paquetes / contenedores. Se eligió para este proyecto la segunda opción, el despliegue mediante paquetes de la distribución 16.04 de Security Onion ya que al momento del desarrollo de este trabajo integrador era la versión estable del sistema. Por consiguiente, se dispuso de un sistema operativo Ubuntu Server 16.04 con la particularidad de tener dos discos montados: el principal para el sistema operativo y el secundario para los datos recolectados en un directorio /nsm: índices en el caso de un servidor Master y capturas de paquetes o logs en el caso de un nodo Forward. Luego de finalizada la instalación de Security Onion, es necesario elegir el rol (Master o Forward) del nodo mediante el asistente y posteriormente realizar la configuración del mismo. Para esto último, se cuenta con la guia del asistente integrado que permite elegir y configurar las interfaces disponibles (observación o administración); en el caso de un nodo Forward, elegir el motor IDS (Snort o Suricata). El último paso consiste en elegir entre dos tipos de modo de funcionamiento: Producción o Evaluación.

|  |
| --- |
|  |
| Figura N+3: Asistente de instalación de Security Onion 16.04 |

|  |
| --- |
|  |
| Figura N+4: El asistente de instalación permite elegir el modo de despliegue |

Con el objetivo de cumplir uno de los requerimientos no funcionales del proyecto, que implica la automatización del despliegue (instalación y configuración) del sistema, se utilizó una herramienta de administración automatizada de servidores llamada Ansible en su versión 2.8.4 para la cual se desarrollaron scripts YAML conteniendo la secuencia de instalación de los paquetes, configuraciones, rol del nodo (Forward o Master) y librerías requeridas para el apropiado funcionamiento del sistema.

### Instalación y configuración de TheHive - Cortex

Para la instalación del gestor de incidentes, que tiene como componentes a TheHive y Cortex, se utilizó el sistema operativo Debian 10. En primer lugar se instaló TheHive, para ello fue necesario realizar la instalación previa de los componentes necesarios como las librerías de Java, Python y Elasticsearch; este último requirió una configuración en su archivo elasticsearch.yaml:

|  |
| --- |
|  |
| Figura N+5: Configuración añadida a elasticsearch.yaml para la instalación de TheHive |

Finalmente, los últimos pasos para la instalación de TheHive consisten en habilitar e iniciar el servicio de elasticsearch, agregar el repositorio que contiene los paquetes de TheHive, instalarlo y luego habilitar el servicio para poder iniciarlo.

En cuanto a Cortex, el proceso es similar al anteriormente descrito para TheHive, donde una vez descargados e instalados los paquetes de Cortex con su correspondiente secuencia de habilitación e inicio; se procedió a descargar del repositorio los responders y analyzers respectivos. Por último, se modifica el archivo de configuración de Cortex para indicar la ubicación del directorio que contiene los responders y analyzers mencionados anteriormente.

Posteriormente se actualizó la base de datos elasticsearch mediante la GUI web de Cortex, se creó un superusuario y luego las organizaciones donde se administrarán usuarios comunes y analyzers; es necesario crear un usuario con el rol de administrador de organizaciones. Las organizaciones tendrán habilitados y configurados determinados responders y analyzers según sea necesario.

El último paso del proceso consiste en comunicar TheHive y Cortex entre sí. Para ello se genera una API key en Cortex que será usada como parte de las modificaciones necesarias al archivo application.conf de TheHive. Las modificaciones completas que se realizaron al mencionado archivo se pueden apreciar en la siguiente imagen:

|  |
| --- |
|  |
| Figura N+6: Modificación al archivo application.conf de TheHive para la comunicación con Cortex |

## Automatización de acciones

El mecanismo elegido para automatizar las acciones fue mediante webhooks, para ello fue necesario implementar un entorno de virtualización en el mismo servidor donde se encuentran alojados TheHive y Cortex. Para ello se optó por utilizar el módulo de python “venv”, lo que requirió la instalación de Python 3.6 como primer paso. En segundo lugar se modificó el archivo application.conf de TheHive que se mencionó en la sección anterior para permitir la comunicación con el puerto del entorno de virtualización. En tercer lugar se verificó que en el nodo Master de Security Onion las reglas de ElastAlert tengan los campos necesarios configurados como observables ya que estos serán necesarios posteriormente dado que en TheHive están creados los observables que esperan esta información (source\_ip, destination\_ip, source\_port, destination\_port, alert, classification, category, etc).

