ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DESPLIEGUE DE UN SISTEMA DE GESTIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD DE CÓDIGO ABIERTO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

ALEX FERNANDO QUILACHAMÍN MOROCHO

DIRECTOR: MSc. GABRIEL ROBERTO LÓPEZ FONSECA

CODIRECTOR: MSc. FRANKLIN LEONEL SÁNCHEZ CATOTA

Quito, noviembre 2019

AVAL

Certificamos que el presente trabajo fue desarrollado por Alex Fernando Quilachamín Morocho, bajo nuestra supervisión.

MSc. GABRIEL ROBERTO LÓPEZ FONSECA
DIRECTOR DEL TRABAJO DE TITULACIÓN

MSc. FRANKLIN LEONEL SÁNCHEZ CATOTA
CODIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Yo, Alex Fernando Quilachamín Morocho, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración dejo constancia de que la Escuela Politécnica Nacional podrá hacer uso del presente trabajo según los términos estipulados en la Ley, Reglamentos y Normas vigentes.

ALEX FERNANDO QUILACHAMÍN MOROCHO

DEDICATORIA

Este trabajo se lo dedico a mi familia, quienes me han brindado su apoyo en todo momento.

AGRADECIMIENTO

Agradezco a Dios. A mi familia. A mis padres Joaquín y Lourdes por su apoyo, sacrificio y guía que me ha permitido ser una mejor persona cada día.

Un agradecimiento especial a mis directores MSc. Gabriel López y MSc. Franklin Sánchez por su confianza y orientación en el presente trabajo

ÍNDICE DE CONTENIDO

GLOSARIO DE ABREVIATURAS

GMS	Grupo Microsistemas Jovichsa
OSSIM	Open Source Security Information Management (Gestor de información de Seguridad)
SIEM	Security Information and Event Management (Gestor de Eventos de Información de Seguridad)
SIM	Security Information Management (Gestor de Información de Seguridad)
SEM	Security Event Management (Gestor de Eventos de Seguridad)
IDS	Intrusion Detection System (Sistema de Detección de Intrusiones)
HIDS	Host Intrusion Detection System (Sistema de Detección de Intrusiones basado en Host)
SPAN	Switched Port Analyzer (Analizador de Puertos Conmutados)
OSSEC	Open Source HIDS SECurity (Seguridad HIDS de Código Abierto)
SQL	Structured Query Language (Lenguaje de consulta estructurada)
OTX	Open Threat Exchange
TIC	Tecnologías de la Información y la Comunicación
DLP	Data Loss Prevention (Prevención de Pérdida de Datos)
SNMP	Simple Network Management Protocol (Protocolo Simple de Gestión de Redes)
RFC	Request For Comments (Solicitudes de comentarios)
GPL	GNU General Public License (Licencia Pública General de GNU)
MAC	Media Access Control (Control de Acceso a Medios)
IP	Internet Protocol (Protocolo de Internet)
NAS	Network Attached Storage (Almacenmiento conectado a la Red)
CRM	Customer Relationship Management (Gestor de Relación con el Cliente)

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

ÍNDICE DE TABLAS

RESUMEN

El presente Trabajo de Titulación propone el despliegue de un Sistema de Gestión de Eventos e Información (SIEM) de código abierto. La plataforma para desplegar es OSSIM (Open Source Security Information Management). Se utiliza como referencia la información y recursos proporcionados por la empresa GMS. Los activos para monitorear son 5 y la selección se la realiza mediante un análisis de riesgos a 14 activos basado en la metodología Magerit versión 3. Se elaboran directivas de correlación de eventos específicas para los activos a monitorear y se verifica el alertamiento de dichos eventos mediante pruebas realizadas en cada equipo.

En el primer capítulo se detalla la metodología Magerit versión 3 para el desarrollo de un análisis de riesgos; se describen las diferentes funcionalidades que tiene un sistema SIEM y los diferentes componentes que lo conforman; se presenta OSSIM como plataforma de correlación de eventos SIEM, y los métodos de monitoreo y recolección de logs que ofrece.

En el segundo capítulo, se presenta el análisis de riesgos y la selección de activos a monitorear. Se diseñan las directivas de correlación a implementar y se detalla el proceso de despliegue de la plataforma OSSIM, así como la integración de los activos a monitorear

En el tercer capítulo se indican las pruebas realizadas para verificar el funcionamiento de las directivas implementadas.

El cuarto capítulo contiene las conclusiones y recomendaciones generadas durante el desarrollo de este proyecto técnico

PALABRAS CLAVE: OSSIM, SIEM, Magerit, Seguridad en Redes, Análisis de riesgos, Syslog

ABSTRACT

This degree work proposes the deployment of a SIEM Open Source tool. The deployed platform is OSSIM, which is used as an event management and security information system.

The information and resources provided by the company “GMS” are used as a reference. In total 5 assets are been monitored and the selection is made through a risk analysis of 14 assets based on the Magerit version 3 methodology. Correlation directives for specific events ware prepared for the assets to be monitored and verify the alert of these events through tests made on each asset.

The Magerit version 3 methodology for the development of a risk analysis is detailed in first chapter; as well as the different functionalities of a SIEM system and different components that integrate it are described; OSSIM is presented as a SIEM event correlation platform and the monitoring and record collection methods it offers.

Second chapter discusses the development of the risk analysis and the selection of assets to monitor. The correlation directives to be implemented are designed, and the OSSIM platform deployment process is detailed as well as the integration of the assets to monitor.

Third chapter describes the tests carried out to verify the functioning of the implemented directives.

Fourth chapter contains the conclusions and recommendations gathered during the development of this technical project.

KEYWORDS: OSSIM, SIEM, Magerit, Network Security, Risk assessment, Syslog

1. INTRODUCCIÓN

Actualmente las medianas y grandes empresas cuentan con activos de información, entre los cuales se puede destacar los siguientes: servidores de correo, servidores de archivos, servidores de aplicaciones, equipos perimetrales como firewall, switches, routers; que forman parte de la infraestructura de red que brindan servicios a todos los usuarios finales.

Estos activos son propensos a ser víctimas de diferentes ataques que pueden ocasionar la toma de control por personal no autorizado, extracción de información personal o el cambio de información sensible para la empresa debido a una falta de monitoreo sobre los mismos. Una falta de monitoreo a los activos tecnológicos que son críticos para las empresas produce una brecha en la seguridad, dado que no existe un control de eventos sobre los mismos, ocasionando que la detección de un incidente llegue a tomar varios días y causando pérdidas económicas [1].

De acuerdo con [2], solo el 45% de las empresas de América Latina cuentan con un Sistema de Gestión de Eventos e Información (SIEM) y uno de los factores que ocasiona esto es la falta de presupuesto. Esto da como resultado una falta de visibilidad sobre eventos importantes como accesos fuera de horario de oficina, cambios en la configuración o modificación de archivos críticos.

El presente proyecto propone el despliegue de una herramienta SIEM Open Source, utilizando un análisis de riesgo para detectar qué activos dentro de una red son susceptibles de amenazas y con esto realizar un monitoreo constante sobre las mismas. El SIEM informará sobre eventos que pongan en riesgo la seguridad de la red.

En este capítulo se presentarán los objetivos del presente proyecto tanto general como específicos, alcance y el marco teórico. En el marco teórico se detalla la metodología de análisis de riesgos Magerit versión 3, se describen las diferentes funcionalidades que tienen los sistemas SIEM y los diferentes componentes que los conforman y se presenta OSSIM (Open Source Security Information Management) como plataforma de correlación de eventos SIEM, así como los métodos de monitoreo y recolección de logs que ofrece.

1.1 OBJETIVOS

El objetivo del presente trabajo de titulación es desplegar un sistema de gestión de eventos e información de seguridad de código abierto.

Los objetivos específicos son:

- Analizar la tecnología de OSSIM y las diferentes herramientas que lo componen.

- Definir parámetros necesarios para el despliegue del SIEM.
- Implementar OSSIM como herramienta SIEM.
- Analizar los resultados de las pruebas de funcionamiento realizadas a la herramienta OSSIM.

1.2 ALCANCE

El trabajo de titulación presentado propone el despliegue de la herramienta OSSIM, la cual es un SIEM Open Source. Se utilizará como referencia la información y recursos proporcionados por la empresa GMS para realizar el despliegue del SIEM y se utilizará su infraestructura de red para la demostración de uso de la herramienta de monitoreo de al menos 5 activos críticos de información. Los activos de información serán seleccionados mediante un análisis de riesgos basado en la metodología MAGERIT [3] versión 3 dado que es la más reciente y además es una de las más utilizadas para el análisis de riesgos.

Como un paso previo para la implementación de OSSIM se realizará un análisis de riesgos al menos a 10 activos de información que la empresa ha considerado como relevantes para su operación. Se establecerá la valoración de los activos de acuerdo con las dimensiones de confidencialidad, disponibilidad e integridad. Este análisis estará basado en modelo cualitativo el cual permitirá conocer cuál es el riesgo presente en cada activo de información. Con el resultado de este análisis se podrán definir los activos más críticos de la empresa y de los cuales se escogerán al menos 5 activos para realizar la integración con la herramienta OSSIM y llevar a cabo un monitoreo constante.

Para la instalación de OSSIM se usará un servidor proporcionado por la empresa, el cual tendrá como requisitos mínimos 8 Cores, 8 GB de RAM, 2 interfaces de red y 300 GB de disco duro. Después de completar la instalación se realizarán pruebas generales del sistema para verificar que se cuente con comunicación a internet y a los equipos que se encuentren dentro de la red [4].

En los equipos que se haya definido para el monitoreo, se realizará las respectivas configuraciones para que envíen logs utilizando el protocolo syslog [5] o se utilizará un agente OSSEC [6], el cual tiene compatibilidad con OSSIM, para realizar el envío de logs de manera cifrada.

Se utilizará la característica de analizador de red que posee la herramienta [7] para detectar anomalías presentes en la red mediante firmas de ataques conocidos como denegación de servicio, escaneo de puertos o conexiones hacia dominios maliciosos.

En base a los eventos que se reciban, se verificará las alarmas que se generen con las directivas precargadas que trae la herramienta. Se elaborará políticas para descartar falsos positivos que se presenten durante la realización de este proyecto técnico.

Se realizará un monitoreo de integridad de archivos de configuración en los servidores, utilizando el agente OSSEC y se configurará la directiva necesaria para que se genere una alarma cuando estos hayan sido modificados. Las directivas permiten detectar parámetros que tienen los eventos que llegan al SIEM y definir si el evento o sucesión de eventos deben ser notificados como una alarma.

Se configurarán directivas que permitan detectar las siguientes anomalías en los equipos:

- Ataques de fuerza bruta.
- Cambios en la configuración de los equipos.
- Conexiones permitidas desde el firewall hacia direcciones IP que han sido reportadas como maliciosas.

Se realizarán casos de prueba utilizando una computadora personal, la cual será usada para realizar ataques de fuerza bruta hacia los activos, también se accederá a los equipos para realizar cambios en las configuraciones y se accederá a las direcciones IP que se encuentren reportadas como maliciosas en Open Threat Exchange (OTX) [8], la cual es una comunidad donde se comparten indicadores de compromiso, y así verificar que las directivas funcionen correctamente.

El diagrama de red que se tendrá para el funcionamiento de la herramienta OSSIM se muestra en la Figura 1.1

Este presente proyecto de titulación tendrá un producto final demostrable

1.3 MARCO TEÓRICO

1.3.1 METODOLOGÍA MAGERIT

Magerit se refiere a la Metodología de Análisis y Gestión de Riesgos en los Sistemas de Información, la mismo se encarga de cubrir el Proceso de Gestión de Riesgos para la evaluación de riesgos en función de la organización o proyecto. Esto quiere decir que Magerit implementa el Proceso de Gestión de Riesgos dentro de las funcionalidades de la organización para la justificación de la toma de decisiones frente a riesgos derivados del uso de las tecnologías de información.

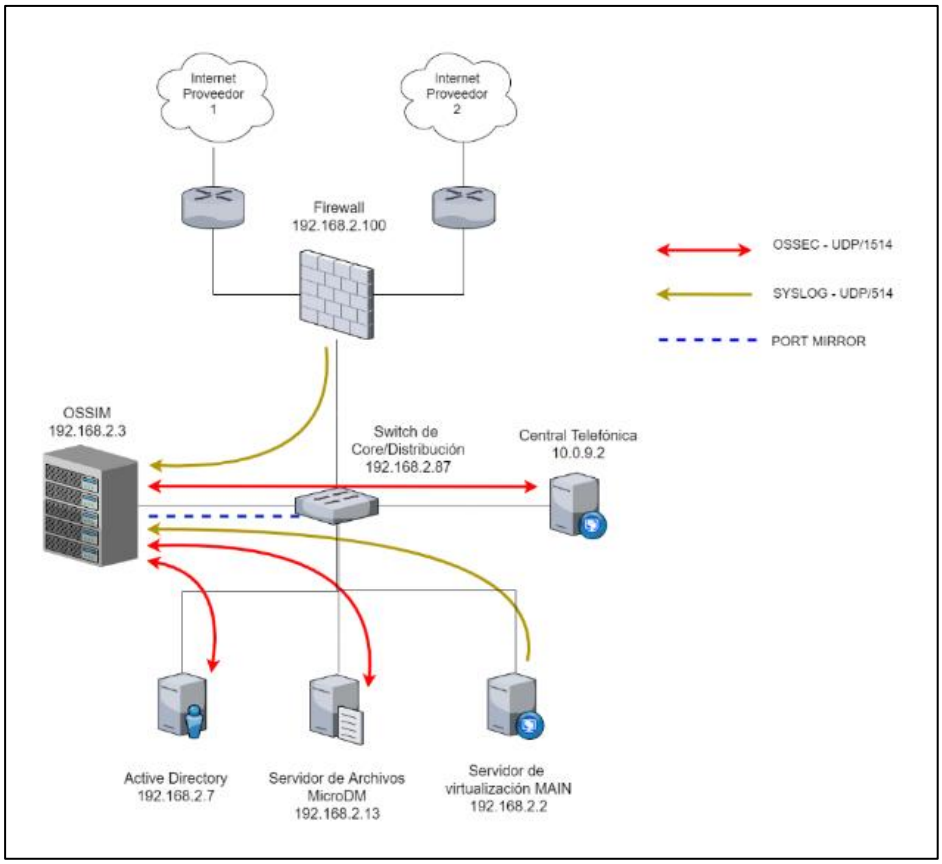


Figura 1.1 Diagrama de red

La primera versión de Magerit fue desarrollada por el Consejo Superior de Administración Electrónica del Gobierno de España en 1997. Actualmente se encuentra en la tercera versión, y la misma se ha adaptado al cambio e implementación de normas internacionales ISO [3].

1.3.1.1 Objetivos de Magerit

De acuerdo con el Libro I de MAGERIT, titulado “Método”, los objetivos que persigue la metodología son los siguientes:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

1.3.1.2 Organización de Guías

La versión 3 de Magerit que se encuentra vigente, está estructurada en dos libros y una guía de técnicas:

- **Libro I – Método:** En este libro se presentan conceptos y describe las actividades de análisis y tratamiento dentro de un proceso. De la misma forma incluye actividades, describe opciones y anticipa problemas con respecto al análisis de riesgos. Método de Análisis de Riesgos, Proyecto de Análisis de Riesgos y Plan de Seguridad.
- **Libro II - Catálogo de Elementos:** En este libro se marcan las pautas con respecto a: tipos de activos, dimensión de valoración de los mismo, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información.
- **Libro III - Guía de Técnicas:** Aporta luz adicional y orientación sobre algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos.

1.3.2 SECURITY INFORMATION AND EVENT MANAGEMENT

Actualmente las organizaciones cuentan con una gran cantidad de equipos de red dentro de sus infraestructuras. Estos equipos generan una gran cantidad de información de eventos que registran acciones realizadas dentro del mismo, a estos registros se los conoce como log.

La necesidad de llevar un control sobre grandes cantidades de información generada por estos equipos ha llevado a la creación de tecnologías que ayuden a las tareas de los administradores de red con referencia a la seguridad de información dentro de sus infraestructuras.

Entre estas soluciones tecnológicas se encuentran:

- **SIM:** Gestor de información de seguridad
- **SEM:** Gestor de eventos de seguridad
- **SIEM:** Gestor de eventos e información de seguridad

1.3.2.1 Security Information Management (SIM)

Un gestor de información de seguridad o SIM es un tipo de solución tecnológica que automáticamente reúne logs de eventos a partir de equipos de seguridad como: firewall, servidores proxy, DLP, entre otros. Dentro de información de seguridad se encuentra datos de numerosas fuentes que incluye todo tipo y marcas de equipos de red.

Un SIM traduce los datos registrados a formatos más simplificados y correlacionados. Muchas arquitecturas SIM proveen reportes de seguridad, análisis y reportes para auditorías de cumplimiento como: Sarbanes-oxley, HIPPA, Basel II.

Esta herramienta provee capacidades robustas de administración de logs y tienen la capacidad de almacenar gran cantidad de logs (en orden de terabytes), dando como resultado un alto nivel de compresión de datos.

Dentro de la categoría de SIM, se pueden encontrar soluciones como: Splunk, ArcSight, Log Logic, RSA envision, IBM TCIM, entre otros.

1.3.2.2 Security Event Management (SEM)

Esta solución provee una administración de eventos, análisis en tiempo real de amenazas, visualización, etiquetado, respuesta a incidentes y operaciones de seguridad. Generalmente son basados en herramientas de base de datos SQL como Oracle.

De cierta forma SEM es una mejora a SIM, a pesar de que ambos son vistos desde distintas áreas de la administración de seguridad. Los datos son usualmente tomados desde el computador terminal hasta un repositorio central mediante el uso de SNMP (Simple Network Management Protocol), syslog u otro protocolo de comunicación.

El repositorio central asegura un almacenamiento seguro de los eventos y alertas registrados durante el funcionamiento de este.

La información recolectada es entonces analizada con algoritmos y cálculos estadísticos para identificar amenazas, vulnerabilidades y riesgos presentes en la red. El SEM tiene la capacidad de normalizar entradas para identificar información de importancia a medida que los datos llegan a la central, y de esta forma notificar a la persona encargada si una entrada requiere de mayor atención o revisión.

Dentro de las soluciones comerciales de SEM se encuentran: SolarWinds SEM.

1.3.2.3 Security Information and Event Management (SIEM)

Un gestor de eventos e información de seguridad, por sus siglas en inglés SIEM (Security Information and Event Manager), es una plataforma capaz de recolectar, registrar y analizar

eventos de aplicaciones y sistemas. Se puede considerar que es el resultado de la fusión de los conceptos de SIM y SEM. Para que una herramienta pueda ser considerada como SIEM debe tener la capacidad de correlacionar eventos de los distintos dispositivos de red.

La recolección de estos eventos puede ser en tiempo real o cercano al mismo. La importancia de que las organizaciones cuenten con una plataforma SIEM ha ido creciendo con el tiempo ya que es una herramienta avanzada que permite la administración de una gran cantidad de eventos provenientes de varias fuentes como: firewall, consola de antivirus, DLP, Directorio Activo, entre otros.

1.3.2.3.1 Capacidades de SIEM

La arquitectura de SIEM integra varios componentes, los mismos que se han desarrollado basándose en la gestión de logs. En la Figura 1.2 se muestran las capacidades que manejan esta plataforma.

Los principales componentes de arquitectura de un SIEM son los siguientes:

- **Sensores**

Equipos de seguridad encargados de capturar la información generada por los diversos equipos de red a monitorear. Cualquier dispositivo que intervenga en la seguridad de la organización debería ser considerado conectarse hacia el SIEM.

- **Recolección de logs**

Como se ha mencionado anteriormente, la recolección de logs se refiere al traslado de los registros hacia el equipo SIEM. Se pueden implementar dos métodos para la recolección de logs: “pull method” y “push method”. Dentro de “pull method”, se necesita una petición de conexión iniciada por el SIEM para extraer los logs del equipo solicitado, por otra parte, en “push method” el envío de logs es constante y en tiempo real mientras estos son generados.

- **Filtrado y normalización de logs.**

Los logs provenientes de diferentes sensores y equipos adoptan un formato que depende del funcionamiento de estos. El formato utilizado es distinto dependiendo de la fuente y puede seguir distintos estándares para la generación de estos. El SIEM debe tener la capacidad de normalizar los distintos formatos provenientes de los sensores para facilitar la lectura y permitir un solo formato estándar para la posterior correlación de los eventos.

- **Reglas de correlación**

El SIEM cuenta con la capacidad de generar alertas vía visualización, mensajería, entre otros, de todos los incidentes que activan las reglas de seguridad establecidas en el mismo. Estas alertas deben ser generadas por la asociación de diferentes incidentes con el objetivo de evitar falsos positivos y no generar falsas alertas que opaquen alarmas importantes en la red. Por ejemplo, una equivocación en el ingreso de datos de una persona no debe confundirse por una alarma de ataque de fuerza bruta.

- **Almacenamiento de logs**

Ya que SIEM trabaja con grandes volúmenes de registros y aplica reglas de retención en los mismos, se necesita de un buen dimensionamiento de almacenamiento, el mismo que puede resultar en una base de datos como Oracle Database, MySQL, entre otros. Dependiendo del volumen de logs generados se puede considerar utilizar varios nodos de almacenamiento formando clústeres.

- **Monitorización**

Es la parte final de la arquitectura SIEM. Una vez que los logs se hayan recolectado y procesado, se requiere la capacidad de acceder a la información almacenada mediante búsquedas inteligentes, además de presentar informes, gráficos entre otros. La etapa de monitorización de SIEM hace que se pueda visualizar en un único lugar el estado de todos los sensores conectados hacia el mismo. Y facilita el poder desarrollar nuevas reglas que extraen información de los eventos que se encuentran procesando en el SIEM.

1.3.3 OSSIM

OSSIM es la abreviatura de Open Source Security Information Management System (es una colección de herramientas bajo la licencia GPL) desarrollado para gestionar la seguridad de red en las empresas.

OSSIM es una aplicación compleja, ya que se compone de múltiples soluciones de código abierto de seguridad para el monitoreo y localización de patrones de redes como: Nessus, Snort, Nmap, Ntop, Nagios, entre otras, incorporándolas en una arquitectura que se servirá de todas sus capacidades para ampliar la seguridad de las redes.

El uso de OSSIM provee de algunas ventajas siendo la principal la de facilitar una gestión de red de forma eficiente y centralizada, además de ser una plataforma gratuita.

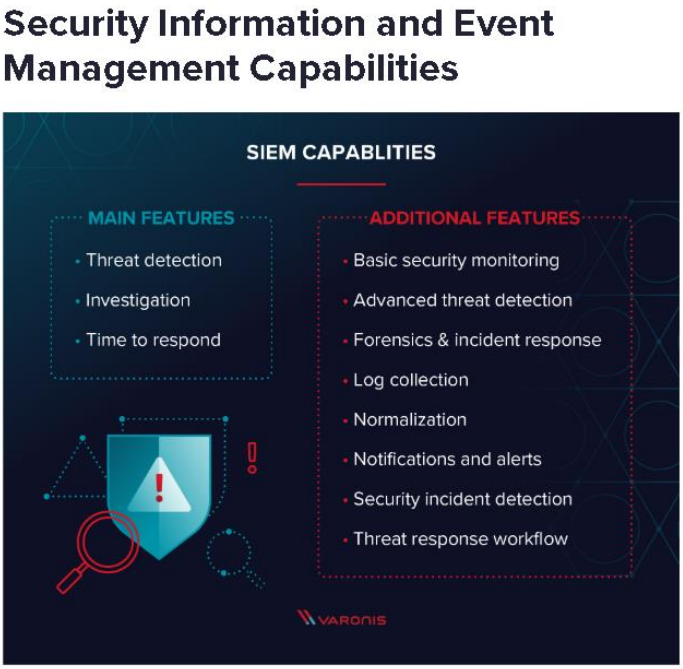


Figura 1.2. Capacidades de un SIEM [9]

1.3.3.1 Capas de OSSIM

OSSIM se encuentra organizado en tres capas, las cuales cumplen funciones específicas como se muestra en la Figura 1.3

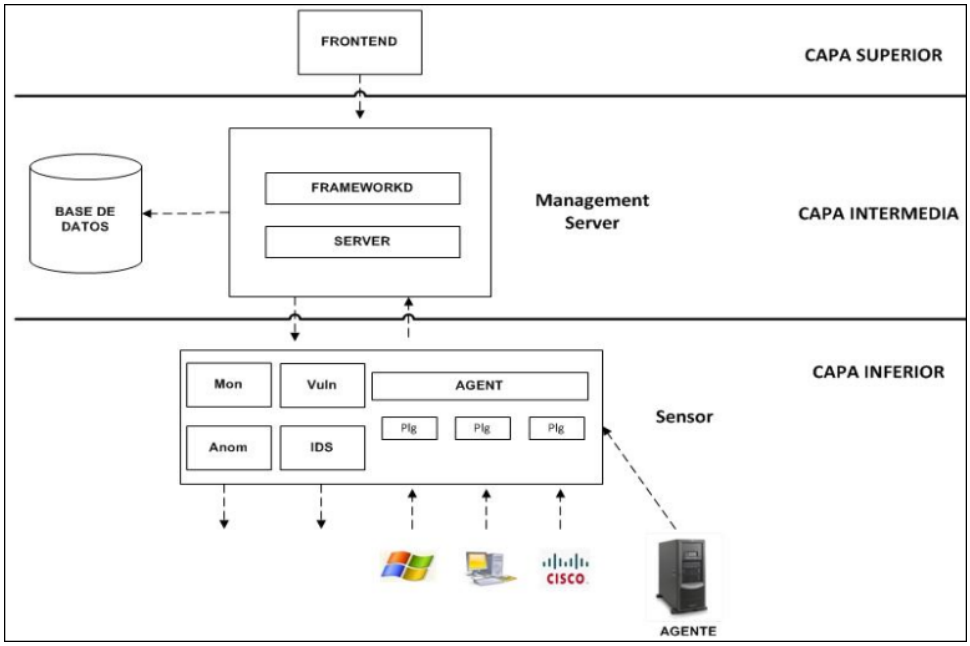


Figura 1.3. Capas de OSSIM [9]

1.3.3.1.1 Capa Inferior

Conocida como Preprocesador, el cual se encarga de la recolección de datos a través de un conjunto de sensores y monitores. En esta capa se encuentran todos los equipos a monitorear.

