## 

## Modificaciones solicitadas 23/10/2020

Pequeña introducción sobre los riesgos a los que se exponen las redes modernas. Esto me llevará a la necesidad de justificar un SOC. Luego para desplegar un SOC/CSIRT, tomó como referencia el documento del SANS Inst. y esto me da lugar de forma natural, a presentar un SIEM.

CSIRT/SOC, su organización, la propuesta del SANS.

SIEM, sus funciones,etc…

Soluciones propietarias de SIEM, las versiones libres a las que dan soporte.

Soluciones open source para implementar un SIEM. Mencionar más de una para poder justificar la opción por la que voy a utilizar.

Los distintos tipos de CSIRT me van a permitir justificar la construcción de un CSIRT en la UNC.

### Hoja de ruta

1. Reordenar las partes
   1. comparar la estructura de lo solicitado con la que tenemos y cambiar lo necesario
   2. identificar los párrafos
   3. modificar las oraciones necesarias para mantener una coherencia en el texto
2. Incorporar la iteración 1 al marco teórico
3. Revisar los requerimientos y ordenarlos como se pide
4. Colocar los requerimientos después del marco teórico

# Marco Teórico modificado (SANS)

Las infracciones a las políticas de seguridad y los ataques han concentrado la atención sobre las capacidades de detección, investigación y mitigación de incidentes de las organizaciones. Si bien muchas veces no es posible evitar un incidente de seguridad, es necesario poder detectar y responder rápidamente para evitar un daño completo. Para ello es necesario realizar inversiones inteligentes basadas en un plan de seguridad de seguridad que comprenda la realidad y necesidades específicas de la organización, ya que un gran monto de dinero o equipos adquiridos por si solos no garantizan una mayor protección.

Este plan debe incluir personal especializado, procedimientos e infraestructura adaptados a la organización, con una gestión de objetivos a cumplir a corto, mediano y largo plazo.

Para las organizaciones sin una capacidad formalizada de manejo de incidentes, la creación desde cero de un centro de operaciones de seguridad (SOC) o también conocido como CSIRT (Equipo de Respuesta a Incidentes de Seguridad de Computación) que permita la visibilidad, las alertas y la investigación centralizadas puede ser un proceso muy complejo y costoso. Lo anterior no implica que para disponer de la capacidad de seguridad sea necesaria una gran inversión, ya que es posible desarrollar una solución a escala de la organización en base a un análisis apropiado.

El centro de operaciones de seguridad debe tener una perspectiva flexible y escalable para mantener el ritmo de las tácticas de los adversarios, acompañando el crecimiento y evolución de la organización. Para alcanzar este objetivo, una vez identificadas las necesidades de la organización, el proceso de creación del CSIRT requiere la colaboración y comunicación entre los tres pilares fundacionales de un SOC: el personal, la tecnología y los procesos como se muestra en la Figura 1.

|  |
| --- |
|  |
| Figura 1: Pilares de un CSIRT |

## Personal

En cuanto al personal, estos comprenden tanto a los encargados de dar respuesta a los incidentes como a los analistas del CSIRT. Si bien la propia organización puede designar a sus integrantes para asumir estas funciones, existen otras alternativas como la tercerización mediante empresas especializadas que proveen el servicio (llamadas MSSP por sus siglas en inglés) o contratar especialistas en respuesta a incidentes (IR) en el caso de una emergencia o un problema complejo. Otra vía consiste en la creación de equipos híbridos compuestos por personal perteneciente a la organización y especialistas de compañías especializadas. De acuerdo a una encuesta del SANS Institute del año 2014, el 61 % de las organizaciones relevadas manifestaron haber recurrido a personal de emergencia para cubrir incidentes críticos y el 58 % tenía un equipo de respuesta propio. Por lo que las organizaciones raramente cubren sus necesidades con miembros de su propia plantilla y en algunos casos las tareas recaen por completo en los servicios de personal externo. Esto se debe a que sin importar la estructura del equipo, el personal de un SOC debe contar con el entrenamiento necesario para tratar con los cambios constantes y en algunos casos desafiantes, de las tareas de análisis de seguridad, investigación, especialistas en amenazas y director de un SOC. La tabla 1 muestra las responsabilidades y la formación requerida para cada uno de los tipos de integrantes de un SOC.