Satisfechos los pasos anteriores, la instalación siguió los siguientes pasos:

1. Se creo una carpeta con el nombre webhooksenv
2. Un entorno virtual fue creado y activado en la mencionada carpeta
3. Se procedió a instalar las librerias necesarias: Flask, Gunicorn, Wheel, Request y Netaddr.
4. Se desactivo el entorno virtual y se habilitó en el firewall el puerto 5000
5. Se agregaron y modificaron valores al archivo de parámetros que utiliza webhooks.
6. Se inició y comprobó el estado del servicio.

Finalmente, se modificaron los archivos de configuración de TheHive y Cortex para actualizar la información necesaria referida a los webhooks.

# Iteración 4: “Reportes de incidentes y acciones automáticas”

En Security Onion y otros sistemas, el elemento descriptor que identifica y procesa a cada definición de incidente en particular es la regla. Las reglas comprenden una serie de campos que describen con precisión la naturaleza de un incidente dado y por lo tanto, existen tantas reglas como amenazas en circulación.

Cuando un nuevo malware es descubierto por el equipo de algún CSIRT con la capacidad de investigación suficiente o reportado a un laboratorio apropiado para este fin, es posible realizar un estudio de sus características y una vez identificadas estas últimas, proceder a crear una regla y agregarla al repositorio correspondiente para que otros CSIRT actualicen sus IDS con esta nueva definición y así contar con un filtro (la regla) que permita detectar este malware. Las reglas tienen un conjunto de campos donde se detallan características del paquete y su contexto, tales como el puerto de origen y destino, protocolo empleado, dirección IP, etc y unos campos dedicados a la naturaleza del incidente (clasificación, mensaje, prioridad, etc). Algunos de estos campos son comunes a todas las reglas y permiten agruparlas para administrar eficientemente las alertas generadas cuando una regla coincide con la descripción de un incidente. Dado que estos campos también se pueden considerar observables, es posible utilizarlos por TheHive y Cortex para automatizar respuestas.

## Análisis de prioridades de los incidentes

Como se indicó anteriormente, la estructura de las reglas consisten en dos partes bien definidas: un encabezado (header) que es obligatorio y un conjunto de campos opcionales. Dentro del header encontramos la acción (alerta, notificación, etc), el protocolo (tcp, udp), puertos de origen y destino, el sentido del evento (entrante o bidireccional) y las direcciones IP de origen y destino.

La segunda parte de las reglas incluye dos tipos de campos: los que describen la naturaleza del evento y aquellos que contienen información del paquete de datos. Dentro del primer grupo encontramos aquellos tales como msg (descripción del evento), sid (id de la firma), classtype (clasificación de reglas o alertas), priority (prioridad de la firma y/o alerta), target (especifica de qué lado está el objetivo, es decir puerto de origen y puerto de destino), entre otros. El segundo grupo contiene datos extraídos que provienen desde de la capa de red hasta la de aplicación de la pila OSI. Se pueden mencionar a los campos “GeoIP” (localización geográfica de la IP), “Fragbits” (presencia del bit de fragmentación), “ACK” (presencia del campo ACK en paquete TCP), “itype” (número del tipo de mensaje ICMP), “http.method” (tipo de método HTTP usado), entre otros.

|  |
| --- |
|  |
| Figura N+7: Estructura general de una regla |

Como se describió en los párrafos precedentes, como los campos están presentes en todas las reglas, es posible hacer uso de algunos de ellos para agrupar reglas que describen amenazas pertenecientes a un mismo grupo o categoría de malware, intentos de intrusión, reconocimiento, escalado de privilegios, etc y por lo tanto son útiles para gestionar los incidentes.