1.3.3.1.2 Capa Intermedia

Conocida como post-procesado, encargada de cumplir el procesamiento y análisis de datos recolectados por la capa inferior. Aquí entra en funcionamiento lo que es la correlación de eventos para otorgar niveles de prioridad y valorar el riesgo que se puede dar en el sistema.

Aquí se llevan a cabo tareas como normalización, correlación, priorización y valoración de riesgos. Se pueden distinguir tres elementos importantes.

- **Base de datos de eventos:** Almacena todos los logs generados por los sensores dispersos en la red.
- **Base de datos de Framework:** Almacena las configuraciones desde las políticas de seguridad aplicadas para poder identificar el tipo de información que se genera en los dispositivos de la red.
- **Base de datos de Perfiles:** Almacena los datos aprendidos en el monitoreo continuo de la red discriminarlos y tomar las precauciones necesarias para eventos futuros.

1.3.3.1.3 Capa Superior

Corresponde el framework, o front-end, lo cual incluye la consola web de administración. La misma que permite la configuración y visualización de todos los módulos que constituyen el sistema de seguridad. En esta consola se definen topologías, inventario de activos, políticas de seguridad, reglas de correlación.

1.3.3.2 Componentes de OSSIM

OSSIM se compone de tres programas internos en su sistema operático: ossim-server, ossim-framework y ossim-agent. Además, tiene su propia base de datos encargada de recopilar eventos.

1.3.3.2.1 Ossim-server

Se ejecuta en segundo plano y se conecta con la base de datos para obtener e ingresar datos desde los agentes y el framework. Sus funciones principales son:

- Recolectar datos desde agentes

- Priorizar eventos recibidos
- Correlacionar eventos recibidos desde fuentes
- Realizar evaluación de riesgos
- Disparar alarmas

1.3.3.2.2 Ossim- framework

Se encarga de la ejecución de tares misceláneas dentro de la plataforma, las cuales no se pueden realizar por los agentes, server o el front-end. Este accede tanto a la base de datos de OSSIM como a la base de datos de los eventos.

Entre sus funciones se encuentra:

- Leer y escribir archivos del filesystem, evitando que el servidor web lo haga directamente.
- Ejecutar comandos externos
- Ejecutar en segundo plano tareas que requieran uso intensivo de CPU

1.3.3.2.3 Ossim- Agent

Es un ejecutable que es instalado en cada máquina que se requiera ser utilizada como sensor (equipos terminales de usuarios). Los agentes OSSEC son encargados de recolectar datos de los distintos dispositivos, estandarizar los mismos y enviarlos hacia el servidor SIEM

1.3.3.3 Herramientas de OSSIM

1.3.3.3.1 SNORT

Utilizado como Sistema Detector de Intrusos (IDS), encargado de realizar el análisis de tráfico de red a través de la inspección del contenido de los paquetes que envían y reciben los equipos conectados a la red. Snort realiza el análisis de la red, generalmente a través de un puerto SPAN (Switched Port Analyzer) y mediante un catálogo de reglas predefinidas se determina si el tráfico es malicioso o no. Cada regla tiene como parámetros de análisis direcciones IP origen y destino, puertos utilizados y contenido del mensaje, lo cual permite ser muy flexible al usuario para la creación de reglas personalizadas.

1.3.3.3.2 OSSEC

OSSEC permite tener las capacidades de detección de intrusiones a nivel de host, a través del análisis de los datos que se generen en cada equipo y así validar posibles ataques

intencionados. Esta actividad se realiza mediante el análisis de logs, monitoreo de integridad de archivos, modificación de llaves de registro, detección de rootkits. OSSEC se encuentra formado por una plataforma central (mánager), el cual recibe los datos de los equipos ya sea por agentes, protocolo syslog o mediante consultas directas a las fuentes (agentless) como se indica en la Figura 1.4.

Figura 1.4 Arquitectura OSSEC [6]

Los agentes son programas que se encuentran instalados en los equipos que se realiza el monitoreo y son los encargados de enviar la información a la plataforma central.

1.3.3.3.3 NESSUS

La herramienta Nessus permite el escaneo de vulnerabilidades periódico en una red, a través de tareas secuenciales como la detección de puertos abiertos, ejecución de scripts específicos y la generación de informes detallados con las vulnerabilidades encontradas en cada equipo indicando la severidad que representa y las posibles formas de mitigar la amenaza.

1.3.3.3.4 NAGIOS

Permite llevar a cabo el monitoreo de redes mediante la visibilidad del estado de cada activo en la red utilizando principalmente el protocolo SNMP o un cliente Nagios como se indica en la Figura 1.5. Adicionalmente, puede generar alertas en caso de detectar umbrales de monitoreo o fallas presentes en los equipos.

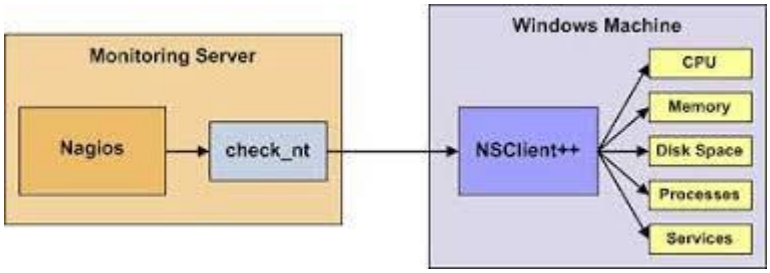


Figura 1.5 Cliente Nagios [10]

1.3.3.3.5 FROBE

Colecta información que llega a las interfaces de red y las convierte en flujos Netflow para que sean usados por herramientas de análisis de flujo.

1.3.3.3.6 NFSen

Genera gráficas de flujos utilizando los datos de Netflow, lo cual permite aplicar filtros y generar alarmas basadas en las condiciones que se haya predeterminado. Adicionalmente, permite la creación de vistas y almacenarlos como históricos para su uso posterior.

1.3.3.3.7 NTOP

Permite la visualización de estadísticas en tiempo real del tráfico que circula a través de las interfaces de OSSIM. Genera alertas utilizando filtros específicos y umbrales establecidos.

1.3.3.3.8 PADS (Passive Asset Detection System)

Sistema de detección pasiva de activos el cual permite la detección de equipos conectados a la red a través de un análisis de tráfico, con el cual se puede obtener información de servicios utilizados, violación de políticas y correlación de eventos.

1.3.3.3.9 NMAP (Network Mapper)

Escáner de red que permite la detección de servicios activos en los equipos presentes en la red y administrar los resultados a través de la consola web.

1.3.3.3.10 Nikto

Enfocado en el escaneo de servidores web, permite realizar diferentes pruebas de detección de vulnerabilidades y configuraciones erróneas en los sistemas

1.3.3.3.11 ARPwatch

Detecta cambios en las direcciones MACs de los sistemas conectados a la red mediante una base de datos local, en la cual asocia cada dirección IP a una dirección MAC específica y alerta sobre cambios detectados.

1.3.4 PROTOCOLO SYSLOG

El protocolo syslog, especificado en el RFC 5424, es un método estandarizado por la industria que permite registrar e informar eventos que ocurren en un dispositivo determinado. La mayoría de los equipos de red como switch, firewall, router tienen la capacidad de generar mensajes syslog, que pueden ser dirigidos hacia una unidad remota de almacenamiento o hacia un equipo específico que realizará el análisis de dichos mensajes como lo hace un SIEM.

Para la utilización de este protocolo en la realización de un análisis de eventos, es necesario considerar qué tipo de mensajes son necesarios llevar la trazabilidad, ya que estos mensajes van a variar de dispositivo en dispositivo.

2. METODOLOGÍA

En el presente capítulo se detallan los procesos de análisis de riesgos, selección de activos a monitorear, diseño y despliegue de un sistema de gestión de eventos e información de seguridad que toma como referencia la información proporcionada por la empresa GMS. El análisis de riesgos se lo realizará a al menos 10 activos de información, de los cuales se seleccionará a al menos 5 activos críticos para la integración con la plataforma OSSIM.

También, se presenta el diseño de directivas específicas para la detección de ataques de fuerza bruta (basado en accesos fallidos y correctos), cambios en la configuración de los equipos (basado en la creación de usuarios) y la detección de conexiones desde equipos dentro de la red local hacia direcciones IP catalogadas como maliciosas, la implementación de estas a través del despliegue de la plataforma OSSIM, y la integración de los 5 activos críticos al monitoreo.

2.1 ANÁLISIS DE RIESGOS

Para el análisis de riesgo se utiliza la metodología MAGERIT v3 [3], la cual permite tener una aproximación en la determinación del riesgo presente en los activos correspondientes a una organización. De acuerdo con esta metodología se van a utilizar los pasos presentados a continuación para el cálculo del riesgo:

1. Determinación de los activos de la organización
2. Determinación de las amenazas que están expuestos los activos
3. Estimación del impacto del activo derivado de la materialización de la amenaza
4. Estimación del riesgo referido a la materialización de la amenaza

2.1.1 DETERMINACIÓN DE LOS ACTIVOS

Para la caracterización de los activos se consideraron los activos esenciales que la empresa tiene en su núcleo de negocio.

2.1.1.1 Identificación de los activos

De acuerdo con la información proporcionada por la empresa GMS, se tienen los siguientes activos:

- **[SVM] Servidor de virtualización Main:** Servidor que mantiene las instancias de telefonía, CRM
- **[SAD] Servidor de Active Directory:** Servidor de Directorio Activo para la red perteneciente a GMS.
- **[SMDM] Servidor de Archivos MicroDM:** Servidor que aloja información relacionada a clientes, productos y servicios que ofrece la empresa.
- **[SNAS] Servidor de almacenamiento NAS:** Equipo orientado al almacenamiento en red, el cual permite guardar respaldos de los servidores pertenecientes a GMS.
- **[SMON] Servidor de monitoreo Nagios:** Servidor que permite llevar un monitoreo de disponibilidad de los servidores que se encuentran en red.
- **[SWEB] Servidor WEB:** Servidor encargado de alojar la página web que brinda información a los clientes.
- **[SAV] Servidor de Antivirus:** Equipo que aloja la consola de administración de la plataforma antivirus.
- **[SCRMEC] Servidor de aplicación CRM:** Servidor que aloja la plataforma para gestionar la relación con los clientes en la cual están los datos de los clientes, prospectos y toda la relación hasta el momento de la venta.
- **[SRRHH] Servidor de aplicaciones RRHH:** Equipo que mantiene en ejecución aplicaciones de uso específico para el manejo de nómina.
- **[SSPC] Servidor de aplicación SPC:** Equipo en el cual se encuentra el sistema administrativo contable interno de GMS.
- **[SAI] Servidor de aplicaciones Indicadores:** Equipo que muestra indicadores relacionados al manejo de clientes y tiempos de respuesta.

- **[TEL] Central Telefónica:** Equipo que maneja las comunicaciones entre la línea telefónica y las extensiones internas.
- **[FIRW] Firewall perimetral:** Equipo de seguridad de red que maneja las conexiones entrantes y salientes a internet.
- **[SW] Switch de distribución/acceso:** Equipo de conmutación que maneja la comunicación de red local.

De acuerdo con Magerit, estos activos pueden categorizarse en uno de los siguientes tipos [3]:

- **Datos** que materializan la información (ficheros, copias de respaldo, datos de configuración, credenciales).
- **Servicios auxiliares** que se necesitan para poder organizar el sistema.
- **Las aplicaciones informáticas (software)** que permiten manejar los datos.
- **Los equipos informáticos (hardware)** y que permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar** que complementa el material informático.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las instalaciones** que acogen equipos informáticos y de comunicaciones.
- **Las personas** que explotan u operan todos los elementos anteriormente citados.

La tipificación de los activos permite tener un criterio para la identificación de las amenazas potenciales y los respectivos salvaguardas. Para el alcance de este proyecto se categorizó a los activos en el tipo de **datos**, **servicios y software** porque son los que entran bajo el alcance de un monitoreo utilizando una herramienta SIEM. Esto fue utilizado para la determinación de las amenazas en la sección 2.1.2.1

2.1.1.2 Valoración de los activos

Una vez que se obtiene la identificación de los activos en 2.1.1.1, se realiza una sesión de trabajo con el personal de infraestructura de GMS y la jefatura de servicios gestionados para llevar a cabo la valoración de cada activo utilizando las siguientes preguntas, tomando como consideración las dimensiones de disponibilidad [D], Integridad de los datos [I] y la confidencialidad de los datos [C] para cada activo :

- **Disponibilidad:** ¿Cuál es el daño que se tendría el no poder utilizar el activo?
- **Integridad:** ¿Cuál es el daño que se tendría si la información hubiera sido manipulada?
- **Confidencialidad:** ¿Cuál es el daño que se tendría si la información la conociera personas que no deben?

Como criterios de valoración se toma la escala presentada en la Tabla 2.1 [3]

Tabla 2.1 Criterios de Valoración

Valor	Descripción
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy alto

La valoración que se dio a los activos se presenta en la Tabla 2.2 y el valor que tendría cada activo va a ser representado por el valor más alto presentado en cada dimensión. En el ANEXO A se adjunta la valorización de los activos aceptada por las partes involucradas de GMS.

Tabla 2.2. Valoración de activos

Activos	Dimensiones			Valor Total
	[D]	[I]	[C]	
Servidor de virtualización Main	5	2	2	5
Servidor de Active Directory	5	3	3	5
Servidor de Archivos MicroDM	5	4	4	5
Servidor de almacenamiento NAS	5	4	4	5
Servidor de disponibilidad Nagios	3	3	3	3
Servidor WEB	3	3	3	3
Servidor de Antivirus	3	3	3	4
Servidor de aplicación CRM	4	4	4	4
Servidor de aplicaciones RRHH	3	4	4	4
Servidor de aplicación SPC	5	5	5	5
Servidor de aplicaciones Indicadores	1	1	1	2
Central Telefónica	4	3	2	4
Firewall perimetral	5	4	4	5
Switch de distribución/acceso	4	4	4	4

2.1.2 DETERMINACIÓN DE LAS AMENAZAS

En la metodología Magerit, se ha clasificado a las amenazas en cuatro grupos como se indica a continuación:

- **[N] Desastres Naturales:** Accidentes naturales como terremotos, inundaciones, etc.
- **[I] De origen industrial:** Desastres industriales como fallos eléctricos, contaminación por polvo o suciedad, etc.
- **[E] Errores y fallos no intencionados:** Fallos provocados ticamente de manera accidental por personas que tienen acceso a los sistemas.
- **[A] Ataque intencionados:** Fallos provocados por personas con acceso a los sistemas para obtener algún beneficio o causar perjuicios a los propietarios.

Para el presente proyecto se ha considerado únicamente a las amenazas que se encuentran en los grupos de [E] y [A], ya que son los que se enfocan directamente en la manipulación de la información y están bajo el alcance de una herramienta SIEM.

2.1.2.1 Identificación de las amenazas

Para la identificación de las amenazas se utilizó el Libro II – Catálogo de Elementos [3], en la cual se indica un listado de amenazas para cada grupo como se indicó en la sección 2.1.2 y las dimensiones en la que el activo se vería afectado. Cada amenaza que se encuentra en el listado, indica a qué tipos de activos va a afectar. En este caso [D] Datos/Información, [S] Servicios y [SW] Aplicaciones como se definió en 2.1.1.1.

Por ejemplo, la amenaza [E.1] Errores de los usuarios, está presente en los tipos de activos [D], [S], [SW] y supondrían una afectación en las 3 dimensiones de Integridad, Confidencialidad y Disponibilidad como se indica en la Figura 2.1

Las amenazas consideradas de acuerdo con Magerit son las que se muestran en la Tabla 2.3.

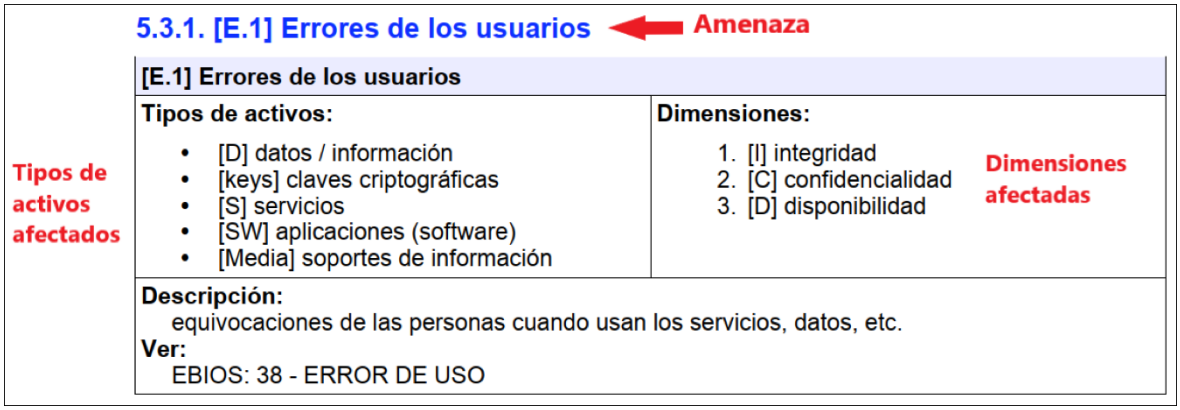


Figura 2.1. Amenaza Errores de los usuarios

Tabla 2.3 Amenazas Identificadas

Amenazas	Tipos de activos afectados		
	Datos	Aplicaciones	Servicios
[E.1] Errores de los usuarios	x	x	x
[E.2] Errores del administrador	x	x	x
[E.3] Errores de monitorización (log)	x		
[E.4] Errores de configuración	x		
[E.8] Difusión de software dañino		x	
[E.9] Errores de [re-]encaminamiento		x	x
[E.10] Errores de secuencia		x	x
[E.15] Alteración accidental de la información	x	x	x
[E.18] Destrucción de información	x	x	x
[E.19] Fugas de información	x	x	x
[E.20] Vulnerabilidades de los programas (software)		x	
[E.21] Errores de mantenimiento / actualización de programas (software)		x	
[E.24] Caída del sistema por agotamiento de recursos			x
[A.3] Manipulación de los registros de actividad (log)	x		
[A.4] Manipulación de la configuración	x		
[A.5] Suplantación de la identidad del usuario	x	x	x
[A.6] Abuso de privilegios de acceso	x	x	x
[A.7] Uso no previsto		x	x
[A.8] Difusión de software dañino		x	
[A.9] [Re-]encaminamiento de mensajes		x	x
[A.10] Alteración de secuencia		x	x
[A.11] Acceso no autorizado	x	x	x
[A.13] Repudio	x		x
[A.15] Modificación deliberada de la información	x	x	x
[A.18] Destrucción de información	x	x	x

Amenazas	Tipos de activos afectados		
	Datos	Aplicaciones	Servicios
[A.19] Divulgación de información	x	x	x
[A.22] Manipulación de programas		x	
[A.24] Denegación de servicio			x

2.1.2.2 Valoración de las amenazas

Cuando se tuvieron las amenazas identificadas como se indicó en la Tabla 2.3, se realizó una sesión de trabajo con el personal de infraestructura y la jefatura de servicios gestionados para evaluar la probabilidad con la que cada amenaza pudiera materializarse en cada activo, y también la degradación (en porcentaje) que causaría la amenaza en cada dimensión del respectivo activo. En el ANEXO B se adjunta la valorización de las amenazas aceptada por las partes involucradas de GMS.

Se utilizó la Tabla 2.4, la cual se indica en [3], para establecer las probabilidades de materialización de cada amenaza

Tabla 2.4 Probabilidad

Valor	Probabilidad
1	Muy bajo
2	Bajo
3	Medio
4	Alto
5	Muy alto

Para la degradación se ha tomado como referencia la Tabla 2.5, la cual se indica en [3]

Tabla 2.5 Degradación

Valor		Criterio
1	Muy alto	Daño extremadamente grave
0,9	Alto	Daño muy grave
0,6 – 0,8	Medio	Daño grave
0,3 – 0,5	Bajo	Daño importante
0,1 – 0,2	Muy bajo	Daño menor

A continuación, se realiza la explicación con un ejemplo de los valores obtenidos contestando a las siguientes preguntas:

Ejemplo de valorización para el activo "Servidor de virtualización Main"

- Amenaza a evaluar = [E.1] Errores de los usuarios

- Dimensión en la que afectaría la amenaza = [D], [I], [C]
- ¿Cuál es la probabilidad de que un usuario no administrador cometa un error?

  Conclusión: Media (3)
- ¿Cuál es la degradación en la disponibilidad [D] si la amenaza ocurriera?

  Conclusión: Bajo (0,5)
- ¿Cuál es la degradación en la integridad [I] si la amenaza ocurriera?

  Conclusión: Muy bajo (0,2)
- ¿Cuál es la degradación en la confidencialidad [C] si la amenaza ocurriera?

