

UNIVERSIDAD ANDRÉS BELLO

FACULTAD DE INGENIERÍA

INGENIERIA EN COMPUTACIÓN E INFORMÁTICA

**Desarrollo de SIEM con herramientas OpenSourse**

**PROYECTO DE TÍTULO PARA OPTAR AL TÍTULO DE**

**Ingeniero en Computación e Informática**

Autor:

Sergio Jofre Contreras

Profesor Guía:

Giannina Costa Lizama

VIÑA DEL MAR, 2018

**Índices de Contenidos.**

[1. Capítulo I 3](#_Toc523263198)

[1.1. Introducción 4](#_Toc523263199)

[2. Capitulo II 5](#_Toc523263200)

[2.1. Definición del problema 6](#_Toc523263201)

[2.2. Objetivo general 7](#_Toc523263202)

[2.3. Objetivos específicos 7](#_Toc523263203)

[2.4. Alcances 7](#_Toc523263204)

[2.5. Limitaciones 8](#_Toc523263205)

[2.6. Alternativas de solución 8](#_Toc523263206)

[2.7. Factibilidades 9](#_Toc523263207)

[2.8. Diseño alto nivel 9](#_Toc523263208)

[2.9. Requerimientos alto nivel 9](#_Toc523263209)

# Capítulo I

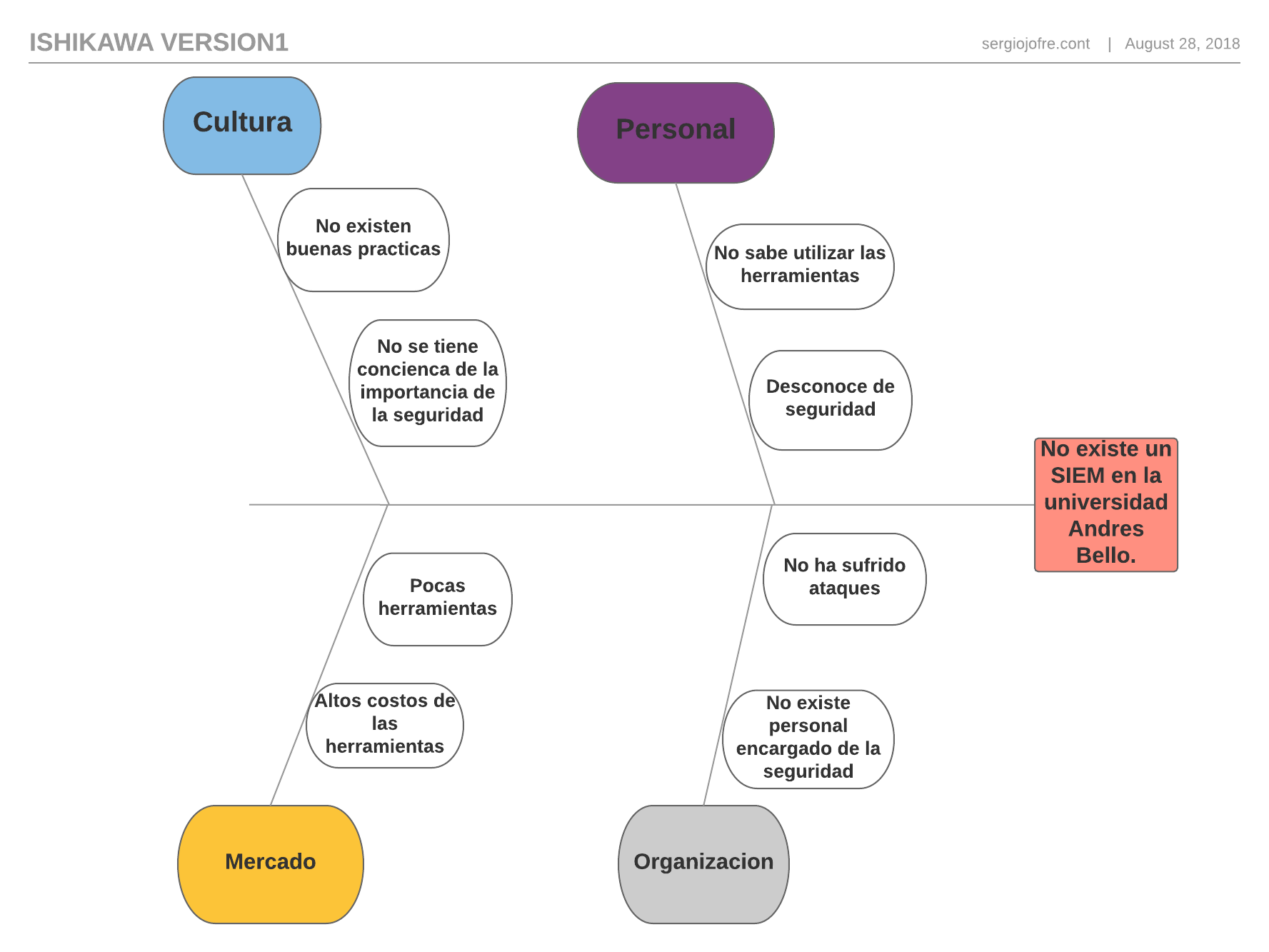
## Introducción

# Capitulo II

## Definición del problema

Un SIEM (Security Information and Event Management) es una categoría de software que tiene como objetivo entregar a las organizaciones información útil sobre potenciales amenazas de seguridad en sus redes (críticas o no) de negocio.

Hoy en día, existen diversas herramientas para la implementación de un SIEM, pero la mayoría de estas son típicamente costosas, de precios muy elevados y son complejas de manejar. Esto genera que las empresas no se interesen en gestionar la seguridad de su información lo cual es una mala práctica y puede traer muy malas consecuencias si no se toman las medidas necesarias para tratar con las amenazas.



## Objetivo general

El objetivo general de este proyecto se enfoca en desarrollar un SIEM con herramientas OpenSource, con el fin de entregar un software para gestionar los incidentes de seguridad de la Universidad.

## Objetivos específicos

## Alcances

* Para este proyecto, solo se considerará realizar un SIEM para la facultad de ingeniería de la Universidad Andrés Bello.
* Se busca gestionar y almacenar eventos con un periodo máximo de un año.
* Se entregará información de los requisitos mínimos para que el sistema gestione y almacene eventos durante un año.