|  |  |  |
| --- | --- | --- |
| Título profesional | Tarea | Entrenamiento requerido |
| Nivel 1 - Analista de alertas | Supervisa continuamente la cola de alertas; clasifica las alertas de seguridad; monitorea el estado de los sensores de seguridad y los puntos finales; recopila los datos y el contexto necesarios para iniciar el trabajo de Nivel 2. | Procedimientos de triaje de alerta; detección de intrusos; gestión de redes, información de seguridad y eventos y capacitación en investigación basada en host; y otra formación específica sobre herramientas. |
| Nivel 2 - Respondedor de incidentes | Realiza un análisis profundo de incidentes al correlacionar datos de varias fuentes; determina si un sistema crítico o un conjunto de datos se ha visto afectado; asesora sobre remediación; proporciona soporte para nuevos métodos analíticos para detectar amenazas. | Análisis forense de redes avanzado, análisis forense basado en host, procedimientos de respuesta a incidentes, revisiones de registros, evaluación básica de malware, análisis forense de redes e inteligencia de amenazas. |
| Nivel 3 - Experto en la materia | Posee un conocimiento profundo sobre redes, endpoints, inteligencia de amenazas, ingeniería forense e ingeniería inversa de malware, así como el funcionamiento de aplicaciones específicas o infraestructura de TI subyacente; actúa como un “cazador” de incidentes, sin esperar que se intensifiquen los incidentes; estrechamente involucrado en el desarrollo, ajuste e implementación de análisis de detección de amenazas | Entrenamiento avanzado en detección de anomalías; Entrenamiento específico de herramientas para la agregación y análisis de datos e inteligencia de amenazas. |
| SOC Manager | Administra recursos para incluir personal, presupuesto, programación de turnos y estrategia tecnológica para cumplir con los acuerdos de nivel de servicio; se comunica con la gerencia; sirve como persona de contacto organizacional para incidentes críticos para el negocio; proporciona una dirección general para el SOC y aporta información a la estrategia de seguridad general. | Gestión de proyectos, formación en gestión de respuesta a incidentes, habilidades generales de gestión de personas. |
| Tabla 1 | | |

Para orquestar el trabajo de los analistas, un SOC necesita un director que coordine los múltiples esfuerzos dentro del equipo, a veces inclusive en la respuesta a incidentes dentro y fuera del SOC. Su responsabilidad es priorizar el trabajo y organizar los recursos con el último fin de detectar, investigar y priorizar incidentes que puedan impactar en la organización. Otra de las misiones asignadas al director consiste en desarrollar un modelo de flujo de trabajo e implementar procedimientos operativos estandarizados para el proceso de manipulación de incidentes que guíen a los analistas a través de un proceso de clasificación y respuesta.

En la Figura 2 se observa una posible organización de un SOC.

|  |
| --- |
|  |
| Figura 2: Organización por niveles de un CSIRT |

## Procesos

Definir procesos repetibles de clasificación de incidentes e investigación, estandariza las acciones que pueden tomar los analistas del SOC y aseguran que no se perderán tareas importantes en el camino. Al crear un flujo de trabajo de gestión de incidentes repetible, se definen las responsabilidades y acciones de los miembros del equipo desde la creación de una alerta y la evaluación de nivel 1 hasta el escalamiento al personal de los niveles 2 o 3; esto incluye la asignación efectiva de los recursos.

Uno de los modelos de procesos de respuesta a incidentes más utilizado es el modelo DOE/CIAC, que consiste en seis etapas: preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas.

## Tecnología

En el núcleo de un SOC se encuentran las tecnologías de recolección de datos, agregación, detección, análisis y administración. En cuanto a la recolección de datos, un sistema de monitoreo obtiene sus datos a partir de un conjunto variado de fuentes como puntos finales (PC, dispositivos móviles, servidores, etc), redes y generadores de logs y eventos. Como resultado de la disponibilidad de los datos de la red, logs y puntos finales, antes y durante el incidente, los analistas pueden utilizar el sistema de monitoreo como una herramienta de investigación revisando las actividades sospechosas del incidente en curso e incluso pueden usarla para gestionar la respuesta al mismo o sus causas. Es importante la compatibilidad de las tecnologías empleadas, en particular si la organización ya cuenta con una herramienta de monitoreo existente y se busca incorporar nuevos sistemas para integrarlos a las herramientas disponibles; la Figura 3 ejemplifica la necesidad de compatibilidad entre sistemas y componentes.