  Conclusión: Muy bajo (0,2)

Como resultado de la valorización de las amenazas se tiene la Tabla 2.6

Tabla 2.6 Valorización de amenazas

Activos	Amenazas	Probabilidad	Degradación [D]	Degradación [I]	Degradación [C]
Servidor de virtualización Main	[E.1] Errores de los usuarios	3	0,5	0,2	0,2
	[E.2] Errores del administrador	3	1,0	0,5	0,5
	[E.3] Errores de monitorización (log)	5	-	0,8	-
	[E.4] Errores de configuración	2	-	0,5	-
	[E.8] Disfusión de software dañino	1	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	1	-	-	0,1
	[E.10] Errores de secuencia	1	-	0,1	-
	[E.15] Alteración accidental de la información	3	-	0,5	-
	[E.18] Destrucción de información	2	0,3	-	-
	[E.19] Fugas de información	1	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	1	0,5	0,1	0,1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	2	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	2	-	1,0	-
	[A.4] Manipulación de la configuración	3	0,8	0,8	0,8
	[A.5] Suplantación de la identidad del usuario	2	0,5	0,2	0,2
	[A.6] Abuso de privilegios de acceso	2	0,9	0,5	0,5
	[A.7] Uso no previsto	2	0,7	0,1	0,1
	[A.8] Difusión de software dañino	2	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	1	-	-	0,1
	[A.10] Alteración de secuencia	1	-	0,1	-
	[A.11] Acceso no autorizado	3	-	0,8	0,8
	[A.13] Repudio	5	-	1,0	-

Activos	Amenazas	Probabilidad	Degradación [D]	Degradación [I]	Degradación [C]
	[A.15] Modificación deliberada de la información	2	-	0,5	-
	[A.18] Destrucción de información	2	0,9	-	-
	[A.19] Divulgación de información	2	-	-	0,4
	[A.22] Manipulación de programas	1	1,0	-	-
	[A.24] Denegación de servicio	1	0,7	-	0,2
Servidor de Active Directory	[E.1] Errores de los usuarios	3	0,5	0,2	0,2
	[E.2] Errores del administrador	3	1,0	0,2	0,2
	[E.3] Errores de monitorización (log)	5	-	1,0	-
	[E.4] Errores de configuración	4	-	0,8	-
	[E.8] Disfusión de software dañino	1	1,0	-	-
	[E.9] Errores de [re-]encaminamiento	1	-	-	0,1
	[E.10] Errores de secuencia	1	-	0,1	-
	[E.15] Alteración accidental de la información	4	-	0,5	-
	[E.18] Destrucción de información	2	0,3	-	-
	[E.19] Fugas de información	1	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	1	0,5	0,1	0,1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	2	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	1,0	-
	[A.4] Manipulación de la configuración	3	0,8	0,5	0,2
	[A.5] Suplantación de la identidad del usuario	2	0,5	0,2	0,2
	[A.6] Abuso de privilegios de acceso	3	0,9	0,5	0,5
	[A.7] Uso no previsto	3	0,7	0,1	0,1
	[A.8] Difusión de software dañino	3	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	1	-	-	0,1
	[A.10] Alteración de secuencia	1	-	0,1	-
	[A.11] Acceso no autorizado	3	-	0,5	0,5
	[A.13] Repudio	5	-	1,0	-
	[A.15] Modificación deliberada de la información	2	-	0,5	-
	[A.18] Destrucción de información	2	0,9	-	-
	[A.19] Divulgación de información	2	-	-	0,4
	[A.22] Manipulación de programas	2	1,0	-	-
	[A.24] Denegación de servicio	1	0,7	-	0,2
Servidor de Archivos MicroDM	[E.1] Errores de los usuarios	3	0,5	0,2	0,2
	[E.2] Errores del administrador	3	1,0	0,2	0,2
	[E.3] Errores de monitorización (log)	5	-	1,0	-
	[E.4] Errores de configuración	4	-	0,8	-
	[E.8] Disfusión de software dañino	1	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	1	-	-	0,1
	[E.10] Errores de secuencia	1	-	0,1	-
	[E.15] Alteración accidental de la información	4	-	0,5	-
	[E.18] Destrucción de información	2	0,3	-	-
	[E.19] Fugas de información	3	-	-	0,2

Activos	Amenazas	Probabilidad	Degradación [D]	Degradación [I]	Degradación [C]
	[E.20] Vulnerabilidades de los programas (software)	3	0,5	0,1	0,1
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	1,0	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	2	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	1,0	-
	[A.4] Manipulación de la configuración	4	0,8	0,2	0,2
	[A.5] Suplantación de la identidad del usuario	2	1,0	0,2	0,2
	[A.6] Abuso de privilegios de acceso	4	1,0	0,5	0,5
	[A.7] Uso no previsto	2	0,7	0,1	0,1
	[A.8] Difusión de software dañino	2	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	1	-	-	0,1
	[A.10] Alteración de secuencia	1	-	0,1	-
	[A.11] Acceso no autorizado	3	-	1,0	1,0
	[A.13] Repudio	5	-	1,0	-
	[A.15] Modificación deliberada de la información	3	-	1,0	-
	[A.18] Destrucción de información	3	1,0	-	-
	[A.19] Divulgación de información	3	-	-	0,4
	[A.22] Manipulación de programas	2	1,0	-	-
	[A.24] Denegación de servicio	1	0,7	-	0,2
Servidor de almacenamiento NAS	[E.1] Errores de los usuarios	2	0,5	0,2	0,2
	[E.2] Errores del administrador	2	0,9	0,2	0,2
	[E.3] Errores de monitorización (log)	4	-	0,5	-
	[E.4] Errores de configuración	2	-	0,5	-
	[E.8] Disfusión de software dañino	1	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	1	-	-	0,1
	[E.10] Errores de secuencia	1	-	0,1	-
	[E.15] Alteración accidental de la información	2	-	0,5	-
	[E.18] Destrucción de información	3	0,3	-	-
	[E.19] Fugas de información	1	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	1	0,5	0,1	0,1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	2	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	0,5	-
	[A.4] Manipulación de la configuración	3	0,8	0,2	0,2
	[A.5] Suplantación de la identidad del usuario	2	0,5	0,2	0,2
	[A.6] Abuso de privilegios de acceso	4	0,9	0,5	0,5
	[A.7] Uso no previsto	2	0,7	0,1	0,1
	[A.8] Difusión de software dañino	2	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	1	-	-	0,1
	[A.10] Alteración de secuencia	1	-	0,1	-
	[A.11] Acceso no autorizado	3	-	0,5	0,2
	[A.13] Repudio	4	-	0,5	-
	[A.15] Modificación deliberada de la información	2	-	0,5	-

Activos	Amenazas	Probabilidad	Degradación [D]	Degradación [I]	Degradación [C]
	[A.18] Destrucción de información	2	0,9	-	-
	[A.19] Divulgación de información	2	-	-	0,4
	[A.22] Manipulación de programas	1	1,0	-	-
	[A.24] Denegación de servicio	1	0,7	-	0,2
Servidor de disponibilidad Nagios	[E.1] Errores de los usuarios	2	0,5	0,2	0,2
	[E.2] Errores del administrador	2	0,9	0,2	0,2
	[E.3] Errores de monitorización (log)	4	-	1,0	-
	[E.4] Errores de configuración	3	-	0,5	-
	[E.8] Disfusión de software dañino	1	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	1	-	-	0,1
	[E.10] Errores de secuencia	1	-	0,1	-
	[E.15] Alteración accidental de la información	2	-	0,5	-
	[E.18] Destrucción de información	2	0,3	-	-
	[E.19] Fugas de información	1	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	2	0,5	0,1	0,1
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	3	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	1,0	-
	[A.4] Manipulación de la configuración	2	0,8	0,2	0,2
	[A.5] Suplantación de la identidad del usuario	2	0,5	0,2	0,2
	[A.6] Abuso de privilegios de acceso	2	0,9	0,5	0,5
	[A.7] Uso no previsto	1	0,7	0,1	0,1
	[A.8] Difusión de software dañino	1	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	1	-	-	0,1
	[A.10] Alteración de secuencia	1	-	0,1	-
	[A.11] Acceso no autorizado	2	-	0,5	0,2
	[A.13] Repudio	4	-	0,5	-
	[A.15] Modificación deliberada de la información	2	-	0,5	-
	[A.18] Destrucción de información	2	0,9	-	-
	[A.19] Divulgación de información	2	-	-	0,4
	[A.22] Manipulación de programas	1	1,0	-	-
	[A.24] Denegación de servicio	1	0,7	-	0,2
Servidor WEB	[E.1] Errores de los usuarios	3	0,5	0,2	0,2
	[E.2] Errores del administrador	3	0,9	0,2	0,2
	[E.3] Errores de monitorización (log)	5	-	1,0	-
	[E.4] Errores de configuración	3	-	0,5	-
	[E.8] Disfusión de software dañino	1	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	1	-	-	0,1
	[E.10] Errores de secuencia	1	-	0,1	-
	[E.15] Alteración accidental de la información	2	-	0,5	-
	[E.18] Destrucción de información	1	0,3	-	-
	[E.19] Fugas de información	1	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	1	0,5	0,1	0,1

Activos	Amenazas	Probabilidad	Degradación [D]	Degradación [I]	Degradación [C]
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	2	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	1,0	-
	[A.4] Manipulación de la configuración	3	0,8	0,2	0,2
	[A.5] Suplantación de la identidad del usuario	3	0,5	0,2	0,2
	[A.6] Abuso de privilegios de acceso	4	0,9	0,5	0,5
	[A.7] Uso no previsto	2	0,7	0,1	0,1
	[A.8] Difusión de software dañino	2	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	1	-	-	0,1
	[A.10] Alteración de secuencia	1	-	0,1	-
	[A.11] Acceso no autorizado	3	-	0,5	0,2
	[A.13] Repudio	4	-	0,5	-
	[A.15] Modificación deliberada de la información	3	-	0,5	-
	[A.18] Destrucción de información	3	0,9	-	-
	[A.19] Divulgación de información	2	-	-	0,4
	[A.22] Manipulación de programas	1	1,0	-	-
	[A.24] Denegación de servicio	4	1,0	-	0,2
Servidor de Antivirus	[E.1] Errores de los usuarios	2	0,5	0,2	0,2
	[E.2] Errores del administrador	2	0,9	0,2	0,2
	[E.3] Errores de monitorización (log)	5	-	0,8	-
	[E.4] Errores de configuración	2	-	0,5	-
	[E.8] Disfusión de software dañino	3	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	1	-	-	0,1
	[E.10] Errores de secuencia	1	-	0,1	-
	[E.15] Alteración accidental de la información	3	-	0,5	-
	[E.18] Destrucción de información	2	0,3	-	-
	[E.19] Fugas de información	1	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	2	1,0	0,1	0,1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	2	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	1,0	-
	[A.4] Manipulación de la configuración	2	0,8	0,2	0,2
	[A.5] Suplantación de la identidad del usuario	2	0,5	0,5	0,2
	[A.6] Abuso de privilegios de acceso	4	0,9	0,5	0,5
	[A.7] Uso no previsto	3	0,7	0,1	0,1
	[A.8] Difusión de software dañino	2	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	1	-	-	0,1
	[A.10] Alteración de secuencia	1	-	0,1	-
	[A.11] Acceso no autorizado	2	-	0,5	0,2
	[A.13] Repudio	4	-	0,5	-
	[A.15] Modificación deliberada de la información	2	-	0,5	-
	[A.18] Destrucción de información	2	0,9	-	-

Activos	Amenazas	Probabilidad	Degradación [D]	Degradación [I]	Degradación [C]
	[A.19] Divulgación de información	2	-	-	0,4
	[A.22] Manipulación de programas	1	1,0	-	-
	[A.24] Denegación de servicio	1	0,7	-	0,2
Servidor de aplicación CRM	[E.1] Errores de los usuarios	2	0,5	0,2	0,2
	[E.2] Errores del administrador	2	0,9	0,2	0,2
	[E.3] Errores de monitorización (log)	5	-	0,5	-
	[E.4] Errores de configuración	2	-	0,5	-
	[E.8] Disfusión de software dañino	1	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	1	-	-	0,1
	[E.10] Errores de secuencia	1	-	0,1	-
	[E.15] Alteración accidental de la información	3	-	0,5	-
	[E.18] Destrucción de información	2	0,3	-	-
	[E.19] Fugas de información	2	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	1	0,5	0,1	0,1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	1	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	0,8	-
	[A.4] Manipulación de la configuración	3	0,8	0,2	0,2
	[A.5] Suplantación de la identidad del usuario	2	0,5	0,2	0,2
	[A.6] Abuso de privilegios de acceso	2	0,9	0,5	0,5
	[A.7] Uso no previsto	2	0,7	0,1	0,1
	[A.8] Difusión de software dañino	2	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	1	-	-	0,1
	[A.10] Alteración de secuencia	1	-	0,1	-
	[A.11] Acceso no autorizado	2	-	0,5	0,2
	[A.13] Repudio	4	-	0,5	-
	[A.15] Modificación deliberada de la información	2	-	0,5	-
	[A.18] Destrucción de información	2	0,9	-	-
	[A.19] Divulgación de información	2	-	-	0,4
	[A.22] Manipulación de programas	1	1,0	-	-
	[A.24] Denegación de servicio	1	1,0	-	0,5
Servidor de aplicaciones RRHH	[E.1] Errores de los usuarios	2	0,4	0,4	0,4
	[E.2] Errores del administrador	2	1,0	0,2	0,2
	[E.3] Errores de monitorización (log)	5	-	0,8	-
	[E.4] Errores de configuración	2	-	0,5	-
	[E.8] Disfusión de software dañino	1	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	1	-	-	0,1
	[E.10] Errores de secuencia	1	-	0,1	-
	[E.15] Alteración accidental de la información	2	-	0,5	-
	[E.18] Destrucción de información	2	0,3	-	-
	[E.19] Fugas de información	2	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	1	0,5	0,1	0,1

Activos	Amenazas	Probabilidad	Degradación [D]	Degradación [I]	Degradación [C]
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	1	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	1,0	-
	[A.4] Manipulación de la configuración	3	0,8	0,2	0,2
	[A.5] Suplantación de la identidad del usuario	2	0,5	0,2	0,2
	[A.6] Abuso de privilegios de acceso	3	0,9	0,5	0,5
	[A.7] Uso no previsto	2	0,7	0,1	0,1
	[A.8] Difusión de software dañino	2	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	1	-	-	0,1
	[A.10] Alteración de secuencia	1	-	0,1	-
	[A.11] Acceso no autorizado	3	-	0,8	0,5
	[A.13] Repudio	4	-	0,5	-
	[A.15] Modificación deliberada de la información	2	-	0,5	-
	[A.18] Destrucción de información	2	0,9	-	-
	[A.19] Divulgación de información	2	-	-	0,8
	[A.22] Manipulación de programas	1	1,0	-	-
	[A.24] Denegación de servicio	1	1,0	-	0,5
Servidor de aplicación - SPC	[E.1] Errores de los usuarios	2	0,5	0,2	0,2
	[E.2] Errores del administrador	2	0,9	0,2	0,2
	[E.3] Errores de monitorización (log)	5	-	1,0	-
	[E.4] Errores de configuración	2	-	0,5	-
	[E.8] Disfusión de software dañino	1	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	1	-	-	0,1
	[E.10] Errores de secuencia	1	-	0,1	-
	[E.15] Alteración accidental de la información	2	-	0,5	-
	[E.18] Destrucción de información	2	0,3	-	-
	[E.19] Fugas de información	1	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	2	0,5	0,1	0,1
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	2	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	1,0	-
	[A.4] Manipulación de la configuración	2	0,8	0,2	0,2
	[A.5] Suplantación de la identidad del usuario	2	0,5	0,2	0,2
	[A.6] Abuso de privilegios de acceso	4	0,9	0,5	0,5
	[A.7] Uso no previsto	2	0,7	0,1	0,1
	[A.8] Difusión de software dañino	2	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	1	-	-	0,1
	[A.10] Alteración de secuencia	1	-	0,1	-
	[A.11] Acceso no autorizado	2	-	0,5	0,2
	[A.13] Repudio	4	-	0,5	-
	[A.15] Modificación deliberada de la información	2	-	0,5	-
	[A.18] Destrucción de información	2	0,9	-	-

Activos	Amenazas	Probabilidad	Degradación [D]	Degradación [I]	Degradación [C]
	[A.19] Divulgación de información	2	-	-	0,4
	[A.22] Manipulación de programas	1	1,0	-	-
	[A.24] Denegación de servicio	1	1,0	-	0,1
Servidor de aplicación - Indicadores	[E.1] Errores de los usuarios	2	0,5	0,2	0,2
	[E.2] Errores del administrador	2	0,9	0,2	0,2
	[E.3] Errores de monitorización (log)	5	-	1,0	-
	[E.4] Errores de configuración	2	-	0,5	-
	[E.8] Disfusión de software dañino	1	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	1	-	-	0,1
	[E.10] Errores de secuencia	1	-	0,1	-
	[E.15] Alteración accidental de la información	2	-	0,5	-
	[E.18] Destrucción de información	2	0,3	-	-
	[E.19] Fugas de información	1	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	3	0,5	0,1	0,1
	[E.21] Errores de mantenimiento / actualización de programas (software)	3	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	2	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	1,0	-
	[A.4] Manipulación de la configuración	2	0,8	0,2	0,2
	[A.5] Suplantación de la identidad del usuario	2	0,5	0,2	0,2
	[A.6] Abuso de privilegios de acceso	4	0,9	0,5	0,5
	[A.7] Uso no previsto	4	0,7	0,1	0,1
	[A.8] Difusión de software dañino	2	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	1	-	-	0,1
	[A.10] Alteración de secuencia	1	-	0,1	-
	[A.11] Acceso no autorizado	2	-	0,5	0,2
	[A.13] Repudio	4	-	0,5	-
	[A.15] Modificación deliberada de la información	2	-	0,5	-
	[A.18] Destrucción de información	2	0,9	-	-
	[A.19] Divulgación de información	2	-	-	0,4
	[A.22] Manipulación de programas	1	1,0	-	-
	[A.24] Denegación de servicio	1	0,7	-	0,2
Central Telefónica	[E.1] Errores de los usuarios	2	0,5	0,2	0,2
	[E.2] Errores del administrador	3	1,0	0,2	0,2
	[E.3] Errores de monitorización (log)	5	-	1,0	-
	[E.4] Errores de configuración	3	-	0,5	-
	[E.8] Disfusión de software dañino	2	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	2	-	-	0,5
	[E.10] Errores de secuencia	3	-	0,5	-
	[E.15] Alteración accidental de la información	3	-	0,5	-
	[E.18] Destrucción de información	2	0,3	-	-
	[E.19] Fugas de información	1	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	1	0,5	0,1	0,1

Activos	Amenazas	Probabilidad	Degradación [D]	Degradación [I]	Degradación [C]
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	2	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	1,0	-
	[A.4] Manipulación de la configuración	4	0,8	0,2	0,2
	[A.5] Suplantación de la identidad del usuario	3	0,9	0,9	0,9
	[A.6] Abuso de privilegios de acceso	4	1,0	0,9	0,9
	[A.7] Uso no previsto	3	0,7	0,1	0,1
	[A.8] Difusión de software dañino	2	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	2	-	-	0,5
	[A.10] Alteración de secuencia	2	-	0,5	-
	[A.11] Acceso no autorizado	4	-	0,9	0,8
	[A.13] Repudio	4	-	1,0	-
	[A.15] Modificación deliberada de la información	3	-	0,5	-
	[A.18] Destrucción de información	3	0,9	-	-
	[A.19] Divulgación de información	2	-	-	0,4
	[A.22] Manipulación de programas	1	1,0	-	-
	[A.24] Denegación de servicio	1	1,0	-	0,2
Firewall perimetral	[E.1] Errores de los usuarios	2	0,5	0,2	0,2
	[E.2] Errores del administrador	3	0,9	0,2	0,2
	[E.3] Errores de monitorización (log)	5	-	1,0	-
	[E.4] Errores de configuración	3	-	0,5	-
	[E.8] Disfusión de software dañino	1	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	2	-	-	0,5
	[E.10] Errores de secuencia	2	-	0,5	-
	[E.15] Alteración accidental de la información	3	-	0,5	-
	[E.18] Destrucción de información	2	0,3	-	-
	[E.19] Fugas de información	1	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	1	0,5	0,1	0,1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	2	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	1,0	-
	[A.4] Manipulación de la configuración	4	0,8	0,8	0,8
	[A.5] Suplantación de la identidad del usuario	3	0,9	0,5	0,2
	[A.6] Abuso de privilegios de acceso	4	0,9	0,5	0,5
	[A.7] Uso no previsto	2	0,7	0,1	0,1
	[A.8] Difusión de software dañino	2	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	3	-	-	0,5
	[A.10] Alteración de secuencia	3	-	0,5	-
	[A.11] Acceso no autorizado	3	-	1,0	0,5
	[A.13] Repudio	5	-	1,0	-
	[A.15] Modificación deliberada de la información	4	-	0,5	-
	[A.18] Destrucción de información	2	0,9	-	-

Activos	Amenazas	Probabilidad	Degradación [D]	Degradación [I]	Degradación [C]
	[A.19] Divulgación de información	3	-	-	0,4
	[A.22] Manipulación de programas	1	1,0	-	-
	[A.24] Denegación de servicio	1	0,7	-	0,2
Switch de distribución/acceso	[E.1] Errores de los usuarios	2	0,5	0,5	0,5
	[E.2] Errores del administrador	3	1,0	0,5	0,2
	[E.3] Errores de monitorización (log)	4	-	1,0	-
	[E.4] Errores de configuración	3	-	0,5	-
	[E.8] Disfusión de software dañino	1	0,1	-	-
	[E.9] Errores de [re-]encaminamiento	2	-	-	0,5
	[E.10] Errores de secuencia	2	-	0,5	-
	[E.15] Alteración accidental de la información	3	-	0,5	-
	[E.18] Destrucción de información	2	0,3	-	-
	[E.19] Fugas de información	1	-	-	0,2
	[E.20] Vulnerabilidades de los programas (software)	1	0,5	0,1	0,1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	0,5	0,2	-
	[E.24] Caída del sistema por agotamiento de recursos	2	1,0	-	-
	[A.3] Manipulación de los registros de actividad (log)	4	-	1,0	-
	[A.4] Manipulación de la configuración	4	0,8	0,8	0,8
	[A.5] Suplantación de la identidad del usuario	3	0,5	0,2	0,2
	[A.6] Abuso de privilegios de acceso	4	0,9	0,9	0,5
	[A.7] Uso no previsto	2	0,7	0,1	0,1
	[A.8] Difusión de software dañino	2	1,0	0,5	0,5
	[A.9] [Re-]encaminamiento de mensajes	3	-	-	0,5
	[A.10] Alteración de secuencia	3	-	0,5	-
	[A.11] Acceso no autorizado	4	-	0,5	0,2
	[A.13] Repudio	4	-	1,0	-
	[A.15] Modificación deliberada de la información	3	-	0,5	-
	[A.18] Destrucción de información	3	0,9	-	-
	[A.19] Divulgación de información	2	-	-	0,4
	[A.22] Manipulación de programas	1	1,0	-	-
	[A.24] Denegación de servicio	1	0,7	-	0,2

2.1.3 ESTIMACIÓN DEL IMPACTO

El impacto puede catalogarse como la medida que tendría el daño ocasionado por la materialización de una amenaza. Una vez que se definió el valor de cada activo en la sección 2.1.1.2 y la degradación que produce la amenaza en cada dimensión en la sección 2.1.2.2, se puede estimar el impacto que tendría la amenaza sobre el activo, realizando la multiplicación de estos valores.

En la Tabla 2.7 se puede observar la estimación del impacto calculada a partir del valor de cada activo y la degradación que produciría la amenaza en cada dimensión obtenida de la Tabla 2.6.

A continuación, se realiza un ejemplo de cálculo para la estimación del impacto para el Servidor de virtualización Main.

