# Objetivo General

## 

## Marco teórico

## Descripción del CSIRT y el rol del SIEM

paper Study\_on\_CSIRT\_Maturity\_29042019.pdf (pagina 8 a la 11)

paper WP2018 O.3.1.3 CSIRT landscape 2020.pdf (pagina 9 a 13)

paper the\_complete\_guide\_to\_log\_and\_event\_management\_wp.pdf (pagina 4 tabla hasta pagina 9)

<https://blogs.gartner.com/anton-chuvakin/2017/08/14/lets-define-siem/>

* <https://www.interempresas.net/Electronica/Articulos/232650-Integracion-SIEM-SOC-Ciberseguridad-privacidad-motores-clave-esencia-accesibilidad.html> (Estructura SOC y su integración con SIEM)

### Incidentes de seguridad informática y el CSIRT

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

### Tipos de CSIRT

* Capítulo 2 (pag 20) - Revisión de literatura (Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management).pdf)
* 1.5 Marco teórico (Propuesta Metodológica y Simulación de la Implementación de un SIEM basado en la Norma ISO 27001 y/o 27002.pdf)
  + 1.5.3. SIEM “Security Information and Event Management”
  + 1.5.3.2. Arquitectura del SIEM

### SIEM dentro de un CSIRT

<https://www.sumologic.com/glossary/siem/>

<https://www.prelude-siem.com/en/what-is-a-siem/>

<https://www.42gears.com/es/blog/siem-a-shift-in-focus-to-threat-monitoring/>

<https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.0.pdf>

## Estado del arte de los CSIRT en el mundo

ENISA

Definicion de CSIRT Nacionales: <https://www.enisa.europa.eu/publications/baseline-capabilities-for-national-governmental-certs>

Red de CSIRT de la Unión Europea:

<https://csirtsnetwork.eu/>

noticia de hack britanico

<https://www.infobae.com/america/mundo/2017/05/12/ciberataque-mundial-impacta-a-instituciones-estatales-y-privadas-en-una-dimension-nunca-antes-vista/>

noticia de hack ucrania

<https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/>

noticia de hack Iran

<https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet>

## Realidad de la Región y casos de uso

2016 - Buenas Prácticas CSIRT.pdf

### Estado de la ciberseguridad en Argentina

### CSIRT Estatales en Argentina <https://www.incibe.es/agenda/xx-arcert>

<https://media.distecna.com/1280-El-Poder-Judicial-de-la-Nacion-asegura-su-infraestructura-con-Nutanix.html>

<https://www.canal-ar.com.ar/Nota.asp?Id=3755>

<http://seguridadinformatica.sgp.gob.ar/paginas.dhtml?pagina=303>

<https://politicacomunicada.com/ba-csirt-el-primer-centro-de-ciberseguridad-en-america-latina/>

CSIRT LA PLATA:

<https://cespi.unlp.edu.ar/cert>

CSIRT BUENOS AIRES:

<https://www.ba-csirt.gob.ar/>

CSIRT NEUQUEN:

<https://csirt-nqn.neuquen.gov.ar/>

CSIRT NIC ARGENTINA:

<https://nic.ar/es/node/293>

CSIRT FFAA:

<http://www.fuerzas-armadas.mil.ar/ComandoConjuntoDeCiberdefensa/Mision.aspx>

<https://www.boletinoficial.gob.ar/detalleAviso/primera/193298/20181005>

<https://www.boletinoficial.gob.ar/pdf/aviso/primera/219968/20191029>

CSIRT MIN. SEGURIDAD NACION:

<https://csirt.minseg.gob.ar/>

DIRECCIÓN NACIONAL DE CIBERSEGURIDAD:

<https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad>

#### Leyes y reglamentaciones

<https://ciberseguridad.com/normativa/latinoamerica/argentina/>

Este no estoy muy seguro: <https://proyecto-aurora.org/nosotros/>

<https://observatoriolegislativocele.com/argentina-proyecto-de-ley-que-crea-el-instituto-de-ciberseguridad-argentina-2019/>

<https://www.siteal.iiep.unesco.org/pais/argentina>

<https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa>

<https://www.ccn-cert.cni.es/gl/gestion-de-incidentes/lucia/23-noticias/522-argentina-crea-un-programa-nacional-de-infraestructuras-criticas-de-informacion-y-ciberseguridad.html>

#### Decretos y Reglamentaciones:

1999:

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/61122/norma.htm>

2004:

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/102188/texact.htm>

2011:

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm>

2013:

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219212/norma.htm>

2015:

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm>

2016:42

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257609/norma.htm>

2016:69

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/259549/norma.htm>

2016: 232

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/259845/norma.htm>

2016: 898

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/263831/norma.htm>

2017:577 modificado por 2019:480

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/325000-329999/325052/norma.htm>

2019: 829

**Esta en un PDF**

2019:1523

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/325000-329999/328599/norma.htm>

2014 UNC:

<http://www.digesto.unc.edu.ar/rectorado/rectorado/resolucion/1221_2014_1>

LACNIC

<https://www.lacnic.net/web/anuncios/2016-amenazas-en-linea>

#### CSIRT “comerciales” en Argentina

<https://www.platinumciber.com/soc-siem-csirt> Empresa que provee productos y servicios de terceros

<https://www.redlink.com.ar/servicio_csirt.html> CSIRT de la red Link

<https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2018/20577/Discussion%20Finance%20Medios%20de%20Pago.pdf> CSIRT de la red Banelco

<https://home.kpmg/ar/es/home/services/advisory/it-advisory/ciberseguridad.html>

Tambien podria ir acá lo del CSIRT del poder Judicial de la Nación que implementó la empresa Nutanix