|  |
| --- |
|  |
| Figura 3: Compatibilidad entre tecnologías de detección |

### Agregando contexto a los incidentes

La incorporación de inteligencia de amenazas, activos, identidades y otras informaciones de contexto es otra manera en la cual una solución de monitoreo de seguridad puede ayudar al proceso de investigación del analista de un SOC. En determinados casos, una alerta es asociada con una red o una actividad relacionada con un host e inicialmente puede contener solo las direcciones IP del punto final sospechoso. Para que los analistas puedan investigar el sistema en cuestión, generalmente necesitan otra información, como el dueño y el nombre de dominio de la máquina, los registros DHCP para mapear la IP y la información del host al momento de la alerta. Si el sistema de monitoreo incorpora información de identidad y de los activos, provee de una gran ventaja en términos de esfuerzo y tiempo del analista, sin mencionar factores clave que el analista puede usar para priorizar los incidentes; en términos generales los activos de mayor valor deben priorizarse sobre los de menor valor.

### Definición de conductas normales

La habilidad de crear una referencia o línea base de la actividad de los usuarios, aplicaciones, infraestructura, redes y otros sistemas; por lo tanto establecer lo que se considera un comportamiento normal es una ventaja de la agregación de datos provenientes de varias fuentes. Contar con una definición de lo que se considera “normal”, facilita la detección de conductas sospechosas; es decir todas aquellas actividades que de alguna manera se encuentran fuera de la norma. Un sistema de monitoreo configurado y con una base de referencia adecuada envía alertas que pueden ser confiables y en ocasiones priorizadas automáticamente antes de llegar al analista de nivel 1. Sin embargo y, de acuerdo al citado informe del SANS Institute del año 2014, uno de los principales desafíos en la utilización de datos de log es la incapacidad de distinguir actividades sospechosas de las normales. La ausencia de una referencia de “normalidad” es un obstáculo común al que se enfrentan las empresas de monitoreo y muchas organizaciones.

La mejor práctica es usar plataformas que pueden crear líneas o patrones de referencia mediante el monitoreo de la red y la actividad de los puntos finales durante un periodo de tiempo, para determinar lo que es “normal” y proveer la capacidad de establecer umbrales de eventos como indicadores de alertas. Cuando un comportamiento inesperado una desviación de una actividad normal es detectada, la plataforma crea una alerta indicando que es necesaria una investigación más detallada.

### Inteligencia de amenazas

Los SOC bien establecidos o maduros desarrollan continuamente la capacidad de consumir y aprovechar inteligencia proveniente tanto de amenazas de sus incidentes pasados como de fuentes de inteligencia compartidas; ejemplos de estas últimas son los proveedores especializados de inteligencia de amenazas, socios industriales, divisiones policiales de cibercrimen, organizaciones de intercambio de información como la IT-ISAC, etc. La capacidad de un sistema de monitoreo para operacionalizar la inteligencia de amenazas y usarla para ayudar a detectar patrones en datos puntos finales, logs y registros de red, así como asociar anomalías con alertas del pasado, incidentes o ataques anteriores, pueden contribuir con el mejoramiento de la capacidad de detección de un sistema o usuario comprometido antes de que se produzcan nuevos incidentes.

### Obstáculos para el manejo eficiente de incidentes del SOC / CSIRT

Parte de los obstáculos que deben ser evitados por un SOC son aquellos que generan cuellos de botella en el proceso de respuesta a incidentes. Dado que este último consiste en el traslado de un incidente entre los niveles 1, 2 y 3 existe la posibilidad de crear “ruido blanco” debido a la presencia de una gran cantidad de alertas de poca importancia y / o falsos positivos; de prolongarse esta situación en el tiempo, se produce un fenómeno llamado “fatiga de alertas” que afecta a los analistas provocando una disminución en sus capacidades de atender alertas.