Ejemplo de cálculo para el activo "Servidor de virtualización Main"

- Valor del activo = 5
- Amenaza a evaluar = [E.1] Errores de los usuarios
- Dimensión en la que afectaría la amenaza = [D], [I], [C]
- Impacto en la Disponibilidad = 5 x 0,5 = 2,5
- Impacto en la Integridad = 5 x 0,2 = 1
- Impacto en la Confidencialidad = 5 x 0,2 = 1
- Impacto promedio de la amenaza = 4,5 ÷ 3 = 1,5

Tabla 2.7 Estimación del Impacto

Activos	Valor	Amenazas	[D]	[I]	[C]	Impacto D	Impacto I	Impacto C	Impacto Promedio
Servidor de virtualización Main	5	[E.1] Errores de los usuarios	0,5	0,2	0,2	2,5	1,0	1,0	1,5
		[E.2] Errores del administrador	1,0	0,5	0,5	5,0	2,5	2,5	3,3
		[E.3] Errores de monitorización (log)	-	0,8	-	-	4,0	-	4,0
		[E.4] Errores de configuración	-	0,5	-	-	2,5	-	2,5
		[E.8] Disfusión de software dañino	0,1	-	-	0,5	-	-	0,5
		[E.9] Errores de [re-]encaminamiento	-	-	0,1	-	-	0,5	0,5
		[E.10] Errores de secuencia	-	0,1	-	-	0,5	-	0,5
		[E.15] Alteración accidental de la información	-	0,5	-	-	2,5	-	2,5
		[E.18] Destrucción de información	0,3	-	-	1,5	-	-	1,5
		[E.19] Fugas de información	-	-	0,2	-	-	1,0	1,0
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	2,5	0,5	0,5	1,2
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	2,5	1,0	-	1,8
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	5,0	-	-	5,0
		[A.3] Manipulación de los registros de actividad (log)	-	1,0	-	-	5,0	-	5,0
		[A.4] Manipulación de la configuración	0,8	0,8	0,8	4,0	4,0	4,0	4,0

Activos	Valor	Amenazas	[D]	[I]	[C]	Impacto D	Impacto I	Impacto C	Impacto Promedio
		[A.5] Suplantación de la identidad del usuario	0,5	0,2	0,2	2,5	1,0	1,0	1,5
		[A.6] Abuso de privilegios de acceso	0,9	0,5	0,5	4,5	2,5	2,5	3,2
		[A.7] Uso no previsto	0,7	0,1	0,1	3,5	0,5	0,5	1,5
		[A.8] Difusión de software dañino	1,0	0,5	0,5	5,0	2,5	2,5	3,3
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,1	-	-	0,5	0,5
		[A.10] Alteración de secuencia	-	0,1	-	-	0,5	-	0,5
		[A.11] Acceso no autorizado	-	0,8	0,8	-	4,0	4,0	4,0
		[A.13] Repudio	-	1,0	-	-	5,0	-	5,0
		[A.15] Modificación deliberada de la información	-	0,5	-	-	2,5	-	2,5
		[A.18] Destrucción de información	0,9	-	-	4,5	-	-	4,5
		[A.19] Divulgación de información	-	-	0,4	-	-	2,0	2,0
		[A.22] Manipulación de programas	1,0	-	-	5,0	-	-	5,0
		[A.24] Denegación de servicio	0,7	-	0,2	3,5	-	1,0	2,3
Servidor de Active Directory	5	[E.1] Errores de los usuarios	0,5	0,2	0,2	2,5	1,0	1,0	1,5
		[E.2] Errores del administrador	1,0	0,2	0,2	5,0	1,0	1,0	2,3
		[E.3] Errores de monitorización (log)	-	1,0	-	-	5,0	-	5,0
		[E.4] Errores de configuración	-	0,8	-	-	4,0	-	4,0
		[E.8] Disfusión de software dañino	1,0	-	-	5,0	-	-	5,0
		[E.9] Errores de [re-]encaminamiento	-	-	0,1	-	-	0,5	0,5
		[E.10] Errores de secuencia	-	0,1	-	-	0,5	-	0,5
		[E.15] Alteración accidental de la información	-	0,5	-	-	2,5	-	2,5
		[E.18] Destrucción de información	0,3	-	-	1,5	-	-	1,5
		[E.19] Fugas de información	-	-	0,2	-	-	1,0	1,0
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	2,5	0,5	0,5	1,2
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	2,5	1,0	-	1,8
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	5,0	-	-	5,0
		[A.3] Manipulación de los registros de actividad (log)	-	1,0	-	-	5,0	-	5,0
		[A.4] Manipulación de la configuración	0,8	0,5	0,2	4,0	2,5	1,0	2,5
		[A.5] Suplantación de la identidad del usuario	0,5	0,2	0,2	2,5	1,0	1,0	1,5
		[A.6] Abuso de privilegios de acceso	0,9	0,5	0,5	4,5	2,5	2,5	3,2
		[A.7] Uso no previsto	0,7	0,1	0,1	3,5	0,5	0,5	1,5
		[A.8] Difusión de software dañino	1,0	0,5	0,5	5,0	2,5	2,5	3,3
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,1	-	-	0,5	0,5
		[A.10] Alteración de secuencia	-	0,1	-	-	0,5	-	0,5
		[A.11] Acceso no autorizado	-	0,5	0,5	-	2,5	2,5	2,5
		[A.13] Repudio	-	1,0	-	-	5,0	-	5,0

Activos	Valor	Amenazas	[D]	[I]	[C]	Impacto D	Impacto I	Impacto C	Impacto Promedio
		[A.15] Modificación deliberada de la información	-	0,5	-	-	2,5	-	2,5
		[A.18] Destrucción de información	0,9	-	-	4,5	-	-	4,5
		[A.19] Divulgación de información	-	-	0,4	-	-	2,0	2,0
		[A.22] Manipulación de programas	1,0	-	-	5,0	-	-	5,0
		[A.24] Denegación de servicio	0,7	-	0,2	3,5	-	1,0	2,3
Servidor de Archivos MicroDM	4	[E.1] Errores de los usuarios	0,5	0,2	0,2	2,0	0,8	0,8	1,2
		[E.2] Errores del administrador	1,0	0,2	0,2	4,0	0,8	0,8	1,9
		[E.3] Errores de monitorización (log)	-	1,0	-	-	4,0	-	4,0
		[E.4] Errores de configuración	-	0,8	-	-	3,2	-	3,2
		[E.8] Disfusión de software dañino	0,1	-	-	0,4	-	-	0,4
		[E.9] Errores de [re-]encaminamiento	-	-	0,1	-	-	0,4	0,4
		[E.10] Errores de secuencia	-	0,1	-	-	0,4	-	0,4
		[E.15] Alteración accidental de la información	-	0,5	-	-	2,0	-	2,0
		[E.18] Destrucción de información	0,3	-	-	1,2	-	-	1,2
		[E.19] Fugas de información	-	-	0,2	-	-	0,8	0,8
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	2,0	0,4	0,4	0,9
		[E.21] Errores de mantenimiento / actualización de programas (software)	1,0	0,2	-	4,0	0,8	-	2,4
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	4,0	-	-	4,0
		[A.3] Manipulación de los registros de actividad (log)	-	1,0	-	-	4,0	-	4,0
		[A.4] Manipulación de la configuración	0,8	0,2	0,2	3,2	0,8	0,8	1,6
		[A.5] Suplantación de la identidad del usuario	1,0	0,2	0,2	4,0	0,8	0,8	1,9
		[A.6] Abuso de privilegios de acceso	1,0	0,5	0,5	4,0	2,0	2,0	2,7
		[A.7] Uso no previsto	0,7	0,1	0,1	2,8	0,4	0,4	1,2
		[A.8] Difusión de software dañino	1,0	0,5	0,5	4,0	2,0	2,0	2,7
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,1	-	-	0,4	0,4
		[A.10] Alteración de secuencia	-	0,1	-	-	0,4	-	0,4
		[A.11] Acceso no autorizado	-	1,0	1,0	-	4,0	4,0	4,0
		[A.13] Repudio	-	1,0	-	-	4,0	-	4,0
		[A.15] Modificación deliberada de la información	-	1,0	-	-	4,0	-	4,0
		[A.18] Destrucción de información	1,0	-	-	4,0	-	-	4,0
		[A.19] Divulgación de información	-	-	0,4	-	-	1,6	1,6
		[A.22] Manipulación de programas	1,0	-	-	4,0	-	-	4,0
		[A.24] Denegación de servicio	0,7	-	0,2	2,8	-	0,8	1,8
Servidor de almacenamiento NAS	5	[E.1] Errores de los usuarios	0,5	0,2	0,2	2,5	1,0	1,0	1,5
		[E.2] Errores del administrador	0,9	0,2	0,2	4,5	1,0	1,0	2,2
		[E.3] Errores de monitorización (log)	-	0,5	-	-	2,5	-	2,5
		[E.4] Errores de configuración	-	0,5	-	-	2,5	-	2,5
		[E.8] Disfusión de software dañino	0,1	-	-	0,5	-	-	0,5

Activos	Valor	Amenazas	[D]	[I]	[C]	Impacto D	Impacto I	Impacto C	Impacto Promedio
		[E.9] Errores de [re-]encaminamiento	-	-	0,1	-	-	0,5	0,5
		[E.10] Errores de secuencia	-	0,1	-	-	0,5	-	0,5
		[E.15] Alteración accidental de la información	-	0,5	-	-	2,5	-	2,5
		[E.18] Destrucción de información	0,3	-	-	1,5	-	-	1,5
		[E.19] Fugas de información	-	-	0,2	-	-	1,0	1,0
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	2,5	0,5	0,5	1,2
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	2,5	1,0	-	1,8
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	5,0	-	-	5,0
		[A.3] Manipulación de los registros de actividad (log)	-	0,5	-	-	2,5	-	2,5
		[A.4] Manipulación de la configuración	0,8	0,2	0,2	4,0	1,0	1,0	2,0
		[A.5] Suplantación de la identidad del usuario	0,5	0,2	0,2	2,5	1,0	1,0	1,5
		[A.6] Abuso de privilegios de acceso	0,9	0,5	0,5	4,5	2,5	2,5	3,2
		[A.7] Uso no previsto	0,7	0,1	0,1	3,5	0,5	0,5	1,5
		[A.8] Difusión de software dañino	1,0	0,5	0,5	5,0	2,5	2,5	3,3
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,1	-	-	0,5	0,5
		[A.10] Alteración de secuencia	-	0,1	-	-	0,5	-	0,5
		[A.11] Acceso no autorizado	-	0,5	0,2	-	2,5	1,0	1,8
		[A.13] Repudio	-	0,5	-	-	2,5	-	2,5
		[A.15] Modificación deliberada de la información	-	0,5	-	-	2,5	-	2,5
		[A.18] Destrucción de información	0,9	-	-	4,5	-	-	4,5
		[A.19] Divulgación de información	-	-	0,4	-	-	2,0	2,0
		[A.22] Manipulación de programas	1,0	-	-	5,0	-	-	5,0
		[A.24] Denegación de servicio	0,7	-	0,2	3,5	-	1,0	2,3
Servidor de disponibilidad Nagios	3	[E.1] Errores de los usuarios	0,5	0,2	0,2	1,5	0,6	0,6	0,9
		[E.2] Errores del administrador	0,9	0,2	0,2	2,7	0,6	0,6	1,3
		[E.3] Errores de monitorización (log)	-	1,0	-	-	3,0	-	3,0
		[E.4] Errores de configuración	-	0,5	-	-	1,5	-	1,5
		[E.8] Disfusión de software dañino	0,1	-	-	0,3	-	-	0,3
		[E.9] Errores de [re-]encaminamiento	-	-	0,1	-	-	0,3	0,3
		[E.10] Errores de secuencia	-	0,1	-	-	0,3	-	0,3
		[E.15] Alteración accidental de la información	-	0,5	-	-	1,5	-	1,5
		[E.18] Destrucción de información	0,3	-	-	0,9	-	-	0,9
		[E.19] Fugas de información	-	-	0,2	-	-	0,6	0,6
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	1,5	0,3	0,3	0,7
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	1,5	0,6	-	1,1
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	3,0	-	-	3,0

Activos	Valor	Amenazas	[D]	[I]	[C]	Impacto D	Impacto I	Impacto C	Impacto Promedio
		[A.3] Manipulación de los registros de actividad (log)	-	1,0	-	-	3,0	-	3,0
		[A.4] Manipulación de la configuración	0,8	0,2	0,2	2,4	0,6	0,6	1,2
		[A.5] Suplantación de la identidad del usuario	0,5	0,2	0,2	1,5	0,6	0,6	0,9
		[A.6] Abuso de privilegios de acceso	0,9	0,5	0,5	2,7	1,5	1,5	1,9
		[A.7] Uso no previsto	0,7	0,1	0,1	2,1	0,3	0,3	0,9
		[A.8] Difusión de software dañino	1,0	0,5	0,5	3,0	1,5	1,5	2,0
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,1	-	-	0,3	0,3
		[A.10] Alteración de secuencia	-	0,1	-	-	0,3	-	0,3
		[A.11] Acceso no autorizado	-	0,5	0,2	-	1,5	0,6	1,1
		[A.13] Repudio	-	0,5	-	-	1,5	-	1,5
		[A.15] Modificación deliberada de la información	-	0,5	-	-	1,5	-	1,5
		[A.18] Destrucción de información	0,9	-	-	2,7	-	-	2,7
		[A.19] Divulgación de información	-	-	0,4	-	-	1,2	1,2
		[A.22] Manipulación de programas	1,0	-	-	3,0	-	-	3,0
		[A.24] Denegación de servicio	0,7	-	0,2	2,1	-	0,6	1,4
Servidor WEB	3	[E.1] Errores de los usuarios	0,5	0,2	0,2	1,5	0,6	0,6	0,9
		[E.2] Errores del administrador	0,9	0,2	0,2	2,7	0,6	0,6	1,3
		[E.3] Errores de monitorización (log)	-	1,0	-	-	3,0	-	3,0
		[E.4] Errores de configuración	-	0,5	-	-	1,5	-	1,5
		[E.8] Disfusión de software dañino	0,1	-	-	0,3	-	-	0,3
		[E.9] Errores de [re-]encaminamiento	-	-	0,1	-	-	0,3	0,3
		[E.10] Errores de secuencia	-	0,1	-	-	0,3	-	0,3
		[E.15] Alteración accidental de la información	-	0,5	-	-	1,5	-	1,5
		[E.18] Destrucción de información	0,3	-	-	0,9	-	-	0,9
		[E.19] Fugas de información	-	-	0,2	-	-	0,6	0,6
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	1,5	0,3	0,3	0,7
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	1,5	0,6	-	1,1
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	3,0	-	-	3,0
		[A.3] Manipulación de los registros de actividad (log)	-	1,0	-	-	3,0	-	3,0
		[A.4] Manipulación de la configuración	0,8	0,2	0,2	2,4	0,6	0,6	1,2
		[A.5] Suplantación de la identidad del usuario	0,5	0,2	0,2	1,5	0,6	0,6	0,9
		[A.6] Abuso de privilegios de acceso	0,9	0,5	0,5	2,7	1,5	1,5	1,9
		[A.7] Uso no previsto	0,7	0,1	0,1	2,1	0,3	0,3	0,9
		[A.8] Difusión de software dañino	1,0	0,5	0,5	3,0	1,5	1,5	2,0
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,1	-	-	0,3	0,3
		[A.10] Alteración de secuencia	-	0,1	-	-	0,3	-	0,3

Activos	Valor	Amenazas	[D]	[I]	[C]	Impacto D	Impacto I	Impacto C	Impacto Promedio
		[A.11] Acceso no autorizado	-	0,5	0,2	-	1,5	0,6	1,1
		[A.13] Repudio	-	0,5	-	-	1,5	-	1,5
		[A.15] Modificación deliberada de la información	-	0,5	-	-	1,5	-	1,5
		[A.18] Destrucción de información	0,9	-	-	2,7	-	-	2,7
		[A.19] Divulgación de información	-	-	0,4	-	-	1,2	1,2
		[A.22] Manipulación de programas	1,0	-	-	3,0	-	-	3,0
		[A.24] Denegación de servicio	1,0	-	0,2	3,0	-	0,6	1,8
Servidor de Antivirus	4	[E.1] Errores de los usuarios	0,5	0,2	0,2	2,0	0,8	0,8	1,2
		[E.2] Errores del administrador	0,9	0,2	0,2	3,6	0,8	0,8	1,7
		[E.3] Errores de monitorización (log)	-	0,8	-	-	3,2	-	3,2
		[E.4] Errores de configuración	-	0,5	-	-	2,0	-	2,0
		[E.8] Disfusión de software dañino	0,1	-	-	0,4	-	-	0,4
		[E.9] Errores de [re-]encaminamiento	-	-	0,1	-	-	0,4	0,4
		[E.10] Errores de secuencia	-	0,1	-	-	0,4	-	0,4
		[E.15] Alteración accidental de la información	-	0,5	-	-	2,0	-	2,0
		[E.18] Destrucción de información	0,3	-	-	1,2	-	-	1,2
		[E.19] Fugas de información	-	-	0,2	-	-	0,8	0,8
		[E.20] Vulnerabilidades de los programas (software)	1,0	0,1	0,1	4,0	0,4	0,4	1,6
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	2,0	0,8	-	1,4
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	4,0	-	-	4,0
		[A.3] Manipulación de los registros de actividad (log)	-	1,0	-	-	4,0	-	4,0
		[A.4] Manipulación de la configuración	0,8	0,2	0,2	3,2	0,8	0,8	1,6
		[A.5] Suplantación de la identidad del usuario	0,5	0,5	0,2	2,0	2,0	0,8	1,6
		[A.6] Abuso de privilegios de acceso	0,9	0,5	0,5	3,6	2,0	2,0	2,5
		[A.7] Uso no previsto	0,7	0,1	0,1	2,8	0,4	0,4	1,2
		[A.8] Difusión de software dañino	1,0	0,5	0,5	4,0	2,0	2,0	2,7
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,1	-	-	0,4	0,4
		[A.10] Alteración de secuencia	-	0,1	-	-	0,4	-	0,4
		[A.11] Acceso no autorizado	-	0,5	0,2	-	2,0	0,8	1,4
		[A.13] Repudio	-	0,5	-	-	2,0	-	2,0
		[A.15] Modificación deliberada de la información	-	0,5	-	-	2,0	-	2,0
		[A.18] Destrucción de información	0,9	-	-	3,6	-	-	3,6
		[A.19] Divulgación de información	-	-	0,4	-	-	1,6	1,6
		[A.22] Manipulación de programas	1,0	-	-	4,0	-	-	4,0
		[A.24] Denegación de servicio	0,7	-	0,2	2,8	-	0,8	1,8
Servidor de aplicación	5	[E.1] Errores de los usuarios	0,5	0,2	0,2	2,5	1,0	1,0	1,5
		[E.2] Errores del administrador	0,9	0,2	0,2	4,5	1,0	1,0	2,2
		[E.3] Errores de monitorización (log)	-	0,5	-	-	2,5	-	2,5

Activos	Valor	Amenazas	[D]	[I]	[C]	Impacto D	Impacto I	Impacto C	Impacto Promedio
		[E.4] Errores de configuración	-	0,5	-	-	2,5	-	2,5
		[E.8] Disfusión de software dañino	0,1	-	-	0,5	-	-	0,5
		[E.9] Errores de [re-]encaminamiento	-	-	0,1	-	-	0,5	0,5
		[E.10] Errores de secuencia	-	0,1	-	-	0,5	-	0,5
		[E.15] Alteración accidental de la información	-	0,5	-	-	2,5	-	2,5
		[E.18] Destrucción de información	0,3	-	-	1,5	-	-	1,5
		[E.19] Fugas de información	-	-	0,2	-	-	1,0	1,0
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	2,5	0,5	0,5	1,2
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	2,5	1,0	-	1,8
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	5,0	-	-	5,0
		[A.3] Manipulación de los registros de actividad (log)	-	0,8	-	-	4,0	-	4,0
		[A.4] Manipulación de la configuración	0,8	0,2	0,2	4,0	1,0	1,0	2,0
		[A.5] Suplantación de la identidad del usuario	0,5	0,2	0,2	2,5	1,0	1,0	1,5
		[A.6] Abuso de privilegios de acceso	0,9	0,5	0,5	4,5	2,5	2,5	3,2
		[A.7] Uso no previsto	0,7	0,1	0,1	3,5	0,5	0,5	1,5
		[A.8] Difusión de software dañino	1,0	0,5	0,5	5,0	2,5	2,5	3,3
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,1	-	-	0,5	0,5
		[A.10] Alteración de secuencia	-	0,1	-	-	0,5	-	0,5
		[A.11] Acceso no autorizado	-	0,5	0,2	-	2,5	1,0	1,8
		[A.13] Repudio	-	0,5	-	-	2,5	-	2,5
		[A.15] Modificación deliberada de la información	-	0,5	-	-	2,5	-	2,5
		[A.18] Destrucción de información	0,9	-	-	4,5	-	-	4,5
		[A.19] Divulgación de información	-	-	0,4	-	-	2,0	2,0
		[A.22] Manipulación de programas	1,0	-	-	5,0	-	-	5,0
		[A.24] Denegación de servicio	1,0	-	0,5	5,0	-	2,5	3,8
Servidor de aplicaciones RRHH	4	[E.1] Errores de los usuarios	0,4	0,4	0,4	1,6	1,6	1,6	1,6
		[E.2] Errores del administrador	1,0	0,2	0,2	4,0	0,8	0,8	1,9
		[E.3] Errores de monitorización (log)	-	0,8	-	-	3,2	-	3,2
		[E.4] Errores de configuración	-	0,5	-	-	2,0	-	2,0
		[E.8] Disfusión de software dañino	0,1	-	-	0,4	-	-	0,4
		[E.9] Errores de [re-]encaminamiento	-	-	0,1	-	-	0,4	0,4
		[E.10] Errores de secuencia	-	0,1	-	-	0,4	-	0,4
		[E.15] Alteración accidental de la información	-	0,5	-	-	2,0	-	2,0
		[E.18] Destrucción de información	0,3	-	-	1,2	-	-	1,2
		[E.19] Fugas de información	-	-	0,2	-	-	0,8	0,8
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	2,0	0,4	0,4	0,9

Activos	Valor	Amenazas	[D]	[I]	[C]	Impacto D	Impacto I	Impacto C	Impacto Promedio
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	2,0	0,8	-	1,4
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	4,0	-	-	4,0
		[A.3] Manipulación de los registros de actividad (log)	-	1,0	-	-	4,0	-	4,0
		[A.4] Manipulación de la configuración	0,8	0,2	0,2	3,2	0,8	0,8	1,6
		[A.5] Suplantación de la identidad del usuario	0,5	0,2	0,2	2,0	0,8	0,8	1,2
		[A.6] Abuso de privilegios de acceso	0,9	0,5	0,5	3,6	2,0	2,0	2,5
		[A.7] Uso no previsto	0,7	0,1	0,1	2,8	0,4	0,4	1,2
		[A.8] Difusión de software dañino	1,0	0,5	0,5	4,0	2,0	2,0	2,7
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,1	-	-	0,4	0,4
		[A.10] Alteración de secuencia	-	0,1	-	-	0,4	-	0,4
		[A.11] Acceso no autorizado	-	0,8	0,5	-	3,2	2,0	2,6
		[A.13] Repudio	-	0,5	-	-	2,0	-	2,0
		[A.15] Modificación deliberada de la información	-	0,5	-	-	2,0	-	2,0
		[A.18] Destrucción de información	0,9	-	-	3,6	-	-	3,6
		[A.19] Divulgación de información	-	-	0,8	-	-	3,2	3,2
		[A.22] Manipulación de programas	1,0	-	-	4,0	-	-	4,0
		[A.24] Denegación de servicio	1,0	-	0,5	4,0	-	2,0	3,0
Servidor de aplicación - SPC	3	[E.1] Errores de los usuarios	0,5	0,2	0,2	1,5	0,6	0,6	0,9
		[E.2] Errores del administrador	0,9	0,2	0,2	2,7	0,6	0,6	1,3
		[E.3] Errores de monitorización (log)	-	1,0	-	-	3,0	-	3,0
		[E.4] Errores de configuración	-	0,5	-	-	1,5	-	1,5
		[E.8] Disfusión de software dañino	0,1	-	-	0,3	-	-	0,3
		[E.9] Errores de [re-]encaminamiento	-	-	0,1	-	-	0,3	0,3
		[E.10] Errores de secuencia	-	0,1	-	-	0,3	-	0,3
		[E.15] Alteración accidental de la información	-	0,5	-	-	1,5	-	1,5
		[E.18] Destrucción de información	0,3	-	-	0,9	-	-	0,9
		[E.19] Fugas de información	-	-	0,2	-	-	0,6	0,6
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	1,5	0,3	0,3	0,7
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	1,5	0,6	-	1,1
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	3,0	-	-	3,0
		[A.3] Manipulación de los registros de actividad (log)	-	1,0	-	-	3,0	-	3,0
		[A.4] Manipulación de la configuración	0,8	0,2	0,2	2,4	0,6	0,6	1,2
		[A.5] Suplantación de la identidad del usuario	0,5	0,2	0,2	1,5	0,6	0,6	0,9
		[A.6] Abuso de privilegios de acceso	0,9	0,5	0,5	2,7	1,5	1,5	1,9
		[A.7] Uso no previsto	0,7	0,1	0,1	2,1	0,3	0,3	0,9
		[A.8] Difusión de software dañino	1,0	0,5	0,5	3,0	1,5	1,5	2,0