### Casos de uso en América Latina de CERTS, CSIRTS y SOCS.

### CSIRT Estatales en América Latina

LACNIC:

<https://warp.lacnic.net/wp-content/uploads/Informe_amparo_fase_I.pdf>

<https://warp.lacnic.net/taller-amparo>

<https://prensa.lacnic.net/news/ciberseguridad/mas-expertos-en-seguridad-informatica-para-la-region>

<https://csirt.lacnic.net/>

<https://csirt.lacnic.net/nuevo-csirt-de-la-region>

<https://csirt.lacnic.net/estadisticas#Incidentes_por_Anio>

Por países:

<http://www.colcert.gov.co/>

<https://www.csirt.gob.cl/quienes-somos/>

<https://www.cert.br/csirts/>

<https://www.cert.org.mx/acerca-de-la-csi>e

OEA:

<https://www.sites.oas.org/cyber/ES/Paginas/Documents.aspx>

<https://www.sites.oas.org/cyber/Es/Paginas/default.aspx>

<https://www.sites.oas.org/cyber/ES/Paginas/Directory/Default.aspx>

<http://www.oas.org/es/temas/seguridad_cibernetica.asp>

<http://www.oas.org/es/sms/cicte/eventos_sesiones.asp>

<https://www.sites.oas.org/cyber/ES/Paginas/Socios.aspx>

#### CSIRT “comerciales” en América Latina

<https://cert.mnemo.com/>

<https://www.scitum.com.mx/ScitumCert>

<https://cert.iqsec.com.mx/es/#&panel1-1>

### Estado de la ciberseguridad en Argentina

<https://www.infobae.com/economia/2017/03/25/en-2016-el-pbi-cayo-en-pesos-pero-alcanzo-un-record-en-dolares/>

<https://www.argentina.gob.ar/sites/default/files/cofemod_comisionciberseguridad_el_panorama_de_la_ciberseguridad_en_numeros_12-08-16.pdf>

<https://www.iproup.com/innovacion/11963-seguridad-argentina-recibio-1-590-millones-de-ciberataques-en-2019>

## Comunidad a la que sirve el SIEM de la PSI-UNC

<http://secretarias.unc.edu.ar/psi/servicios>

### Descripción de la Red

<https://bgp.he.net/AS27790>

## Sistemas de monitoreo

<https://www.varonis.com/blog/ids-vs-ips/>

Chris Sanders and Jason Smith - Applied Network Security Monitoring. Collection, Detection, and Analysis (2014).pdf

<https://www.controlscan.com/blog/network-security-monitoring-beyond-siem/>

The Practice of Network Security Monitoring.pdf

### Sistemas IDS: HIDS y NIDS

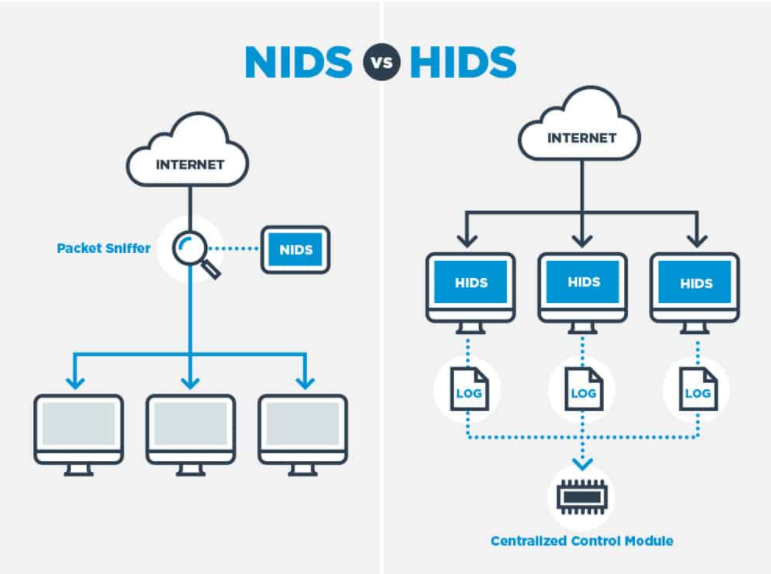


Imagen de página: <https://www.comparitech.com/net-admin/network-intrusion-detection-tools/>

## Sistemas de Gestión de Eventos

### Determinación de requisitos funcionales y no funcionales del SIEM.

# Iteración 1: “Análisis de herramientas disponibles”

## Herramientas de software libre

## Soluciones comerciales

Sector industrial

<https://www.unir.net/ingenieria/revista/por-que-la-ciberseguridad-en-la-industria-4-0-ya-es-tan-necesaria-y-estrategica/>

sector salud

<https://www.ccn-cert.cni.es/pdf/documentos-publicos/i-encuentro-salud/2949-ciberamenazas-sector-salud/file.html>

## Selección de las herramientas

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

## Elección del sistema base de gestión de eventos

### Security Onion

## Arquitectura del sistema de gestión de eventos

### Elastic, ElastAlert, Cortex y TheHive

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

### Analizando y clasificando eventos: ElastAlert

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

### Tomando acciones: TheHiveHooks

## Integración con los sistemas de detección

### Suricata, Snort y Ossec

## Arquitectura del despliegue en la comunidad

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

## Configuración del ambiente de prueba

### Configuración del entorno de virtualización

### Definición y configuración de las redes a observar

### Instalación de las máquinas virtuales

## Configuración inicial del sistema base

### Instalación y configuración de Security Onion

### Pruebas de configuración iniciales

## Automatización de acciones

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

## Análisis de prioridades de los incidentes

## Incidentes a reportar

### Dependencias, activos y administradores de redes

## Automatización de acciones de acuerdo al incidente

# 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