Al momento de elegir una herramienta de monitoreo, se debe considerar que incluya entre sus características la personalización del umbral de alertas y la posibilidad de combinar distintas alertas en un mismo incidente. Una herramienta de este tipo permite a los analistas clasificar las alertas más rápido, reduciendo las capas de evaluación necesarias antes de que el evento pueda ser confirmado y mitigado rápidamente.

### Multiplicidad de herramientas de monitoreo y su integración

A medida que los sistemas de conexión se vuelven cada vez más complejos y deben soportar redes 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 desarrolla un conjunto cada vez más numeroso y especializado de herramientas que intentan cubrir los 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; es necesario un sistema capaz de procesar, filtrar, normalizar, presentar y almacenar toda esta información. Este sistema es un SIEM.

## SIEM: Definición y sus funciones

El proceso de monitoreo de la seguridad de una red de datos compleja requiere recopilar diferentes tipos de datos para detectar, verificar y contener acciones ofensivas. Para ello se requieren tecnologías *Security Information and Event Management* (SIEM). Estas tecnologías proporcionan informes en tiempo real y análisis de eventos de seguridad a largo plazo, como se muestra en la Figura 4. Todo esto ayuda a la tarea de un analista de ciberseguridad cuando debe verificar acciones ofensivas sobre la red de una organización.

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.   
 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.

Como se puede observar en la figura 4, para cumplir con las tareas anteriormente descritas, un SIEM obtiene su información de diversas fuentes:

* Inteligencia de Amenazas, administración de identidades y almacenamiento de logs: la revisión de amenazas pasadas y la inteligencia compartida por otras organizaciones aliadas contribuyen a detectar más rápido patrones anormales de comportamiento.
* Telemetría de Netflow: es un protocolo de recopilacion de informacion del flujo de red IP.
* Captura de paquetes: replicación de paquetes de información con el fin de correlacionar posibles amenazas en el flujo de red.
* Dispositivos Antimalware: componentes especializados en la detección de malware, localizados en puntos finales.
* IDS (HIDS y NIDS): Sistemas de detección de intrusiones, orientados a redes (NIDS) o puntos finales (HIDS).
* Firewalls: software que bloquea y filtra conexiones con origen desde el sistema hacia el exterior y viceversa.
* IPS: Sistema de protección de intrusiones. Ofrecen protección activa frente a comportamientos inusuales ya que pueden tomar acciones programadas para evitar un intento de intrusión.
* Logs de servidores y servicios (Syslog): Syslog es un protocolo para el envío de logs en un formato estandarizado

|  |
| --- |
|  |
| Figura 4: Funciones y flujos de datos de un SIEM. CCNA Cybersecurity Operations, *SIEM and Log Collection* |

Por lo tanto, la secuencia que sigue la información dentro un SIEM se puede graficar como se observa en la Figura 5

|  |
| --- |
|  |
| Figura 5: Procesos de acción de un SIEM |

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. La Figura 6 representa las responsabilidades primarias de un SIEM.

|  |
| --- |
|  |
| *Figura 6: Capacidades Críticas de un SIEM* |

## 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 1: 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** |  |
| Tabla 2: Soluciones SIEM Comerciales y Libres | |

### 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 3. 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 7* |

En las Figuras 7 y 8 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 9 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 8* |

|  |
| --- |
| Gráfico |
| *Figura 9* |

### 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 10 se puede observar el porcentaje de adopción por área en la industria.

|  |
| --- |
| Gráfico |
| *Figura 10* |

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 11

|  |
| --- |
| Gráfico |
| *Figura 11* |

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.

## Ámbitos de actuación de los CSIRT

En la actualidad existen en todo el mundo CSIRT pertenecientes a organizaciones que responden a distintos ámbitos de la sociedad y de diferente naturaleza (pública o privada). En términos generales, estos equipos se clasifican dependiendo de la comunidad a la que atienden, diferenciándose entre:

* CSIRT para el sector de PYMES: En este caso, el tamaño de las empresas hace poco viable que las organizaciones de este sector puedan implementar de forma individual las funciones de un CSIRT. Por lo tanto, surge la necesidad de unificar esfuerzos y servicios en un solo CSIRT capaz de dar soporte a varias empresas. La naturaleza de estos CSIRT puede ser pública o privada, dependiendo del contexto en el que se encuentren estas compañías.
* CSIRT académico: El área de responsabilidad de este tipo de equipos se circunscribe a instituciones académicas. Su tamaño, por lo tanto, puede variar dependiendo de las dimensiones de la comunidad, esto también condiciona los servicios que ofrezcan, el modo en que lo hagan y su grado de intervención.
* CSIRT comercial: estos centros prestan distintos servicios a cambio de una contraprestación económica. Habitualmente utilizan acuerdos de servicios específicos con cada cliente.
* CSIRT de proveedor: se centra en los productos o servicios específicos de un proveedor. Su objetivo es proveer servicios y soluciones para eliminar o reducir el impacto negativo de las vulnerabilidades de estos últimos, ya sea un producto tecnológico o un servicio TIC.
* CSIRT del sector militar: Prestan servicios a organizaciones militares con responsabilidades en infraestructuras TIC necesarias con fines de defensa. Su comunidad está conformada por las instituciones militares y de entidades estrechamente relacionadas con éstas como, por ejemplo, del Ministerio de Defensa. Por ejemplo, en nuestro país es el Comando Conjunto de Ciberdefensa dependiente del Estado Mayor Conjunto de las Fuerzas Armadas.
* CSIRT para protección de infraestructuras críticas: Los CSIRT de este sector se centran principalmente en la protección de las infraestructuras críticas y de las infraestructuras críticas de la información (administración, centrales y redes de energía, tecnologías de la información y las comunicaciones, sistema financiero y tributario, sector sanitario, espacio, instalaciones de investigación, alimentación, agua, transportes, las industrias nuclear y química entre otras).
* CSIRT gubernamental: Bajo esta denominación se sitúan los equipos cuyo principal objetivo es asegurar la infraestructura TIC de un Gobierno/Estado y los servicios ofrecidos a la población. La Comunidad a la que están dirigidos son las administraciones públicas y sus distintos organismos. A su vez, esta comunidad puede dar servicio, a la administración local, provincial, nacional o a todas ellas. Estos CSIRT gubernamentales generalmente forman parte y están patrocinados por instituciones del Estado.
* CSIRT Nacional: Este es un equipo con responsabilidad general de coordinación sobre todos los sectores y tiene una amplia responsabilidad sobre prácticamente todos los puntos tratados anteriormente. Este centro funciona como punto focal de contacto tanto en el entorno nacional como para requerimientos internacionales. ENISA, la Agencia de Ciberseguridad para la Unión Europea, define en un documento elaborado en diciembre de 2009, a este tipo CSIRT como aquel que actúa como el Punto Nacional de Contacto (POC) con otros CSIRT nacionales y/o internacionales. De hecho, podría considerarse como “CSIRT del último recurso”, por su papel de coordinación. En muchos casos el CSIRT nacional también actúa como CSIRT gubernamental o tiene su origen en él. De igual modo, señala el documento, el CSIRT nacional de facto suele ser aquel que ha sido establecido primero por un Gobierno y actúa como contacto con otros países. Cada CSIRT es único, en el sentido de que establece sus operaciones, su organización y su imperativo legal para satisfacer las necesidades de su país y su comunidad.

|  |
| --- |
|  |
| Figura 12: CSIRT Nacional como centro de coordinación |

Frente a esto, todos los CSIRT tienen un objetivo común, mantener seguras las redes de sus países. De este modo podemos concluir que, aunque cada CSIRT utiliza herramientas y procedimientos diferentes, todos comparten el mismo objetivo:

* + Designar un punto de contacto para la coordinación de la respuesta a incidentes.
  + Construir y mantener una red de contactos extensa, tanto nacional como internacional.
  + Monitorización de la situación actual y mejora de la concientización.

Es importante destacar que la constitución de un CSIRT nacional o gubernamental no es la única medida a tener en cuenta en una estrategia de ciberseguridad completa por parte de un Estado, pero sí una parte importante de la misma, teniendo en cuenta, además, que este tipo de equipos deberían asumir, además, la responsabilidad de la Protección de las Infraestructuras Críticas de Información (CIIP).

# Descripción de Requerimientos

La idea es presentar requerimientos desde arriba hacia abajo. Desde el nivel de sistema hasta el nivel detallado.

## 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 de múltiples fuentes: 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.

# 