Activos	Valor	Amenazas	[D]	[I]	[C]	Impacto D	Impacto I	Impacto C	Impacto Promedio
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,1	-	-	0,3	0,3
		[A.10] Alteración de secuencia	-	0,1	-	-	0,3	-	0,3
		[A.11] Acceso no autorizado	-	0,5	0,2	-	1,5	0,6	1,1
		[A.13] Repudio	-	0,5	-	-	1,5	-	1,5
		[A.15] Modificación deliberada de la información	-	0,5	-	-	1,5	-	1,5
		[A.18] Destrucción de información	0,9	-	-	2,7	-	-	2,7
		[A.19] Divulgación de información	-	-	0,4	-	-	1,2	1,2
		[A.22] Manipulación de programas	1,0	-	-	3,0	-	-	3,0
		[A.24] Denegación de servicio	1,0	-	0,1	3,0	-	0,3	1,7
Servidor de aplicación - Indicadores	2	[E.1] Errores de los usuarios	0,5	0,2	0,2	1,0	0,4	0,4	0,6
		[E.2] Errores del administrador	0,9	0,2	0,2	1,8	0,4	0,4	0,9
		[E.3] Errores de monitorización (log)	-	1,0	-	-	2,0	-	2,0
		[E.4] Errores de configuración	-	0,5	-	-	1,0	-	1,0
		[E.8] Disfusión de software dañino	0,1	-	-	0,2	-	-	0,2
		[E.9] Errores de [re-]encaminamiento	-	-	0,1	-	-	0,2	0,2
		[E.10] Errores de secuencia	-	0,1	-	-	0,2	-	0,2
		[E.15] Alteración accidental de la información	-	0,5	-	-	1,0	-	1,0
		[E.18] Destrucción de información	0,3	-	-	0,6	-	-	0,6
		[E.19] Fugas de información	-	-	0,2	-	-	0,4	0,4
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	1,0	0,2	0,2	0,5
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	1,0	0,4	-	0,7
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	2,0	-	-	2,0
		[A.3] Manipulación de los registros de actividad (log)	-	1,0	-	-	2,0	-	2,0
		[A.4] Manipulación de la configuración	0,8	0,2	0,2	1,6	0,4	0,4	0,8
		[A.5] Suplantación de la identidad del usuario	0,5	0,2	0,2	1,0	0,4	0,4	0,6
		[A.6] Abuso de privilegios de acceso	0,9	0,5	0,5	1,8	1,0	1,0	1,3
		[A.7] Uso no previsto	0,7	0,1	0,1	1,4	0,2	0,2	0,6
		[A.8] Difusión de software dañino	1,0	0,5	0,5	2,0	1,0	1,0	1,3
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,1	-	-	0,2	0,2
		[A.10] Alteración de secuencia	-	0,1	-	-	0,2	-	0,2
		[A.11] Acceso no autorizado	-	0,5	0,2	-	1,0	0,4	0,7
		[A.13] Repudio	-	0,5	-	-	1,0	-	1,0
		[A.15] Modificación deliberada de la información	-	0,5	-	-	1,0	-	1,0
		[A.18] Destrucción de información	0,9	-	-	1,8	-	-	1,8
		[A.19] Divulgación de información	-	-	0,4	-	-	0,8	0,8
		[A.22] Manipulación de programas	1,0	-	-	2,0	-	-	2,0
		[A.24] Denegación de servicio	0,7	-	0,2	1,4	-	0,4	0,9

Activos	Valor	Amenazas	[D]	[I]	[C]	Impacto D	Impacto I	Impacto C	Impacto Promedio
Central Telefónica	4	[E.1] Errores de los usuarios	0,5	0,2	0,2	2,0	0,8	0,8	1,2
		[E.2] Errores del administrador	1,0	0,2	0,2	4,0	0,8	0,8	1,9
		[E.3] Errores de monitorización (log)	-	1,0	-	-	4,0	-	4,0
		[E.4] Errores de configuración	-	0,5	-	-	2,0	-	2,0
		[E.8] Disfusión de software dañino	0,1	-	-	0,4	-	-	0,4
		[E.9] Errores de [re-]encaminamiento	-	-	0,5	-	-	2,0	2,0
		[E.10] Errores de secuencia	-	0,5	-	-	2,0	-	2,0
		[E.15] Alteración accidental de la información	-	0,5	-	-	2,0	-	2,0
		[E.18] Destrucción de información	0,3	-	-	1,2	-	-	1,2
		[E.19] Fugas de información	-	-	0,2	-	-	0,8	0,8
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	2,0	0,4	0,4	0,9
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	2,0	0,8	-	1,4
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	4,0	-	-	4,0
		[A.3] Manipulación de los registros de actividad (log)	-	1,0	-	-	4,0	-	4,0
		[A.4] Manipulación de la configuración	0,8	0,2	0,2	3,2	0,8	0,8	1,6
		[A.5] Suplantación de la identidad del usuario	0,9	0,9	0,9	3,6	3,6	3,6	3,6
		[A.6] Abuso de privilegios de acceso	1,0	0,9	0,9	4,0	3,6	3,6	3,7
		[A.7] Uso no previsto	0,7	0,1	0,1	2,8	0,4	0,4	1,2
		[A.8] Difusión de software dañino	1,0	0,5	0,5	4,0	2,0	2,0	2,7
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,5	-	-	2,0	2,0
		[A.10] Alteración de secuencia	-	0,5	-	-	2,0	-	2,0
		[A.11] Acceso no autorizado	-	0,9	0,8	-	3,6	3,2	3,4
		[A.13] Repudio	-	1,0	-	-	4,0	-	4,0
		[A.15] Modificación deliberada de la información	-	0,5	-	-	2,0	-	2,0
		[A.18] Destrucción de información	0,9	-	-	3,6	-	-	3,6
		[A.19] Divulgación de información	-	-	0,4	-	-	1,6	1,6
		[A.22] Manipulación de programas	1,0	-	-	4,0	-	-	4,0
		[A.24] Denegación de servicio	1,0	-	0,2	4,0	-	0,8	2,4
Firewall perimetral	5	[E.1] Errores de los usuarios	0,5	0,2	0,2	2,5	1,0	1,0	1,5
		[E.2] Errores del administrador	0,9	0,2	0,2	4,5	1,0	1,0	2,2
		[E.3] Errores de monitorización (log)	-	1,0	-	-	5,0	-	5,0
		[E.4] Errores de configuración	-	0,5	-	-	2,5	-	2,5
		[E.8] Disfusión de software dañino	0,1	-	-	0,5	-	-	0,5
		[E.9] Errores de [re-]encaminamiento	-	-	0,5	-	-	2,5	2,5
		[E.10] Errores de secuencia	-	0,5	-	-	2,5	-	2,5
		[E.15] Alteración accidental de la información	-	0,5	-	-	2,5	-	2,5
		[E.18] Destrucción de información	0,3	-	-	1,5	-	-	1,5
		[E.19] Fugas de información	-	-	0,2	-	-	1,0	1,0

Activos	Valor	Amenazas	[D]	[I]	[C]	Impacto D	Impacto I	Impacto C	Impacto Promedio
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	2,5	0,5	0,5	1,2
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	2,5	1,0	-	1,8
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	5,0	-	-	5,0
		[A.3] Manipulación de los registros de actividad (log)	-	1,0	-	-	5,0	-	5,0
		[A.4] Manipulación de la configuración	0,8	0,8	0,8	4,0	4,0	4,0	4,0
		[A.5] Suplantación de la identidad del usuario	0,9	0,5	0,2	4,5	2,5	1,0	2,7
		[A.6] Abuso de privilegios de acceso	0,9	0,5	0,5	4,5	2,5	2,5	3,2
		[A.7] Uso no previsto	0,7	0,1	0,1	3,5	0,5	0,5	1,5
		[A.8] Difusión de software dañino	1,0	0,5	0,5	5,0	2,5	2,5	3,3
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,5	-	-	2,5	2,5
		[A.10] Alteración de secuencia	-	0,5	-	-	2,5	-	2,5
		[A.11] Acceso no autorizado	-	1,0	0,5	-	5,0	2,5	3,8
		[A.13] Repudio	-	1,0	-	-	5,0	-	5,0
		[A.15] Modificación deliberada de la información	-	0,5	-	-	2,5	-	2,5
		[A.18] Destrucción de información	0,9	-	-	4,5	-	-	4,5
		[A.19] Divulgación de información	-	-	0,4	-	-	2,0	2,0
		[A.22] Manipulación de programas	1,0	-	-	5,0	-	-	5,0
		[A.24] Denegación de servicio	0,7	-	0,2	3,5	-	1,0	2,3
Switch de distribución/acceso	4	[E.1] Errores de los usuarios	0,5	0,5	0,5	2,0	2,0	2,0	2,0
		[E.2] Errores del administrador	1,0	0,5	0,2	4,0	2,0	0,8	2,3
		[E.3] Errores de monitorización (log)	-	1,0	-	-	4,0	-	4,0
		[E.4] Errores de configuración	-	0,5	-	-	2,0	-	2,0
		[E.8] Disfusión de software dañino	0,1	-	-	0,4	-	-	0,4
		[E.9] Errores de [re-]encaminamiento	-	-	0,5	-	-	2,0	2,0
		[E.10] Errores de secuencia	-	0,5	-	-	2,0	-	2,0
		[E.15] Alteración accidental de la información	-	0,5	-	-	2,0	-	2,0
		[E.18] Destrucción de información	0,3	-	-	1,2	-	-	1,2
		[E.19] Fugas de información	-	-	0,2	-	-	0,8	0,8
		[E.20] Vulnerabilidades de los programas (software)	0,5	0,1	0,1	2,0	0,4	0,4	0,9
		[E.21] Errores de mantenimiento / actualización de programas (software)	0,5	0,2	-	2,0	0,8	-	1,4
		[E.24] Caída del sistema por agotamiento de recursos	1,0	-	-	4,0	-	-	4,0
		[A.3] Manipulación de los registros de actividad (log)	-	1,0	-	-	4,0	-	4,0
		[A.4] Manipulación de la configuración	0,8	0,8	0,8	3,2	3,2	3,2	3,2
		[A.5] Suplantación de la identidad del usuario	0,5	0,2	0,2	2,0	0,8	0,8	1,2
		[A.6] Abuso de privilegios de acceso	0,9	0,9	0,5	3,6	3,6	2,0	3,1

Activos	Valor	Amenazas	[D]	[I]	[C]	Impacto D	Impacto I	Impacto C	Impacto Promedio
		[A.7] Uso no previsto	0,7	0,1	0,1	2,8	0,4	0,4	1,2
		[A.8] Difusión de software dañino	1,0	0,5	0,5	4,0	2,0	2,0	2,7
		[A.9] [Re-]encaminamiento de mensajes	-	-	0,5	-	-	2,0	2,0
		[A.10] Alteración de secuencia	-	0,5	-	-	2,0	-	2,0
		[A.11] Acceso no autorizado	-	0,5	0,2	-	2,0	0,8	1,4
		[A.13] Repudio	-	1,0	-	-	4,0	-	4,0
		[A.15] Modificación deliberada de la información	-	0,5	-	-	2,0	-	2,0
		[A.18] Destrucción de información	0,9	-	-	3,6	-	-	3,6
		[A.19] Divulgación de información	-	-	0,4	-	-	1,6	1,6
		[A.22] Manipulación de programas	1,0	-	-	4,0	-	-	4,0
		[A.24] Denegación de servicio	0,7	-	0,2	2,8	-	0,8	1,8

2.1.4 ESTIMACIÓN DEL RIESGO

El riesgo se cataloga como la medida del daño que un activo recibiría. Una vez que se conoce el impacto de una amenaza, se puede calcular el riesgo que ésta amenaza tendría sobre el activo considerando la probabilidad de que la amenaza llegue a materializarse, realizando la multiplicación de estos valores.

En la Tabla 2.8 se puede observar la estimación del riesgo calculada a partir del impacto promedio, obtenido en la sección 2.1.3, y la probabilidad de ocurrencia de cada amenaza definido en la sección 2.1.2.2.

A continuación, se realiza un ejemplo de cálculo del riesgo para el Servidor de virtualización Main.

Ejemplo de cálculo de riesgo para el activo "Servidor de virtualización Main"

- Amenaza a evaluar = [E.1] Errores de los usuarios
- Probabilidad que la amenaza se materialice = 3
- Impacto promedio que ocasionaría la amenaza = 1,5
- Riesgo = 3 x 1,5 = 5

Tabla 2.8 Estimación del Riesgo

Activos	Amenazas	Probabilidad	Impacto Promedio	Riesgo
Servidor de virtualización Main	[E.1] Errores de los usuarios	3	1,5	5
	[E.2] Errores del administrador	3	3,3	10
	[E.3] Errores de monitorización (log)	5	4,0	20
	[E.4] Errores de configuración	2	2,5	5
	[E.8] Disfusión de software dañino	1	0,5	1
	[E.9] Errores de [re-]encaminamiento	1	0,5	1
	[E.10] Errores de secuencia	1	0,5	1
	[E.15] Alteración accidental de la información	3	2,5	8
	[E.18] Destrucción de información	2	1,5	3
	[E.19] Fugas de información	1	1,0	1
	[E.20] Vulnerabilidades de los programas (software)	1	1,2	1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1,8	2
	[E.24] Caída del sistema por agotamiento de recursos	2	5,0	10
	[A.3] Manipulación de los registros de actividad (log)	2	5,0	10
	[A.4] Manipulación de la configuración	3	4,0	12
	[A.5] Suplantación de la identidad del usuario	2	1,5	3
	[A.6] Abuso de privilegios de acceso	2	3,2	6
	[A.7] Uso no previsto	2	1,5	3
	[A.8] Difusión de software dañino	2	3,3	7
	[A.9] [Re-]encaminamiento de mensajes	1	0,5	1
	[A.10] Alteración de secuencia	1	0,5	1
	[A.11] Acceso no autorizado	3	4,0	12
	[A.13] Repudio	5	5,0	25
	[A.15] Modificación deliberada de la información	2	2,5	5
	[A.18] Destrucción de información	2	4,5	9
	[A.19] Divulgación de información	2	2,0	4
	[A.22] Manipulación de programas	1	5,0	5
	[A.24] Denegación de servicio	1	2,3	2
Servidor de Active Directory	[E.1] Errores de los usuarios	3	1,5	5
	[E.2] Errores del administrador	3	2,3	7
	[E.3] Errores de monitorización (log)	5	5,0	25
	[E.4] Errores de configuración	4	4,0	16
	[E.8] Disfusión de software dañino	1	5,0	5
	[E.9] Errores de [re-]encaminamiento	1	0,5	1
	[E.10] Errores de secuencia	1	0,5	1
	[E.15] Alteración accidental de la información	4	2,5	10
	[E.18] Destrucción de información	2	1,5	3
	[E.19] Fugas de información	1	1,0	1
	[E.20] Vulnerabilidades de los programas (software)	1	1,2	1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1,8	2

Activos	Amenazas	Probabilidad	Impacto Promedio	Riesgo
	[E.24] Caída del sistema por agotamiento de recursos	2	5,0	10
	[A.3] Manipulación de los registros de actividad (log)	4	5,0	20
	[A.4] Manipulación de la configuración	3	2,5	8
	[A.5] Suplantación de la identidad del usuario	2	1,5	3
	[A.6] Abuso de privilegios de acceso	3	3,2	10
	[A.7] Uso no previsto	3	1,5	5
	[A.8] Difusión de software dañino	3	3,3	10
	[A.9] [Re-]encaminamiento de mensajes	1	0,5	1
	[A.10] Alteración de secuencia	1	0,5	1
	[A.11] Acceso no autorizado	3	2,5	8
	[A.13] Repudio	5	5,0	25
	[A.15] Modificación deliberada de la información	2	2,5	5
	[A.18] Destrucción de información	2	4,5	9
	[A.19] Divulgación de información	2	2,0	4
	[A.22] Manipulación de programas	2	5,0	10
	[A.24] Denegación de servicio	1	2,3	2
Servidor de Archivos MicroDM	[E.1] Errores de los usuarios	3	1,2	4
	[E.2] Errores del administrador	3	1,9	6
	[E.3] Errores de monitorización (log)	5	4,0	20
	[E.4] Errores de configuración	4	3,2	13
	[E.8] Disfusión de software dañino	1	0,4	0
	[E.9] Errores de [re-]encaminamiento	1	0,4	0
	[E.10] Errores de secuencia	1	0,4	0
	[E.15] Alteración accidental de la información	4	2,0	8
	[E.18] Destrucción de información	2	1,2	2
	[E.19] Fugas de información	3	0,8	2
	[E.20] Vulnerabilidades de los programas (software)	3	0,9	3
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	2,4	5
	[E.24] Caída del sistema por agotamiento de recursos	2	4,0	8
	[A.3] Manipulación de los registros de actividad (log)	4	4,0	16
	[A.4] Manipulación de la configuración	4	1,6	6
	[A.5] Suplantación de la identidad del usuario	2	1,9	4
	[A.6] Abuso de privilegios de acceso	4	2,7	11
	[A.7] Uso no previsto	2	1,2	2
	[A.8] Difusión de software dañino	2	2,7	5
	[A.9] [Re-]encaminamiento de mensajes	1	0,4	0
	[A.10] Alteración de secuencia	1	0,4	0
	[A.11] Acceso no autorizado	3	4,0	12
	[A.13] Repudio	5	4,0	20
	[A.15] Modificación deliberada de la información	3	4,0	12
	[A.18] Destrucción de información	3	4,0	12
	[A.19] Divulgación de información	3	1,6	5
	[A.22] Manipulación de programas	2	4,0	8

Activos	Amenazas	Probabilidad	Impacto Promedio	Riesgo
	[A.24] Denegación de servicio	1	1,8	2
Servidor de almacenamiento NAS	[E.1] Errores de los usuarios	2	1,5	3
	[E.2] Errores del administrador	2	2,2	4
	[E.3] Errores de monitorización (log)	4	2,5	10
	[E.4] Errores de configuración	2	2,5	5
	[E.8] Disfusión de software dañino	1	0,5	1
	[E.9] Errores de [re-]encaminamiento	1	0,5	1
	[E.10] Errores de secuencia	1	0,5	1
	[E.15] Alteración accidental de la información	2	2,5	5
	[E.18] Destrucción de información	3	1,5	5
	[E.19] Fugas de información	1	1,0	1
	[E.20] Vulnerabilidades de los programas (software)	1	1,2	1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1,8	2
	[E.24] Caída del sistema por agotamiento de recursos	2	5,0	10
	[A.3] Manipulación de los registros de actividad (log)	4	2,5	10
	[A.4] Manipulación de la configuración	3	2,0	6
	[A.5] Suplantación de la identidad del usuario	2	1,5	3
	[A.6] Abuso de privilegios de acceso	4	3,2	13
	[A.7] Uso no previsto	2	1,5	3
	[A.8] Difusión de software dañino	2	3,3	7
	[A.9] [Re-]encaminamiento de mensajes	1	0,5	1
	[A.10] Alteración de secuencia	1	0,5	1
	[A.11] Acceso no autorizado	3	1,8	5
	[A.13] Repudio	4	2,5	10
	[A.15] Modificación deliberada de la información	2	2,5	5
	[A.18] Destrucción de información	2	4,5	9
	[A.19] Divulgación de información	2	2,0	4
	[A.22] Manipulación de programas	1	5,0	5
	[A.24] Denegación de servicio	1	2,3	2
Servidor de disponibilidad Nagios	[E.1] Errores de los usuarios	2	0,9	2
	[E.2] Errores del administrador	2	1,3	3
	[E.3] Errores de monitorización (log)	4	3,0	12
	[E.4] Errores de configuración	3	1,5	5
	[E.8] Disfusión de software dañino	1	0,3	0
	[E.9] Errores de [re-]encaminamiento	1	0,3	0
	[E.10] Errores de secuencia	1	0,3	0
	[E.15] Alteración accidental de la información	2	1,5	3
	[E.18] Destrucción de información	2	0,9	2
	[E.19] Fugas de información	1	0,6	1
	[E.20] Vulnerabilidades de los programas (software)	2	0,7	1
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	1,1	2
	[E.24] Caída del sistema por agotamiento de recursos	3	3,0	9

Activos	Amenazas	Probabilidad	Impacto Promedio	Riesgo
	[A.3] Manipulación de los registros de actividad (log)	4	3,0	12
	[A.4] Manipulación de la configuración	2	1,2	2
	[A.5] Suplantación de la identidad del usuario	2	0,9	2
	[A.6] Abuso de privilegios de acceso	2	1,9	4
	[A.7] Uso no previsto	1	0,9	1
	[A.8] Difusión de software dañino	1	2,0	2
	[A.9] [Re-]encaminamiento de mensajes	1	0,3	0
	[A.10] Alteración de secuencia	1	0,3	0
	[A.11] Acceso no autorizado	2	1,1	2
	[A.13] Repudio	4	1,5	6
	[A.15] Modificación deliberada de la información	2	1,5	3
	[A.18] Destrucción de información	2	2,7	5
	[A.19] Divulgación de información	2	1,2	2
	[A.22] Manipulación de programas	1	3,0	3
	[A.24] Denegación de servicio	1	1,4	1
Servidor WEB	[E.1] Errores de los usuarios	3	0,9	3
	[E.2] Errores del administrador	3	1,3	4
	[E.3] Errores de monitorización (log)	5	3,0	15
	[E.4] Errores de configuración	3	1,5	5
	[E.8] Disfusión de software dañino	1	0,3	0
	[E.9] Errores de [re-]encaminamiento	1	0,3	0
	[E.10] Errores de secuencia	1	0,3	0
	[E.15] Alteración accidental de la información	2	1,5	3
	[E.18] Destrucción de información	1	0,9	1
	[E.19] Fugas de información	1	0,6	1
	[E.20] Vulnerabilidades de los programas (software)	1	0,7	1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1,1	1
	[E.24] Caída del sistema por agotamiento de recursos	2	3,0	6
	[A.3] Manipulación de los registros de actividad (log)	4	3,0	12
	[A.4] Manipulación de la configuración	3	1,2	4
	[A.5] Suplantación de la identidad del usuario	3	0,9	3
	[A.6] Abuso de privilegios de acceso	4	1,9	8
	[A.7] Uso no previsto	2	0,9	2
	[A.8] Difusión de software dañino	2	2,0	4
	[A.9] [Re-]encaminamiento de mensajes	1	0,3	0
	[A.10] Alteración de secuencia	1	0,3	0
	[A.11] Acceso no autorizado	3	1,1	3
	[A.13] Repudio	4	1,5	6
	[A.15] Modificación deliberada de la información	3	1,5	5
	[A.18] Destrucción de información	3	2,7	8
	[A.19] Divulgación de información	2	1,2	2
	[A.22] Manipulación de programas	1	3,0	3
	[A.24] Denegación de servicio	4	1,8	7

Activos	Amenazas	Probabilidad	Impacto Promedio	Riesgo
Servidor de Antivirus	[E.1] Errores de los usuarios	2	1,2	2
	[E.2] Errores del administrador	2	1,7	3
	[E.3] Errores de monitorización (log)	5	3,2	16
	[E.4] Errores de configuración	2	2,0	4
	[E.8] Disfusión de software dañino	3	0,4	1
	[E.9] Errores de [re-]encaminamiento	1	0,4	0
	[E.10] Errores de secuencia	1	0,4	0
	[E.15] Alteración accidental de la información	3	2,0	6
	[E.18] Destrucción de información	2	1,2	2
	[E.19] Fugas de información	1	0,8	1
	[E.20] Vulnerabilidades de los programas (software)	2	1,6	3
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1,4	1
	[E.24] Caída del sistema por agotamiento de recursos	2	4,0	8
	[A.3] Manipulación de los registros de actividad (log)	4	4,0	16
	[A.4] Manipulación de la configuración	2	1,6	3
	[A.5] Suplantación de la identidad del usuario	2	1,6	3
	[A.6] Abuso de privilegios de acceso	4	2,5	10
	[A.7] Uso no previsto	3	1,2	4
	[A.8] Difusión de software dañino	2	2,7	5
	[A.9] [Re-]encaminamiento de mensajes	1	0,4	0
	[A.10] Alteración de secuencia	1	0,4	0
	[A.11] Acceso no autorizado	2	1,4	3
	[A.13] Repudio	4	2,0	8
	[A.15] Modificación deliberada de la información	2	2,0	4
	[A.18] Destrucción de información	2	3,6	7
	[A.19] Divulgación de información	2	1,6	3
	[A.22] Manipulación de programas	1	4,0	4
	[A.24] Denegación de servicio	1	1,8	2
Servidor de aplicación CRM	[E.1] Errores de los usuarios	2	1,5	3
	[E.2] Errores del administrador	2	2,2	4
	[E.3] Errores de monitorización (log)	5	2,5	13
	[E.4] Errores de configuración	2	2,5	5
	[E.8] Disfusión de software dañino	1	0,5	1
	[E.9] Errores de [re-]encaminamiento	1	0,5	1
	[E.10] Errores de secuencia	1	0,5	1
	[E.15] Alteración accidental de la información	3	2,5	8
	[E.18] Destrucción de información	2	1,5	3
	[E.19] Fugas de información	2	1,0	2
	[E.20] Vulnerabilidades de los programas (software)	1	1,2	1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1,8	2
	[E.24] Caída del sistema por agotamiento de recursos	1	5,0	5
	[A.3] Manipulación de los registros de actividad (log)	4	4,0	16