* Se trabajará con base de datos MySQL.

## Limitaciones

* Solo se realizarán comparaciones de las siguientes herramientas: Snort, Suricata, OSSIM, OSSEC, Bro (herramientas de detección) con Snorby, Prelude, Kibana (herramientas de visualizacion).

## Alternativas de solución

A continuación, se presentarán las diferentes alternativas de solución existentes en el mercado (solo las más importantes).

* Micro Focus ArcSight: ArcSight: Sistema SIEM de clase empresarial que puede ingerir datos de más de 350 fuentes y procesar hasta 75,000 eventos de seguridad por segundo. Se puede entregar a través de un dispositivo, software o nube.
* Splunk Enterprise Security: Es una solución de seguridad que proporciona información acerca de los datos de máquina generados por tecnologías de seguridad, como por ejemplo la información de identidad, redes, endpoint, accesos, malware y vulnerabilidades.
* IBM Security QRadar: QRadar: Es una plataforma de gestión de seguridad de red que proporciona conocimiento situacional y soporte de cumplimiento de políticas mediante la combinación del conocimiento de los flujos de red, de la correlación de sucesos de seguridad y de la evaluación de vulnerabilidades de activos.
* LogRhythm UEBA: Diseñado para aumentar su entorno de seguridad actual, puede funcionar como un producto independiente de análisis de comportamiento de la entidad y del usuario (UEBA) o como un complemento de la implementación actual de su SIEM. LogRhythm UEBA detecta amenazas a través de aprendizaje automático supervisado y no supervisado, y análisis de comportamiento multidimensional para mostrar y priorizar rápidamente eventos críticos.
* McAfee Enterprise Security Manager (ESM): Procesa decenas de miles de eventos por segundo y puede almacenar miles de millones de eventos y flujos. Es particularmente popular entre el sector público, la educación superior y las compañías de atención médica, y McAfee ha agregado capacidades específicas para respaldar esos mercados. Está disponible como un dispositivo físico o virtual.

## Factibilidades

## Diseño alto nivel

## Requerimientos alto nivel