Es posible configurar esta gestión a través de un archivo que relaciona campos como categorías de eventos con prioridades de la alerta generada. Este archivo llamado “classification.config” se encuentra bajo el directorio que almacena las reglas descargadas desde diversas fuentes; en particular relaciona los campos “classtype” con “priority”, de manera tal que cualquier regla cuyo campo classtype contenga a los descritos en este archivo, generará una alerta con prioridad definida también en este. De esta manera, es posible administrar un enorme número de reglas agrupadas en un reducido grupo de categorías y modificar el nivel de prioridad que tendrá en el sistema las alertas que generan.

El objetivo de asignar distintos niveles de prioridad a las alertas generadas por los eventos que sucedan radica en la naturaleza de los eventos, su importancia y la gestión de la atención de los analistas del CSIRT. Esto se debe a las necesidades de optimizar el uso de los recursos técnicos y humanos del centro de respuesta a incidentes para cumplir de la manera más eficiente posible con los objetivos y políticas de la organización a la cual pertenece. De esta manera, la naturaleza de los incidentes determina su elegibilidad para una respuesta automatizada al tener en cuenta por un lado su estructura bien conocida y por el otro su alta tasa de repetición en un periodo determinado. En estos casos, sería inutil destinar valiosos recursos como la atención de un analista ya que se conoce perfectamente la estructura del incidente y por lo tanto la respuesta apropiada o en aquellos casos en los que aún conocida su estructura, el incidente proviene en simultáneo de múltiples fuentes en muy poco tiempo, de manera que la capacidad humana de responder de a uno a la vez estaria tan sobrepasada que no sería efectiva. Estos son los casos de ataques de reconocimiento y los de denegación distribuida de servicio, entre otros.

De aproximadamente cuarenta y siete (47) categorías de incidentes disponibles por defecto, consideramos para el máximo nivel de prioridad a siete clasificaciones dado su nivel de ocurrencia y nivel de impacto para la organización.

* Web-application-attack: esta categoría engloba a un conjunto enorme de malware y ataques a nivel de capa de aplicación. Gusanos, ransomware, ataques de reconocimiento entre otras amenazas comparten esta categoría. Sobre el caso particular de los ataques de reconocimiento, se aplicaron filtros para separarlos de los demás ya mencionados.
* Unsuccessful User: intentos repetidos de ganar acceso en ciertos activos e infraestructura de la organización.
* Attempted-dos: intentos de ataque de denegación de servicio y su variante distribuida
* Known client side exploit attempt: intento de ejecución de exploits en el lado del cliente.
* Exploit Kit Activity Detected: detección de actividad de un kit de exploits
* A suspicious filename was detected: detección de nombres de archivos sospechosos
* Network Trojan: detección de un virus troyano de red.

## Automatización de acciones

La automatización de acciones puede dividirse en dos categorías: acciones activas ya sea sobre el incidente, las causas que lo provocan (vulnerabilidades, puertos, direcciones del atacante, etc) o bien mediante notificaciones de la detección a los analistas del CSIRT y/o los responsables designados (analistas de un NOC, administradores de redes, encargados o usuarios de los activos afectados, entre otros). Se eligió esta última categoría por considerar que era la más apropiada para notificar y generar el mayor impacto al cubrir gran parte de los medios de comunicación disponibles en la organización.

Cuando un incidente es reportado por ElastAlert a TheHive tal como se describió al final de la sección anterior, se inicia una serie de pasos en la cual intervienen webhooks y Cortex como se puede apreciar en la figura siguiente:

|  |
| --- |
|  |
| Figura N+8: Secuencia de respuesta automatizada |

# Iteración 5: “Testing y corrección para puesta a prueba”

## Test de detección de ataques varios

## Test de reportes de incidentes

## Test de acciones automáticas

# Conclusión

# Futuros trabajos

# 

# 

# 

# 

# Bibliografía

[1]CCNA Cybersecurity Operations. CSIRT Overview ,Chapter 13 Incident Response and Handling, 2018. [Consultado 6-12-2019].

[N] LACNIC: acerca de; <https://www.lacnic.net/966/1/lacnic/acerca-de-lacnic>

# Anexos