Activos	Amenazas	Probabilidad	Impacto Promedio	Riesgo
	[A.4] Manipulación de la configuración	3	2,0	6
	[A.5] Suplantación de la identidad del usuario	2	1,5	3
	[A.6] Abuso de privilegios de acceso	2	3,2	6
	[A.7] Uso no previsto	2	1,5	3
	[A.8] Difusión de software dañino	2	3,3	7
	[A.9] [Re-]encaminamiento de mensajes	1	0,5	1
	[A.10] Alteración de secuencia	1	0,5	1
	[A.11] Acceso no autorizado	2	1,8	4
	[A.13] Repudio	4	2,5	10
	[A.15] Modificación deliberada de la información	2	2,5	5
	[A.18] Destrucción de información	2	4,5	9
	[A.19] Divulgación de información	2	2,0	4
	[A.22] Manipulación de programas	1	5,0	5
	[A.24] Denegación de servicio	1	3,8	4
Servidor de aplicaciones RRHH	[E.1] Errores de los usuarios	2	1,6	3
	[E.2] Errores del administrador	2	1,9	4
	[E.3] Errores de monitorización (log)	5	3,2	16
	[E.4] Errores de configuración	2	2,0	4
	[E.8] Disfusión de software dañino	1	0,4	0
	[E.9] Errores de [re-]encaminamiento	1	0,4	0
	[E.10] Errores de secuencia	1	0,4	0
	[E.15] Alteración accidental de la información	2	2,0	4
	[E.18] Destrucción de información	2	1,2	2
	[E.19] Fugas de información	2	0,8	2
	[E.20] Vulnerabilidades de los programas (software)	1	0,9	1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1,4	1
	[E.24] Caída del sistema por agotamiento de recursos	1	4,0	4
	[A.3] Manipulación de los registros de actividad (log)	4	4,0	16
	[A.4] Manipulación de la configuración	3	1,6	5
	[A.5] Suplantación de la identidad del usuario	2	1,2	2
	[A.6] Abuso de privilegios de acceso	3	2,5	8
	[A.7] Uso no previsto	2	1,2	2
	[A.8] Difusión de software dañino	2	2,7	5
	[A.9] [Re-]encaminamiento de mensajes	1	0,4	0
	[A.10] Alteración de secuencia	1	0,4	0
	[A.11] Acceso no autorizado	3	2,6	8
	[A.13] Repudio	4	2,0	8
	[A.15] Modificación deliberada de la información	2	2,0	4
	[A.18] Destrucción de información	2	3,6	7
	[A.19] Divulgación de información	2	3,2	6
	[A.22] Manipulación de programas	1	4,0	4
	[A.24] Denegación de servicio	1	3,0	3
	[E.1] Errores de los usuarios	2	0,9	2

Activos	Amenazas	Probabilidad	Impacto Promedio	Riesgo
Servidor de aplicación - SPC	[E.2] Errores del administrador	2	1,3	3
	[E.3] Errores de monitorización (log)	5	3,0	15
	[E.4] Errores de configuración	2	1,5	3
	[E.8] Disfusión de software dañino	1	0,3	0
	[E.9] Errores de [re-]encaminamiento	1	0,3	0
	[E.10] Errores de secuencia	1	0,3	0
	[E.15] Alteración accidental de la información	2	1,5	3
	[E.18] Destrucción de información	2	0,9	2
	[E.19] Fugas de información	1	0,6	1
	[E.20] Vulnerabilidades de los programas (software)	2	0,7	1
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	1,1	2
	[E.24] Caída del sistema por agotamiento de recursos	2	3,0	6
	[A.3] Manipulación de los registros de actividad (log)	4	3,0	12
	[A.4] Manipulación de la configuración	2	1,2	2
	[A.5] Suplantación de la identidad del usuario	2	0,9	2
	[A.6] Abuso de privilegios de acceso	4	1,9	8
	[A.7] Uso no previsto	2	0,9	2
	[A.8] Difusión de software dañino	2	2,0	4
	[A.9] [Re-]encaminamiento de mensajes	1	0,3	0
	[A.10] Alteración de secuencia	1	0,3	0
	[A.11] Acceso no autorizado	2	1,1	2
	[A.13] Repudio	4	1,5	6
	[A.15] Modificación deliberada de la información	2	1,5	3
	[A.18] Destrucción de información	2	2,7	5
	[A.19] Divulgación de información	2	1,2	2
	[A.22] Manipulación de programas	1	3,0	3
	[A.24] Denegación de servicio	1	1,7	2
Servidor de aplicación - Indicadores	[E.1] Errores de los usuarios	2	0,6	1
	[E.2] Errores del administrador	2	0,9	2
	[E.3] Errores de monitorización (log)	5	2,0	10
	[E.4] Errores de configuración	2	1,0	2
	[E.8] Disfusión de software dañino	1	0,2	0
	[E.9] Errores de [re-]encaminamiento	1	0,2	0
	[E.10] Errores de secuencia	1	0,2	0
	[E.15] Alteración accidental de la información	2	1,0	2
	[E.18] Destrucción de información	2	0,6	1
	[E.19] Fugas de información	1	0,4	0
	[E.20] Vulnerabilidades de los programas (software)	3	0,5	1
	[E.21] Errores de mantenimiento / actualización de programas (software)	3	0,7	2
	[E.24] Caída del sistema por agotamiento de recursos	2	2,0	4
	[A.3] Manipulación de los registros de actividad (log)	4	2,0	8
	[A.4] Manipulación de la configuración	2	0,8	2

Activos	Amenazas	Probabilidad	Impacto Promedio	Riesgo
	[A.5] Suplantación de la identidad del usuario	2	0,6	1
	[A.6] Abuso de privilegios de acceso	4	1,3	5
	[A.7] Uso no previsto	4	0,6	2
	[A.8] Difusión de software dañino	2	1,3	3
	[A.9] [Re-]encaminamiento de mensajes	1	0,2	0
	[A.10] Alteración de secuencia	1	0,2	0
	[A.11] Acceso no autorizado	2	0,7	1
	[A.13] Repudio	4	1,0	4
	[A.15] Modificación deliberada de la información	2	1,0	2
	[A.18] Destrucción de información	2	1,8	4
	[A.19] Divulgación de información	2	0,8	2
	[A.22] Manipulación de programas	1	2,0	2
	[A.24] Denegación de servicio	1	0,9	1
Central Telefónica	[E.1] Errores de los usuarios	2	1,2	2
	[E.2] Errores del administrador	3	1,9	6
	[E.3] Errores de monitorización (log)	5	4,0	20
	[E.4] Errores de configuración	3	2,0	6
	[E.8] Disfusión de software dañino	2	0,4	1
	[E.9] Errores de [re-]encaminamiento	2	2,0	4
	[E.10] Errores de secuencia	3	2,0	6
	[E.15] Alteración accidental de la información	3	2,0	6
	[E.18] Destrucción de información	2	1,2	2
	[E.19] Fugas de información	1	0,8	1
	[E.20] Vulnerabilidades de los programas (software)	1	0,9	1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1,4	1
	[E.24] Caída del sistema por agotamiento de recursos	2	4,0	8
	[A.3] Manipulación de los registros de actividad (log)	4	4,0	16
	[A.4] Manipulación de la configuración	4	1,6	6
	[A.5] Suplantación de la identidad del usuario	3	3,6	11
	[A.6] Abuso de privilegios de acceso	4	3,7	15
	[A.7] Uso no previsto	3	1,2	4
	[A.8] Difusión de software dañino	2	2,7	5
	[A.9] [Re-]encaminamiento de mensajes	2	2,0	4
	[A.10] Alteración de secuencia	2	2,0	4
	[A.11] Acceso no autorizado	4	3,4	14
	[A.13] Repudio	4	4,0	16
	[A.15] Modificación deliberada de la información	3	2,0	6
	[A.18] Destrucción de información	3	3,6	11
	[A.19] Divulgación de información	2	1,6	3
	[A.22] Manipulación de programas	1	4,0	4
	[A.24] Denegación de servicio	1	2,4	2
Firewall perimetral	[E.1] Errores de los usuarios	2	1,5	3
	[E.2] Errores del administrador	3	2,2	7

Activos	Amenazas	Probabilidad	Impacto Promedio	Riesgo
	[E.3] Errores de monitorización (log)	5	5,0	25
	[E.4] Errores de configuración	3	2,5	8
	[E.8] Disfusión de software dañino	1	0,5	1
	[E.9] Errores de [re-]encaminamiento	2	2,5	5
	[E.10] Errores de secuencia	2	2,5	5
	[E.15] Alteración accidental de la información	3	2,5	8
	[E.18] Destrucción de información	2	1,5	3
	[E.19] Fugas de información	1	1,0	1
	[E.20] Vulnerabilidades de los programas (software)	1	1,2	1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1,8	2
	[E.24] Caída del sistema por agotamiento de recursos	2	5,0	10
	[A.3] Manipulación de los registros de actividad (log)	4	5,0	20
	[A.4] Manipulación de la configuración	4	4,0	16
	[A.5] Suplantación de la identidad del usuario	3	2,7	8
	[A.6] Abuso de privilegios de acceso	4	3,2	13
	[A.7] Uso no previsto	2	1,5	3
	[A.8] Difusión de software dañino	2	3,3	7
	[A.9] [Re-]encaminamiento de mensajes	3	2,5	8
	[A.10] Alteración de secuencia	3	2,5	8
	[A.11] Acceso no autorizado	3	3,8	11
	[A.13] Repudio	5	5,0	25
	[A.15] Modificación deliberada de la información	4	2,5	10
	[A.18] Destrucción de información	2	4,5	9
	[A.19] Divulgación de información	3	2,0	6
	[A.22] Manipulación de programas	1	5,0	5
	[A.24] Denegación de servicio	1	2,3	2
Switch de distribución/acceso	[E.1] Errores de los usuarios	2	2,0	4
	[E.2] Errores del administrador	3	2,3	7
	[E.3] Errores de monitorización (log)	4	4,0	16
	[E.4] Errores de configuración	3	2,0	6
	[E.8] Disfusión de software dañino	1	0,4	0
	[E.9] Errores de [re-]encaminamiento	2	2,0	4
	[E.10] Errores de secuencia	2	2,0	4
	[E.15] Alteración accidental de la información	3	2,0	6
	[E.18] Destrucción de información	2	1,2	2
	[E.19] Fugas de información	1	0,8	1
	[E.20] Vulnerabilidades de los programas (software)	1	0,9	1
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1,4	1
	[E.24] Caída del sistema por agotamiento de recursos	2	4,0	8
	[A.3] Manipulación de los registros de actividad (log)	4	4,0	16
	[A.4] Manipulación de la configuración	4	3,2	13
	[A.5] Suplantación de la identidad del usuario	3	1,2	4

Activos	Amenazas	Probabilidad	Impacto Promedio	Riesgo
	[A.6] Abuso de privilegios de acceso	4	3,1	12
	[A.7] Uso no previsto	2	1,2	2
	[A.8] Difusión de software dañino	2	2,7	5
	[A.9] [Re-]encaminamiento de mensajes	3	2,0	6
	[A.10] Alteración de secuencia	3	2,0	6
	[A.11] Acceso no autorizado	4	1,4	6
	[A.13] Repudio	4	4,0	16
	[A.15] Modificación deliberada de la información	3	2,0	6
	[A.18] Destrucción de información	3	3,6	11
	[A.19] Divulgación de información	2	1,6	3
	[A.22] Manipulación de programas	1	4,0	4
	[A.24] Denegación de servicio	1	1,8	2

2.2 SELECCIÓN DE ACTIVOS DE MONITOREO

El riesgo más alto que una amenaza puede obtener es de 25, ya que los valores máximos que la probabilidad y el impacto promedio pueden tener es 5 y la multiplicación de éstos daría como resultado 25.

Tomando como referencia la Tabla 2.9, y con base en el análisis de riesgos realizado, se hizo una comparación con la cantidad de valores de riesgo mayores o iguales a 20 (Alto), como se muestra en la Tabla 2.10, con el objetivo de seleccionar los activos críticos a ser integrados en el monitoreo de OSSIM.

Tabla 2.9 Valorización del riesgo

Valor	Descripción
5	Muy bajo
10	Bajo
15	Medio
20	Alto
25	Muy alto

Tabla 2.10 Riesgos mayores a 20

Activos	Valor	Amenazas	Riesgo	Cantidad de valores superiores o iguales a 20
Servidor de virtualización Main	5	[E.1] Errores de los usuarios	5	2
		[E.2] Errores del administrador	10	
		[E.3] Errores de monitorización (log)	20	
		[E.4] Errores de configuración	5	
		[E.8] Disfusión de software dañino	1	

Activos	Valor	Amenazas	Riesgo	Cantidad de valores superiores o iguales a 20
		[E.9] Errores de [re-]encaminamiento	1	
		[E.10] Errores de secuencia	1	
		[E.15] Alteración accidental de la información	8	
		[E.18] Destrucción de información	3	
		[E.19] Fugas de información	1	
		[E.20] Vulnerabilidades de los programas (software)	1	
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	
		[E.24] Caída del sistema por agotamiento de recursos	10	
		[A.3] Manipulación de los registros de actividad (log)	10	
		[A.4] Manipulación de la configuración	12	
		[A.5] Suplantación de la identidad del usuario	3	
		[A.6] Abuso de privilegios de acceso	6	
		[A.7] Uso no previsto	3	
		[A.8] Difusión de software dañino	7	
		[A.9] [Re-]encaminamiento de mensajes	1	
		[A.10] Alteración de secuencia	1	
		[A.11] Acceso no autorizado	12	
		[A.13] Repudio	25	
		[A.15] Modificación deliberada de la información	5	
		[A.18] Destrucción de información	9	
		[A.19] Divulgación de información	4	
		[A.22] Manipulación de programas	5	
		[A.24] Denegación de servicio	2	
Servidor de Active Directory	5	[E.1] Errores de los usuarios	5	3
		[E.2] Errores del administrador	7	
		[E.3] Errores de monitorización (log)	25	
		[E.4] Errores de configuración	16	
		[E.8] Disfusión de software dañino	5	
		[E.9] Errores de [re-]encaminamiento	1	
		[E.10] Errores de secuencia	1	
		[E.15] Alteración accidental de la información	10	
		[E.18] Destrucción de información	3	
		[E.19] Fugas de información	1	
		[E.20] Vulnerabilidades de los programas (software)	1	
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	
		[E.24] Caída del sistema por agotamiento de recursos	10	

Activos	Valor	Amenazas	Riesgo	Cantidad de valores superiores o iguales a 20
		[A.3] Manipulación de los registros de actividad (log)	20	
		[A.4] Manipulación de la configuración	8	
		[A.5] Suplantación de la identidad del usuario	3	
		[A.6] Abuso de privilegios de acceso	10	
		[A.7] Uso no previsto	5	
		[A.8] Difusión de software dañino	10	
		[A.9] [Re-]encaminamiento de mensajes	1	
		[A.10] Alteración de secuencia	1	
		[A.11] Acceso no autorizado	8	
		[A.13] Repudio	25	
		[A.15] Modificación deliberada de la información	5	
		[A.18] Destrucción de información	9	
		[A.19] Divulgación de información	4	
		[A.22] Manipulación de programas	10	
		[A.24] Denegación de servicio	2	
Servidor de Archivos MicroDM	4	[E.1] Errores de los usuarios	4	2
		[E.2] Errores del administrador	6	
		[E.3] Errores de monitorización (log)	20	
		[E.4] Errores de configuración	13	
		[E.8] Disfusión de software dañino	0	
		[E.9] Errores de [re-]encaminamiento	0	
		[E.10] Errores de secuencia	0	
		[E.15] Alteración accidental de la información	8	
		[E.18] Destrucción de información	2	
		[E.19] Fugas de información	2	
		[E.20] Vulnerabilidades de los programas (software)	3	
		[E.21] Errores de mantenimiento / actualización de programas (software)	5	
		[E.24] Caída del sistema por agotamiento de recursos	8	
		[A.3] Manipulación de los registros de actividad (log)	16	
		[A.4] Manipulación de la configuración	6	
		[A.5] Suplantación de la identidad del usuario	4	
		[A.6] Abuso de privilegios de acceso	11	
		[A.7] Uso no previsto	2	
		[A.8] Difusión de software dañino	5	
		[A.9] [Re-]encaminamiento de mensajes	0	
		[A.10] Alteración de secuencia	0	
		[A.11] Acceso no autorizado	12	
		[A.13] Repudio	20	

Activos	Valor	Amenazas	Riesgo	Cantidad de valores superiores o iguales a 20
		[A.15] Modificación deliberada de la información	12	
		[A.18] Destrucción de información	12	
		[A.19] Divulgación de información	5	
		[A.22] Manipulación de programas	8	
		[A.24] Denegación de servicio	2	
Servidor de almacenamiento NAS	5	[E.1] Errores de los usuarios	3	0
		[E.2] Errores del administrador	4	
		[E.3] Errores de monitorización (log)	10	
		[E.4] Errores de configuración	5	
		[E.8] Disfusión de software dañino	1	
		[E.9] Errores de [re-]encaminamiento	1	
		[E.10] Errores de secuencia	1	
		[E.15] Alteración accidental de la información	5	
		[E.18] Destrucción de información	5	
		[E.19] Fugas de información	1	
		[E.20] Vulnerabilidades de los programas (software)	1	
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	
		[E.24] Caída del sistema por agotamiento de recursos	10	
		[A.3] Manipulación de los registros de actividad (log)	10	
		[A.4] Manipulación de la configuración	6	
		[A.5] Suplantación de la identidad del usuario	3	
		[A.6] Abuso de privilegios de acceso	13	
		[A.7] Uso no previsto	3	
		[A.8] Difusión de software dañino	7	
		[A.9] [Re-]encaminamiento de mensajes	1	
		[A.10] Alteración de secuencia	1	
		[A.11] Acceso no autorizado	5	
		[A.13] Repudio	10	
		[A.15] Modificación deliberada de la información	5	
		[A.18] Destrucción de información	9	
		[A.19] Divulgación de información	4	
		[A.22] Manipulación de programas	5	
		[A.24] Denegación de servicio	2	
Servidor de disponibilidad Nagios	3	[E.1] Errores de los usuarios	2	0
		[E.2] Errores del administrador	3	
		[E.3] Errores de monitorización (log)	12	
		[E.4] Errores de configuración	5	
		[E.8] Disfusión de software dañino	0	

Activos	Valor	Amenazas	Riesgo	Cantidad de valores superiores o iguales a 20
		[E.9] Errores de [re-]encaminamiento	0	
		[E.10] Errores de secuencia	0	
		[E.15] Alteración accidental de la información	3	
		[E.18] Destrucción de información	2	
		[E.19] Fugas de información	1	
		[E.20] Vulnerabilidades de los programas (software)	1	
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	
		[E.24] Caída del sistema por agotamiento de recursos	9	
		[A.3] Manipulación de los registros de actividad (log)	12	
		[A.4] Manipulación de la configuración	2	
		[A.5] Suplantación de la identidad del usuario	2	
		[A.6] Abuso de privilegios de acceso	4	
		[A.7] Uso no previsto	1	
		[A.8] Difusión de software dañino	2	
		[A.9] [Re-]encaminamiento de mensajes	0	
		[A.10] Alteración de secuencia	0	
		[A.11] Acceso no autorizado	2	
		[A.13] Repudio	6	
		[A.15] Modificación deliberada de la información	3	
		[A.18] Destrucción de información	5	
		[A.19] Divulgación de información	2	
		[A.22] Manipulación de programas	3	
		[A.24] Denegación de servicio	1	
Servidor WEB	3	[E.1] Errores de los usuarios	3	0
		[E.2] Errores del administrador	4	
		[E.3] Errores de monitorización (log)	15	
		[E.4] Errores de configuración	5	
		[E.8] Disfusión de software dañino	0	
		[E.9] Errores de [re-]encaminamiento	0	
		[E.10] Errores de secuencia	0	
		[E.15] Alteración accidental de la información	3	
		[E.18] Destrucción de información	1	
		[E.19] Fugas de información	1	
		[E.20] Vulnerabilidades de los programas (software)	1	
		[E.21] Errores de mantenimiento / actualización de programas (software)	1	
		[E.24] Caída del sistema por agotamiento de recursos	6	

Activos	Valor	Amenazas	Riesgo	Cantidad de valores superiores o iguales a 20
		[A.3] Manipulación de los registros de actividad (log)	12	
		[A.4] Manipulación de la configuración	4	
		[A.5] Suplantación de la identidad del usuario	3	
		[A.6] Abuso de privilegios de acceso	8	
		[A.7] Uso no previsto	2	
		[A.8] Difusión de software dañino	4	
		[A.9] [Re-]encaminamiento de mensajes	0	
		[A.10] Alteración de secuencia	0	
		[A.11] Acceso no autorizado	3	
		[A.13] Repudio	6	
		[A.15] Modificación deliberada de la información	5	
		[A.18] Destrucción de información	8	
		[A.19] Divulgación de información	2	
		[A.22] Manipulación de programas	3	
		[A.24] Denegación de servicio	7	
Servidor de Antivirus	4	[E.1] Errores de los usuarios	2	0
		[E.2] Errores del administrador	3	
		[E.3] Errores de monitorización (log)	16	
		[E.4] Errores de configuración	4	
		[E.8] Disfusión de software dañino	1	
		[E.9] Errores de [re-]encaminamiento	0	
		[E.10] Errores de secuencia	0	
		[E.15] Alteración accidental de la información	6	
		[E.18] Destrucción de información	2	
		[E.19] Fugas de información	1	
		[E.20] Vulnerabilidades de los programas (software)	3	
		[E.21] Errores de mantenimiento / actualización de programas (software)	1	
		[E.24] Caída del sistema por agotamiento de recursos	8	
		[A.3] Manipulación de los registros de actividad (log)	16	
		[A.4] Manipulación de la configuración	3	
		[A.5] Suplantación de la identidad del usuario	3	
		[A.6] Abuso de privilegios de acceso	10	
		[A.7] Uso no previsto	4	
		[A.8] Difusión de software dañino	5	
		[A.9] [Re-]encaminamiento de mensajes	0	
		[A.10] Alteración de secuencia	0	
		[A.11] Acceso no autorizado	3	
		[A.13] Repudio	8	

Activos	Valor	Amenazas	Riesgo	Cantidad de valores superiores o iguales a 20
		[A.15] Modificación deliberada de la información	4	
		[A.18] Destrucción de información	7	
		[A.19] Divulgación de información	3	
		[A.22] Manipulación de programas	4	
		[A.24] Denegación de servicio	2	
Servidor de aplicación CRM	5	[E.1] Errores de los usuarios	3	0
		[E.2] Errores del administrador	4	
		[E.3] Errores de monitorización (log)	13	
		[E.4] Errores de configuración	5	
		[E.8] Disfusión de software dañino	1	
		[E.9] Errores de [re-]encaminamiento	1	
		[E.10] Errores de secuencia	1	
		[E.15] Alteración accidental de la información	8	
		[E.18] Destrucción de información	3	
		[E.19] Fugas de información	2	
		[E.20] Vulnerabilidades de los programas (software)	1	
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	
		[E.24] Caída del sistema por agotamiento de recursos	5	
		[A.3] Manipulación de los registros de actividad (log)	16	
		[A.4] Manipulación de la configuración	6	
		[A.5] Suplantación de la identidad del usuario	3	
		[A.6] Abuso de privilegios de acceso	6	
		[A.7] Uso no previsto	3	
		[A.8] Difusión de software dañino	7	
		[A.9] [Re-]encaminamiento de mensajes	1	
		[A.10] Alteración de secuencia	1	
		[A.11] Acceso no autorizado	4	
		[A.13] Repudio	10	
		[A.15] Modificación deliberada de la información	5	
		[A.18] Destrucción de información	9	
		[A.19] Divulgación de información	4	
		[A.22] Manipulación de programas	5	
		[A.24] Denegación de servicio	4	
Servidor de aplicaciones RRHH	4	[E.1] Errores de los usuarios	3	0
		[E.2] Errores del administrador	4	
		[E.3] Errores de monitorización (log)	16	
		[E.4] Errores de configuración	4	
		[E.8] Disfusión de software dañino	0	

Activos	Valor	Amenazas	Riesgo	Cantidad de valores superiores o iguales a 20
		[E.9] Errores de [re-]encaminamiento	0	
		[E.10] Errores de secuencia	0	
		[E.15] Alteración accidental de la información	4	
		[E.18] Destrucción de información	2	
		[E.19] Fugas de información	2	
		[E.20] Vulnerabilidades de los programas (software)	1	
		[E.21] Errores de mantenimiento / actualización de programas (software)	1	
		[E.24] Caída del sistema por agotamiento de recursos	4	
		[A.3] Manipulación de los registros de actividad (log)	16	
		[A.4] Manipulación de la configuración	5	
		[A.5] Suplantación de la identidad del usuario	2	
		[A.6] Abuso de privilegios de acceso	8	
		[A.7] Uso no previsto	2	
		[A.8] Difusión de software dañino	5	
		[A.9] [Re-]encaminamiento de mensajes	0	
		[A.10] Alteración de secuencia	0	
		[A.11] Acceso no autorizado	8	
		[A.13] Repudio	8	
		[A.15] Modificación deliberada de la información	4	
		[A.18] Destrucción de información	7	
		[A.19] Divulgación de información	6	
		[A.22] Manipulación de programas	4	
		[A.24] Denegación de servicio	3	
Servidor de aplicación - SPC	3	[E.1] Errores de los usuarios	2	0
		[E.2] Errores del administrador	3	
		[E.3] Errores de monitorización (log)	15	
		[E.4] Errores de configuración	3	
		[E.8] Disfusión de software dañino	0	
		[E.9] Errores de [re-]encaminamiento	0	
		[E.10] Errores de secuencia	0	
		[E.15] Alteración accidental de la información	3	
		[E.18] Destrucción de información	2	
		[E.19] Fugas de información	1	
		[E.20] Vulnerabilidades de los programas (software)	1	
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	
		[E.24] Caída del sistema por agotamiento de recursos	6	

Activos	Valor	Amenazas	Riesgo	Cantidad de valores superiores o iguales a 20
		[A.3] Manipulación de los registros de actividad (log)	12	
		[A.4] Manipulación de la configuración	2	
		[A.5] Suplantación de la identidad del usuario	2	
		[A.6] Abuso de privilegios de acceso	8	
		[A.7] Uso no previsto	2	
		[A.8] Difusión de software dañino	4	
		[A.9] [Re-]encaminamiento de mensajes	0	
		[A.10] Alteración de secuencia	0	
		[A.11] Acceso no autorizado	2	
		[A.13] Repudio	6	
		[A.15] Modificación deliberada de la información	3	
		[A.18] Destrucción de información	5	
		[A.19] Divulgación de información	2	
		[A.22] Manipulación de programas	3	
		[A.24] Denegación de servicio	2	
Servidor de aplicación - Indicadores	2	[E.1] Errores de los usuarios	1	0
		[E.2] Errores del administrador	2	
		[E.3] Errores de monitorización (log)	10	
		[E.4] Errores de configuración	2	
		[E.8] Disfusión de software dañino	0	
		[E.9] Errores de [re-]encaminamiento	0	
		[E.10] Errores de secuencia	0	
		[E.15] Alteración accidental de la información	2	
		[E.18] Destrucción de información	1	
		[E.19] Fugas de información	0	
		[E.20] Vulnerabilidades de los programas (software)	1	
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	
		[E.24] Caída del sistema por agotamiento de recursos	4	
		[A.3] Manipulación de los registros de actividad (log)	8	
		[A.4] Manipulación de la configuración	2	
		[A.5] Suplantación de la identidad del usuario	1	
		[A.6] Abuso de privilegios de acceso	5	
		[A.7] Uso no previsto	2	
		[A.8] Difusión de software dañino	3	
		[A.9] [Re-]encaminamiento de mensajes	0	
		[A.10] Alteración de secuencia	0	
		[A.11] Acceso no autorizado	1	
		[A.13] Repudio	4	

Activos	Valor	Amenazas	Riesgo	Cantidad de valores superiores o iguales a 20
		[A.15] Modificación deliberada de la información	2	
		[A.18] Destrucción de información	4	
		[A.19] Divulgación de información	2	
		[A.22] Manipulación de programas	2	
		[A.24] Denegación de servicio	1	
Central Telefónica	4	[E.1] Errores de los usuarios	2	1
		[E.2] Errores del administrador	6	
		[E.3] Errores de monitorización (log)	20	
		[E.4] Errores de configuración	6	
		[E.8] Disfusión de software dañino	1	
		[E.9] Errores de [re-]encaminamiento	4	
		[E.10] Errores de secuencia	6	
		[E.15] Alteración accidental de la información	6	
		[E.18] Destrucción de información	2	
		[E.19] Fugas de información	1	
		[E.20] Vulnerabilidades de los programas (software)	1	
		[E.21] Errores de mantenimiento / actualización de programas (software)	1	
		[E.24] Caída del sistema por agotamiento de recursos	8	
		[A.3] Manipulación de los registros de actividad (log)	16	
		[A.4] Manipulación de la configuración	6	
		[A.5] Suplantación de la identidad del usuario	11	
		[A.6] Abuso de privilegios de acceso	15	
		[A.7] Uso no previsto	4	
		[A.8] Difusión de software dañino	5	
		[A.9] [Re-]encaminamiento de mensajes	4	
		[A.10] Alteración de secuencia	4	
		[A.11] Acceso no autorizado	14	
		[A.13] Repudio	16	
		[A.15] Modificación deliberada de la información	6	
		[A.18] Destrucción de información	11	
		[A.19] Divulgación de información	3	
		[A.22] Manipulación de programas	4	
		[A.24] Denegación de servicio	2	
Firewall perimetral	5	[E.1] Errores de los usuarios	3	3
		[E.2] Errores del administrador	7	
		[E.3] Errores de monitorización (log)	25	
		[E.4] Errores de configuración	8	
		[E.8] Disfusión de software dañino	1	

Activos	Valor	Amenazas	Riesgo	Cantidad de valores superiores o iguales a 20
		[E.9] Errores de [re-]encaminamiento	5	
		[E.10] Errores de secuencia	5	
		[E.15] Alteración accidental de la información	8	
		[E.18] Destrucción de información	3	
		[E.19] Fugas de información	1	
		[E.20] Vulnerabilidades de los programas (software)	1	
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	
		[E.24] Caída del sistema por agotamiento de recursos	10	
		[A.3] Manipulación de los registros de actividad (log)	20	
		[A.4] Manipulación de la configuración	16	
		[A.5] Suplantación de la identidad del usuario	8	
		[A.6] Abuso de privilegios de acceso	13	
		[A.7] Uso no previsto	3	
		[A.8] Difusión de software dañino	7	
		[A.9] [Re-]encaminamiento de mensajes	8	
		[A.10] Alteración de secuencia	8	
		[A.11] Acceso no autorizado	11	
		[A.13] Repudio	25	
		[A.15] Modificación deliberada de la información	10	
		[A.18] Destrucción de información	9	
		[A.19] Divulgación de información	6	
		[A.22] Manipulación de programas	5	
		[A.24] Denegación de servicio	2	
Switch de distribución/acceso	4	[E.1] Errores de los usuarios	4	0
		[E.2] Errores del administrador	7	
		[E.3] Errores de monitorización (log)	16	
		[E.4] Errores de configuración	6	
		[E.8] Disfusión de software dañino	0	
		[E.9] Errores de [re-]encaminamiento	4	
		[E.10] Errores de secuencia	4	
		[E.15] Alteración accidental de la información	6	
		[E.18] Destrucción de información	2	
		[E.19] Fugas de información	1	
		[E.20] Vulnerabilidades de los programas (software)	1	
		[E.21] Errores de mantenimiento / actualización de programas (software)	1	
		[E.24] Caída del sistema por agotamiento de recursos	8	

Activos	Valor	Amenazas	Riesgo	Cantidad de valores superiores o iguales a 20
		[A.3] Manipulación de los registros de actividad (log)	16	
		[A.4] Manipulación de la configuración	13	
		[A.5] Suplantación de la identidad del usuario	4	
		[A.6] Abuso de privilegios de acceso	12	
		[A.7] Uso no previsto	2	
		[A.8] Difusión de software dañino	5	
		[A.9] [Re-]encaminamiento de mensajes	6	
		[A.10] Alteración de secuencia	6	
		[A.11] Acceso no autorizado	6	
		[A.13] Repudio	16	
		[A.15] Modificación deliberada de la información	6	
		[A.18] Destrucción de información	11	
		[A.19] Divulgación de información	3	
		[A.22] Manipulación de programas	4	
		[A.24] Denegación de servicio	2	

Con base en la Tabla 2.10, se selecciona los 5 activos a monitorear contemplados en el alcance de este proyecto, los cuales poseen la mayor cantidad de valores superiores a 20 en la escala de riesgo:

- Firewall
- Central telefónica
- Servidor de virtualización Main
- Servidor de Active Directory
- Servidor de Archivos MicroDM

2.3 PLANIFICACIÓN PARA LA RECOLECCIÓN DE LOGS

Para el monitoreo de cada activo se debe considerar el método de recolección de logs, ya sea por medio de la instalación de un agente o a través de la configuración de envío de logs propia de cada equipo hacia un servidor remoto.

OSSIM por defecto permite la recolección de logs utilizando agentes OSSEC, los cuales utilizan el puerto UDP/1514, y la recolección a través del uso del protocolo syslog, el cual usa por defecto el puerto UDP/514 [4]. Al utilizar agentes OSSEC, es necesario que se habilite el tráfico bidireccional usando el puerto origen y destino UDP/1514 [4].

Por otro lado, al utilizar el protocolo syslog, solo es necesario habilitar el tráfico unidireccional desde el activo a monitorear hasta la plataforma OSSIM.

Una característica adicional que cuenta OSSIM es el sistema detector de intrusiones (IDS), el cual requiere la configuración de un puerto espejo (Port Mirror) en el switch de core, y que este se encuentre conectado directamente hacia una interfaz de red de OSSIM.

La Figura 2.2 muestra el diagrama lógico de red para la recolección de logs y el análisis de red mediante un port mirror, adicionalmente en la Tabla 2.11 se presenta el direccionamiento IP correspondiente utilizado en los activos a monitorear y en la plataforma OSSIM.

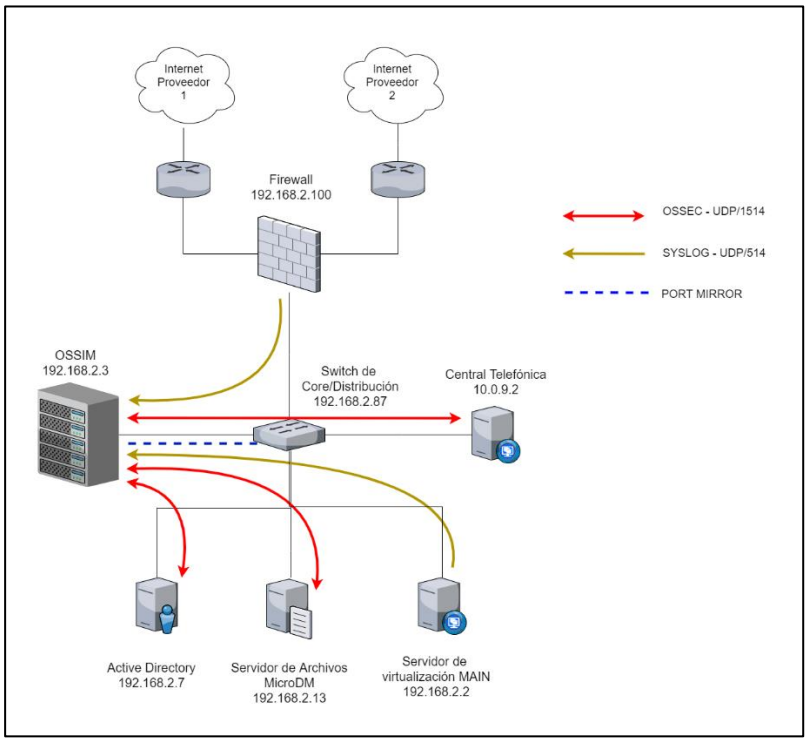


Figura 2.2. Diagrama de Red

Tabla 2.11. Direccionamiento IP

Equipo	**Dirección IP**
Firewall	192.168.2.100
Servidor de virtualización Main	192.168.2.2
Active Directory	192.168.2.7
Servidor de Archivos - MicroDM	192.168.2.13
Central Telefónica	10.0.9.2
OSSIM	192.168.2.3

- En el equipo 192.168.2.7 (Active Directory), se realizará la instalación del agente OSSEC, que genera de manera automática la plataforma OSSIM para sistemas operativos Windows.
- En los equipos 10.0.9.2 (Central Telefónica) y 192.168.2.13 (Servidor de Archivos MicroDM), se realizará la instalación del agente OSSEC correspondiente para plataformas Linux, el cual se descargará de la página oficial https://github.com/ossec/ossec-hids/releases
- En los equipos 192.168.2.100 (Firewall) y 192.168.2.2 (Servidor Main) se configurará el envío de logs mediante el uso del servicio syslog perteneciente a cada plataforma.

2.4 DISEÑO DE DIAGRAMA DE FLUJO PARA LA GENERACIÓN DE DIRECTIVAS DE CORRELACIÓN

Con base en las capacidades de correlación que tiene la plataforma OSSIM, se procedió a diseñar los diagramas de flujo que permitan la detección de los siguientes incidentes:

- Ataque de fuerza bruta
- Cambios en la configuración
- Conexiones hacia direcciones IP que permite el firewall

2.4.1 DIAGRAMA DE FLUJO PARA LA DETECCIÓN DE ATAQUE DE FUERZA BRUTA

Para el diseño del diagrama se ha tomado como guía el artículo “Successful SIEM and Log Management Strategies for Audit and Compliance” [11] y la información presentada por el fabricante PaloAlto Networks en la base de conocimiento [12] que indican las condiciones de detección de un ataque de fuerza bruta. En [11] se menciona que debe considerarse un ataque de fuerza bruta cuando existen más de 3 accesos fallidos en el lapso de 60 segundos desde la misma dirección IP origen. En [12] se indica que debe considerarse un ataque de fuerza bruta cuando existen 30 accesos fallidos en el lapso de 60 segundos.

Con base en los documentos descritos y tomando las consideraciones del personal custodio del activo se planteó 4 niveles de correlación para la detección de un ataque de fuerza bruta. En la Figura 2.3 se muestra el diagrama de flujo genérico para la detección de ataques de fuerza bruta.

A continuación, se presenta el detalle del diagrama mostrado en la Figura 2.3

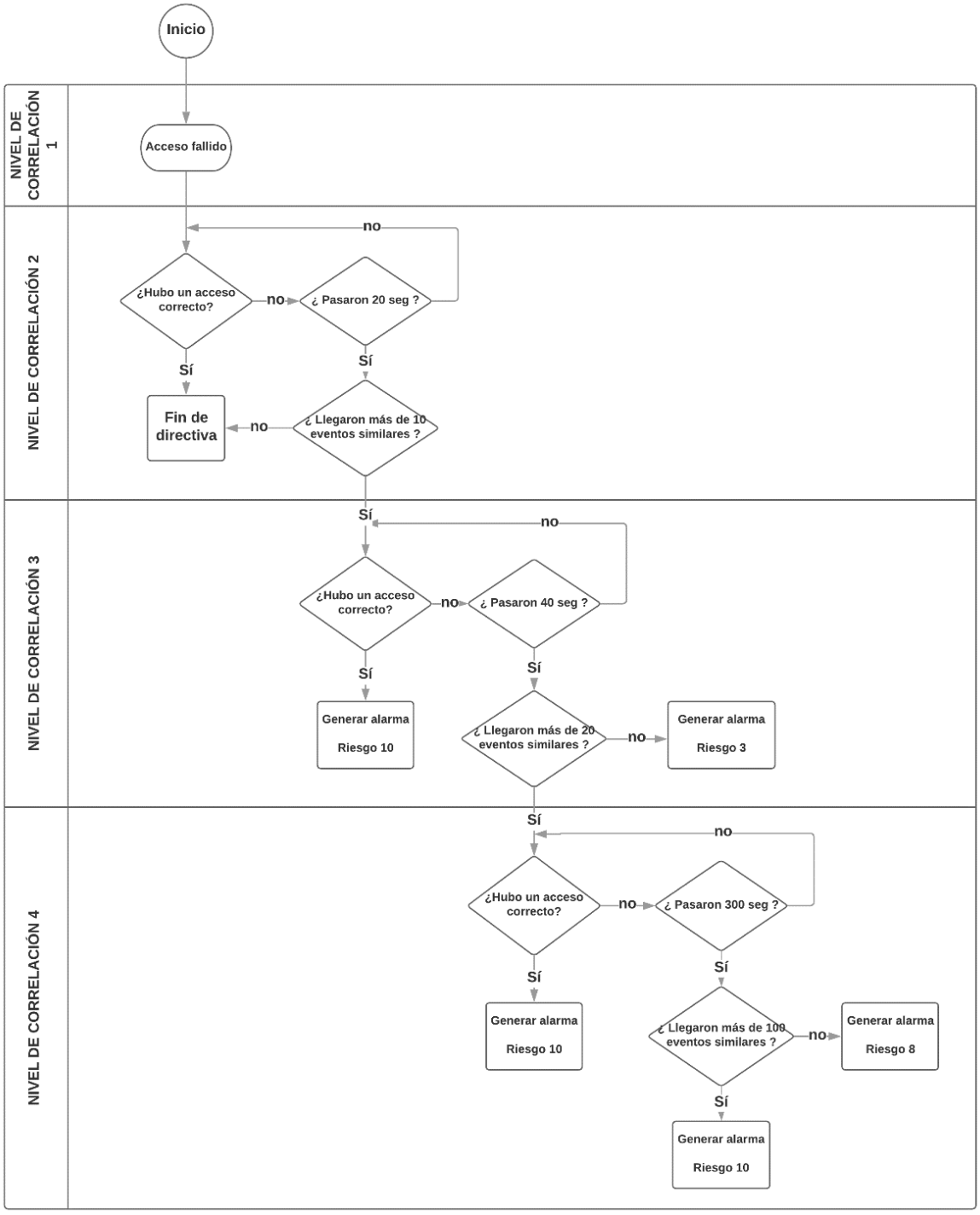


Figura 2.3. Diagrama de flujo - Ataque de fuerza bruta

2.4.1.1 Primer nivel de correlación

En primer lugar, cuando se detecte un evento de acceso fallido, se iniciará la ejecución de la directiva de ataque de fuerza bruta.

2.4.1.2 Segundo nivel de correlación

Después de 20 segundos de llegar el primer evento de acceso fallido, se validará si llegaron más de 10 eventos similares. Si no se ha recibido más de 10, se dará por terminada toda la directiva y no se generará ninguna alarma. Por el contrario, si se recibieron más de 10 eventos de acceso fallido, se dará lugar al inicio del tercer nivel de correlación.

2.4.1.3 Tercer nivel de correlación

Este nivel tendrá una duración de 40 segundos, si durante los 40 segundos no llegan más de 20 eventos, se verificará si hubo un acceso correcto. En caso de haber un acceso correcto, se generará una alarma de riesgo 10, puesto que se trataría de un ataque exitoso. De no recibir un evento de acceso exitoso, se generaría una alarma de riesgo 3, ya que pudiera tratarse de un posible ataque de fuerza bruta fallido. Si llegan más de 20 accesos fallidos, entraría a ejecutarse el cuarto nivel de correlación.

2.4.1.4 Cuarto nivel de correlación

Este nivel tendrá una duración de 300 segundos, si durante los 300 segundos no llegan más de 100 eventos, se verificará si hubo un acceso correcto. En caso de haber un acceso correcto, se generará una alarma de riesgo 10, puesto que se trataría de un ataque exitoso. De no recibir un evento de acceso exitoso, se generaría una alarma de riesgo 8, ya que pudiera tratarse de un posible ataque de fuerza bruta fallido. Si llegan más de 100 accesos fallidos, se generaría una alarma de riesgo 10.

2.4.2 DIAGRAMA DE FLUJO PARA LA DETECCIÓN DE CAMBIOS EN LA CONFIGURACIÓN

OSSIM permite la detección de cambios de configuración mediante 2 maneras:

- Detección de cambios basados en eventos generados por el propio sistema como creación de usuarios, modificación de usuarios, creación de grupos, etc.
- Detección de integridad de archivos a través del agente OSSEC. El agente OSSEC instalado en los servidores Linux y Windows permite llevar un monitoreo a archivos específicos definidos por el usuario.

A manera de prueba de concepto, se realizó el monitoreo de cambio de configuración basado en eventos generados por cada uno de los activos de monitoreo (OSSEC y Syslog), utilizando como referencia la creación de usuarios. Para la detección de integridad de archivos de configuración se usó como referencia la detección de cambios en el archivo /etc/sudoers en los sistemas Linux y la detección de cambios en el archivo

C:\Windows\System32\drivers\etc\hosts en los sistemas Windows, utilizando el monitoreo de OSSEC.

Para el diseño de las directivas se tuvo en consideración si los cambios realizados fueron por un usuario administrador

2.4.2.1 Creación de Usuario

La detección de estos eventos está enfocada en generar visibilidad de cambios que se produzcan a nivel de usuarios, ya que estándares de seguridad como PCI DSS, establecen como un requerimiento que se tenga una evidencia de todas las actividades de creación, borrado y modificación de usuarios [13].

En la Figura 2.4 se tiene el diseño de las directivas que permitirán detectar la creación de usuarios en los sistemas a monitorear. Las directivas que se aplican tienen un nivel de correlación.

2.4.2.1.1 Primer nivel de correlación

Cuando se detecte un evento de creación de usuario, se aplicará una distinción sobre si el usuario que realizó la acción pertenece al grupo de administradores registrados. En caso de no serlo, se generará una alarma de riesgo 8. En el caso que el usuario que realizó la acción pertenezca al grupo de administradores se generará una alarma de riesgo 2

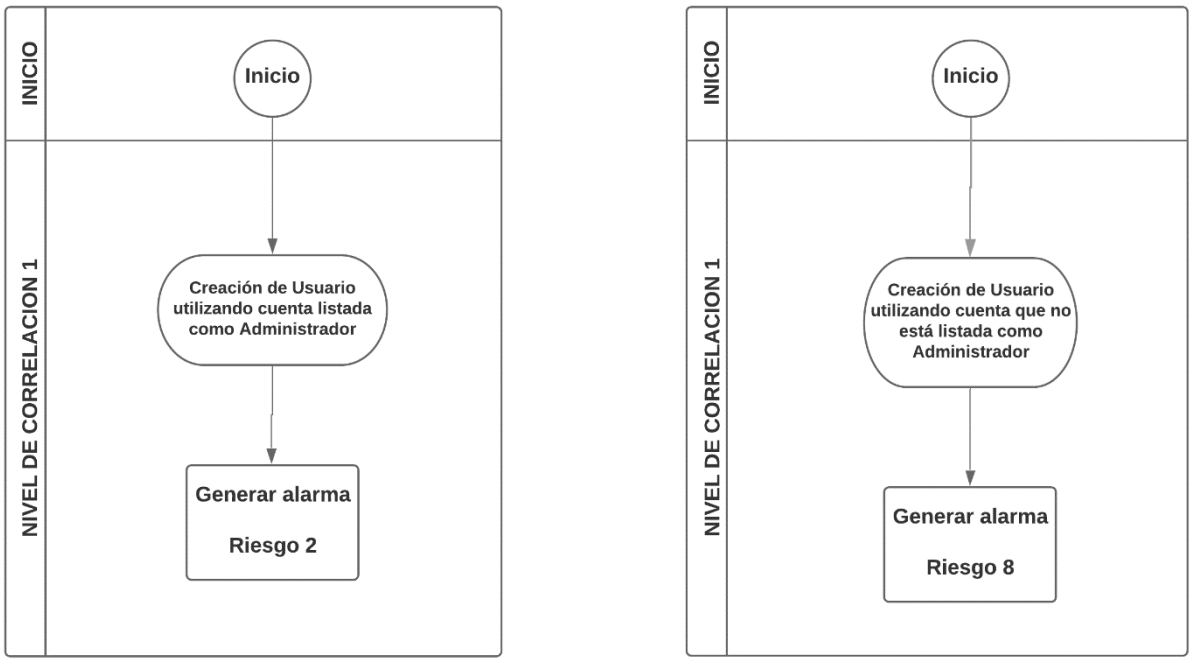


Figura 2.4. Diagrama de flujo - Detección de creación de usuarios

2.4.2.2 Modificación en la integridad de archivos

Utilizando agentes OSSEC, se puede tener una visibilidad de cambios que se produzcan en archivos específicos, ya que estándares de seguridad como PCI DSS, establecen como un requerimiento que se tenga una trazabilidad de la integridad de archivos críticos [13].

En la Figura 2.5 se tiene el diseño de las directivas que permitirán detectar la modificación de archivos específicos en los activos Windows y Linux. La directiva que se aplica tiene un nivel de correlación

2.4.2.2.1 Primer nivel de correlación

Cuando se detecte un evento de modificación de archivos, se generará una alarma de riesgo 10, debido a que los archivos de configuración a monitorear son críticos y es necesario validar si la configuración fue acordada.

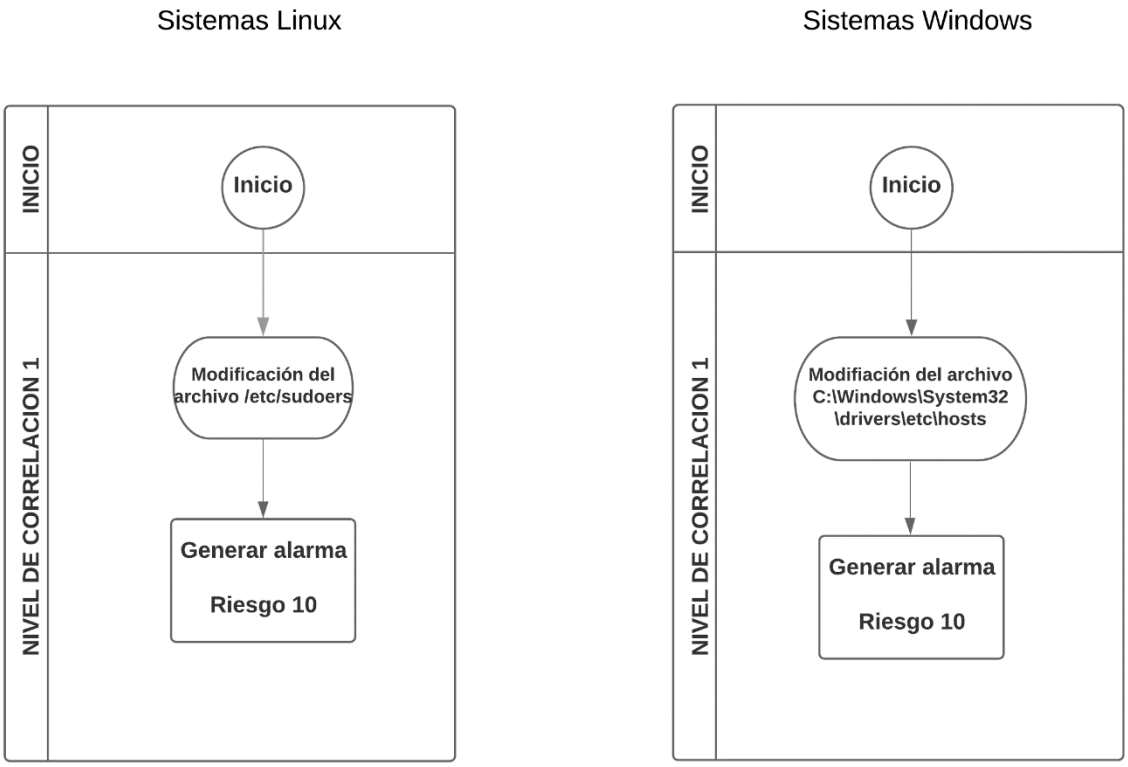
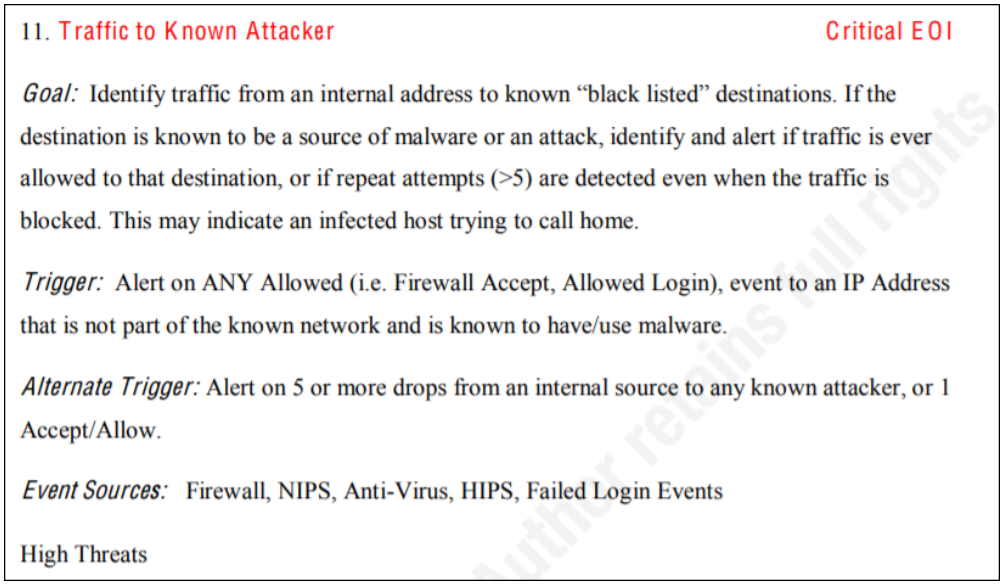


Figura 2.5. Diagrama de flujo - Detección de modificación de integridad

2.4.3 DIAGRAMA DE FLUJO PARA DETECCIÓN DE CONEXIONES HACIA IP MALICIOSAS

De acuerdo con el artículo [11], uno de los eventos que se debe tener interés en monitorear, es el de conexiones que el firewall está permitiendo pasar, teniendo como origen una

dirección IP local hacia una dirección IP pública marcada como maliciosa como se indica en la Figura 2.6.



11. Traffic to Known Attacker — Critical EOI

Goal: Identify traffic from an internal address to known "black listed" destinations. If the destination is known to be a source of malware or an attack, identify and alert if traffic is ever allowed to that destination, or if repeat attempts (>5) are detected even when the traffic is blocked. This may indicate an infected host trying to call home.

Trigger: Alert on ANY Allowed (i.e. Firewall Accept, Allowed Login), event to an IP Address that is not part of the known network and is known to have/use malware.

Alternate Trigger: Alert on 5 or more drops from an internal source to any known attacker, or 1 Accept/Allow.

Event Sources: Firewall, NIPS, Anti-Virus, HIPS, Failed Login Events

High Threats

Figura 2.6. Monitoreo de conexiones salientes desde el firewall

Se indica como directriz, la detección de todas las conexiones que se realicen desde la red Local hacia direcciones IP externas que sean conocidas por ser fuente de malware o por ser propensas a realizar ataques. Inclusive se indica que es necesario la detección de conexiones que el firewall se encuentre bloqueando si la cantidad supera el valor de 5. Esto por el motivo que un equipo perteneciente a la red se encuentre comprometido, y el malware asociado intenta comunicarse con la fuente que lo generó.

Para el diseño de la directiva se contempló solo los accesos que el firewall se encuentre permitiendo hacia direcciones IP denunciadas como maliciosas.

En la Figura 2.7 se muestra el diagrama de flujo genérico para la detección de conexiones desde la red interna hacia direcciones IP denunciadas como maliciosas. La directiva que se aplica tiene un nivel de correlación.

2.4.3.1 Primer nivel de correlación

Cuando se detecte un evento de conexión permitido hacia internet, se evaluará si la dirección IP destino se encuentra catalogada como maliciosa en el repositorio de amenazas OTX (Open Threat Exchange), el cual tiene total integración con OSSIM. Si la IP se encuentra listada, se generará una alarma de riesgo 10. En caso de no estar listada, no se generará ninguna alarma.

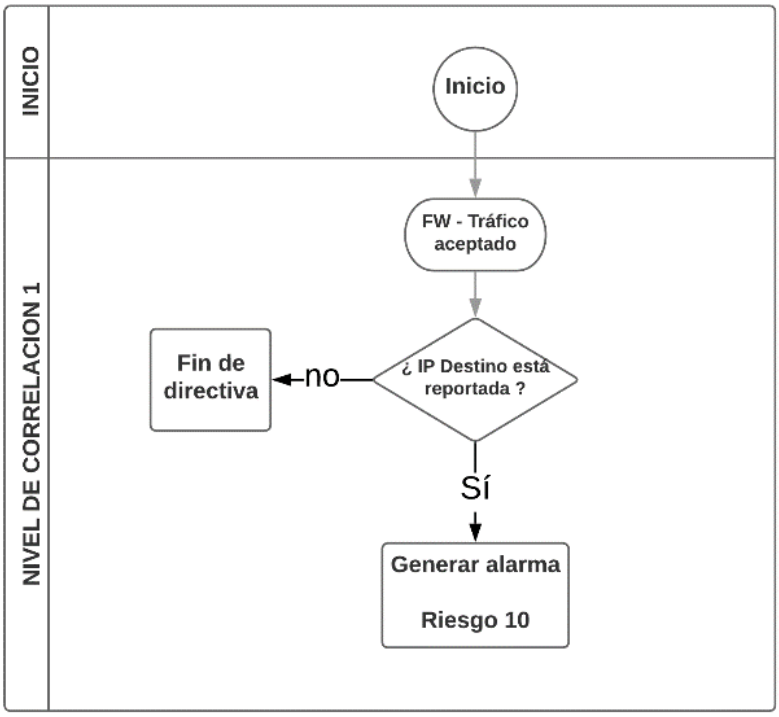


Figura 2.7. Diagrama de flujo - Detección de conexiones maliciosas

2.5 IMPLEMENTACIÓN DE OSSIM

En esta sección se presenta los pasos a realizar para la instalación de la plataforma OSSIM, así como la integración de los activos a monitorear usando agentes OSSEC y el envío de logs usando el protocolo syslog.

2.5.1 PARÁMETROS TÉCNICOS NECESARIOS

Para el funcionamiento de OSSIM es necesario que se cumplan un mínimo de requisitos de hardware (RAM, CPU, Almacenamiento), además de permisos en el firewall para la salida a internet y la conectividad a los activos a monitorear.

2.5.1.1 Requerimientos de Hardware [4]

Como requerimientos para la instalación de la plataforma OSSIM, se recomienda que se cumpla como mínimo los siguientes requisitos:

- 2 CPU cores
- 4 GB RAM
- 250 GB HDD
- E100 tarjeta de red compatible

Estos requisitos podrán variar dependiendo de la cantidad de activos que se vaya a monitorear o a la cantidad de logs que se reciba.

2.5.1.2 Requerimientos de Red

Para la administración de la plataforma OSSIM, es necesario contar con dos interfaces de red. La primera interfaz de red debe tener asignada una dirección IP, la cual será utilizada para la administración de la plataforma y, también será utilizada para la recepción de logs de los equipos que tengan instalado el respectivo agente OSSEC o los equipos que se encuentren configurados para el envío por syslog.

La segunda interfaz, debe ser configurada en modo promiscuo y se utilizará para el análisis de red. Esta última interfaz no tendrá asignada ninguna dirección IP y estará conectada directamente hacia un puerto específico del switch de core, el cual se haya configurado como un puerto espejo (SPAN Port).

En la Tabla 2.12 se presentan los permisos necesarios a internet, los cuales se utiliza para la descarga de actualizaciones o funcionalidades de distintos servicios como la conexión a OTX. En la Tabla 2.13 se presentan los permisos necesarios a nivel de la red local para la conexión de los agentes OSSEC y la recepción de logs mediante syslog [4].

Tabla 2.12. Requerimientos de Internet

NETWORKING EXTERNO			
IP Origen	**Dominio/IP Destino**	**Protocolo**	**Puerto**
IP OSSIM	data.alienvault.com	TCP	80
	maps.google.com		
	maps.gstatic.com		
	www.google.com		
	maps-api-ssl.google.com	TCP	443
	maps.googleapis.com		
	messages.alienvault.com		
	telemetry.alienvault.com		
	reputation.alienvault.com		
	otx.alienvault.com		
	tractorbeam.alienvault.com		
	tractorbeam.alienvault.com	TCP	22

Tabla 2.13. Requerimientos de Red Interno

NETWORKING INTERNO			
IP Origen	**IP Destino**	**Protocolo**	**Puerto**
Red LAN	IP OSSIM	UDP	514
			1514
IP OSSIM	Red LAN	UDP	1514

2.5.2 INSTALACIÓN DE OSSIM

Para la instalación de OSSIM se utilizó el servidor IBM System x3550 M4 Server, el cual tiene las siguientes características:

- 12 CPUs x Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz
- 99,93 GB RAM
- 550 GB HDD

El entorno de virtualización que se utilizó para la instalación es VMware 6.7.0 Update 1 (Build 10302608).

La imagen .ISO se la descargó del siguiente enlace proporcionado en [14].

A continuación, asignó el nombre “OSSIM – GMS UIO” a la máquina virtual asignada para la instalación de OSSIM y se configuró con los recursos que se indican en la Figura 2.8.

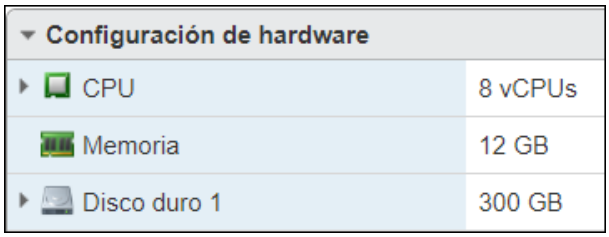


Figura 2.8 Configuración de Máquina Virtual

Una vez que se terminó de configurar los requisitos de hardware, se añadió una unidad de CD/DVD y se seleccionó el archivo .ISO de OSSIM para comenzar con la instalación como se muestra en la Figura 2.9.

Figura 2.9. Carga de ISO OSSIM

2.5.2.1 Opciones de Instalación

La pantalla inicial de instalación que se muestra en la Figura 2.10, permite elegir el tipo de instalación disponible. Se puede elegir una instalación completa de OSSIM (All-in-One) o la instalación únicamente del modo sensor.

- **Instalación completa OSSIM (All-in-One):** Con esta opción se tiene en una única instancia la parte de servidor OSSIM y sensor recolector de logs OSSIM
- **Instalación de sensor OSSIM:** Con esta opción se tiene un único sensor. Este sensor debe ir conectado a otra instancia en donde se encuentre el servidor OSSIM.

En este caso se seleccionó la primera opción, ya que se va a ocupar el sensor y servidor OSSIM en una única instancia.

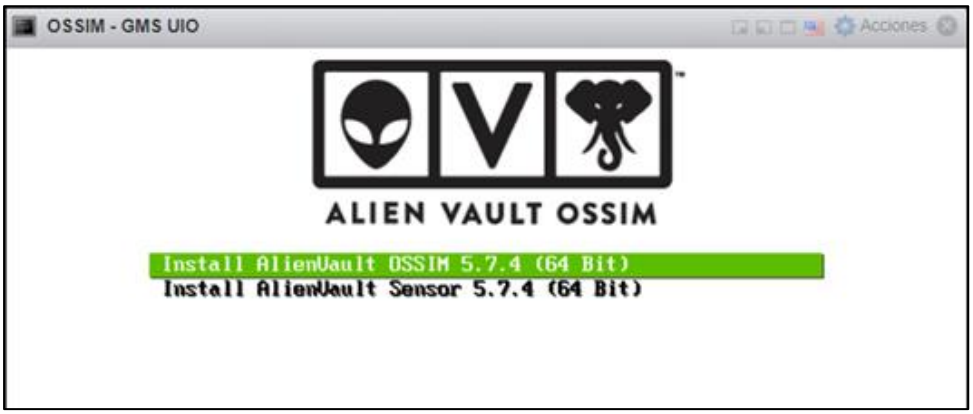


Figura 2.10. Pantalla de instalación OSSIM

2.5.2.2 Idioma y región de instalación

Se eligió idioma por defecto el inglés, como se observa en la Figura 2.11.

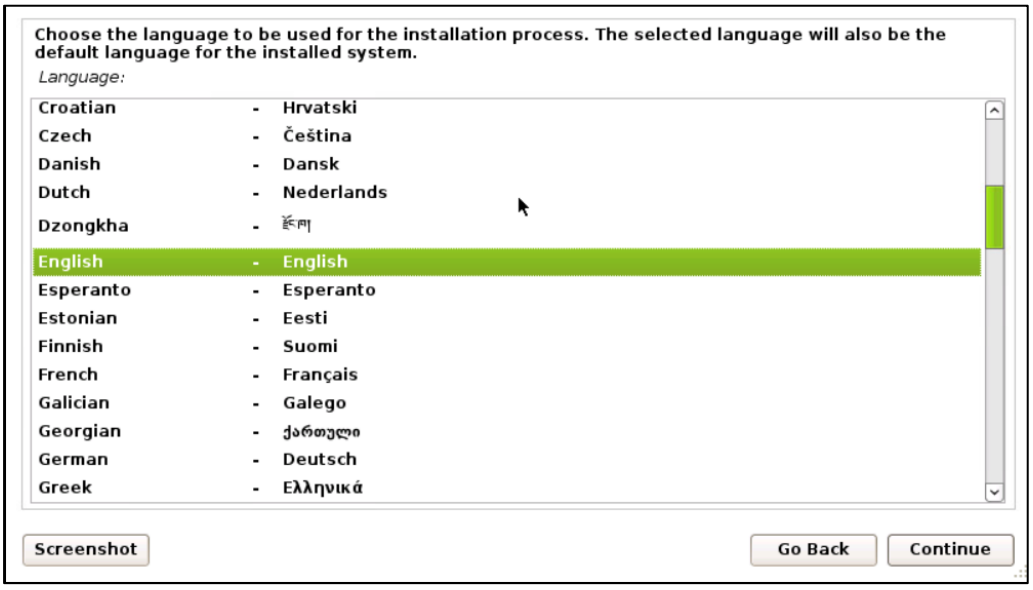


Figura 2.11. Idioma y región de instalación

Como ubicación se seleccionó Ecuador como se muestra en la Figura 2.12.

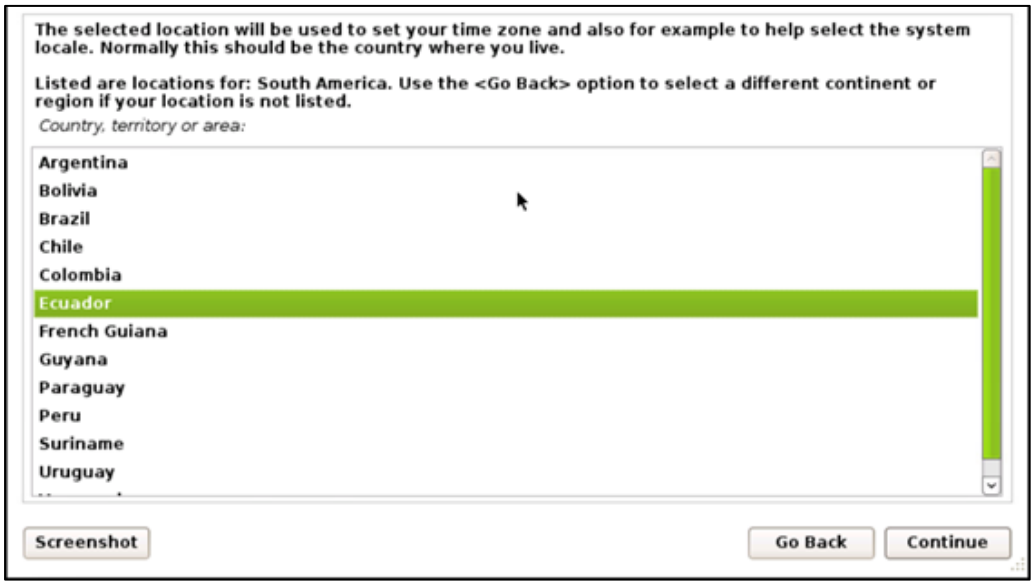


Figura 2.12. Selección de ubicación

Para la configuración regional del idioma, se seleccionó la codificación “en_US_UTF-8” perteneciente a Estados Unidos como se indica en la Figura 2.2

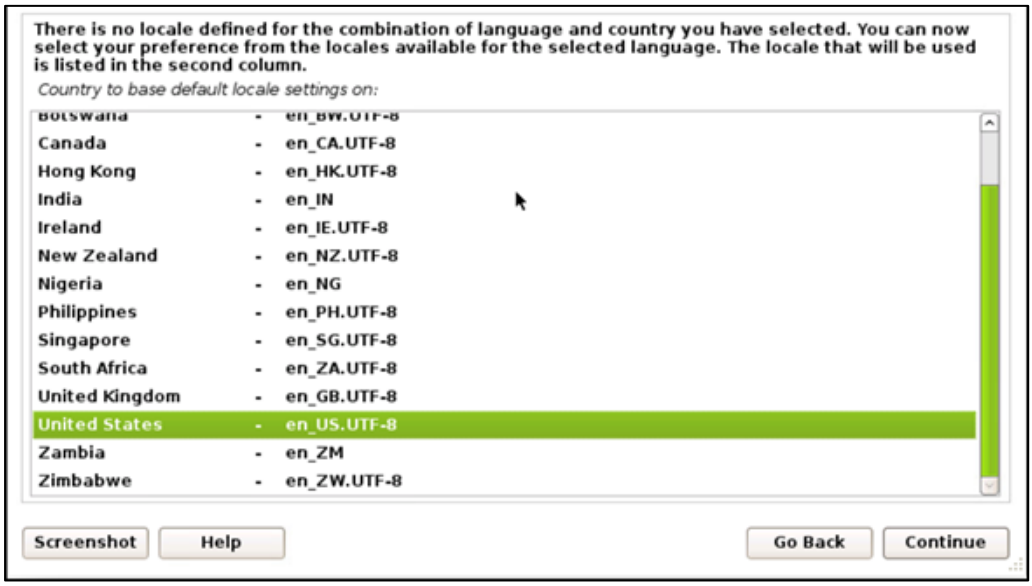


Figura 2.13. Configuración regional

En la configuración del teclado se seleccionó el de Latinoamérica como se tiene en la Figura 2.14.

2.5.2.3 Configuración de red

Se asignó a la plataforma OSSIM la dirección IP 192.168.2.3, definida en 2.3,2.5.1.2 como se muestra en la Figura 2.15. Adicionalmente, se configuró la máscara de red, Gateway y

dirección de DNS como se indican en Figura 2.16, Figura 2.17 y Figura 2.18 respectivamente.

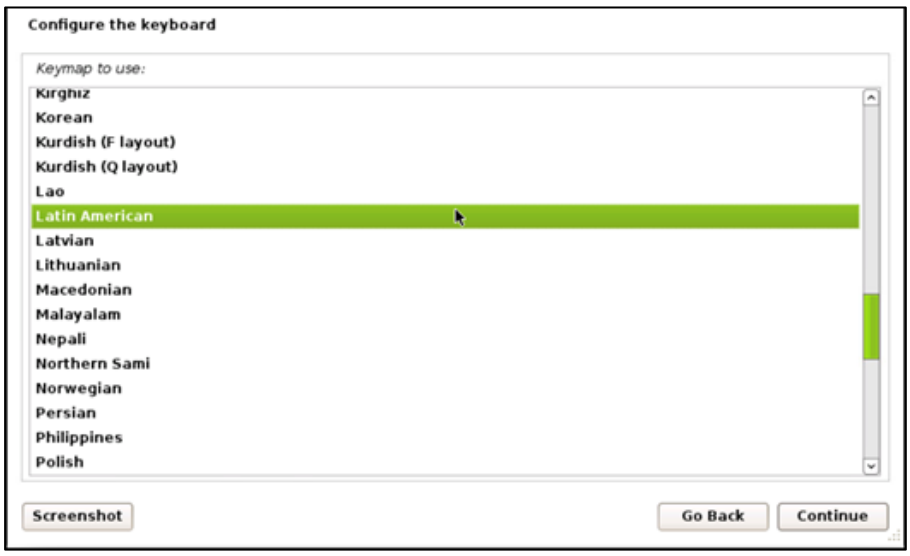


Figura 2.14. Configuración de teclado

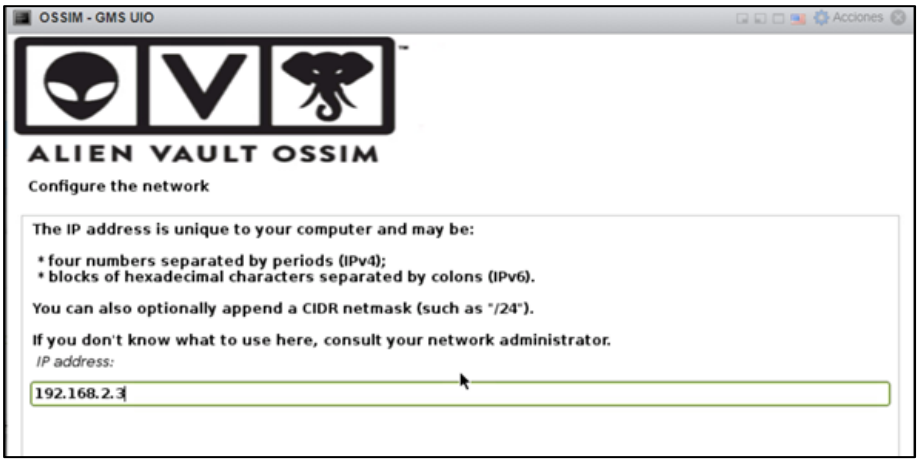


Figura 2.15. Configuración dirección IP OSSIM

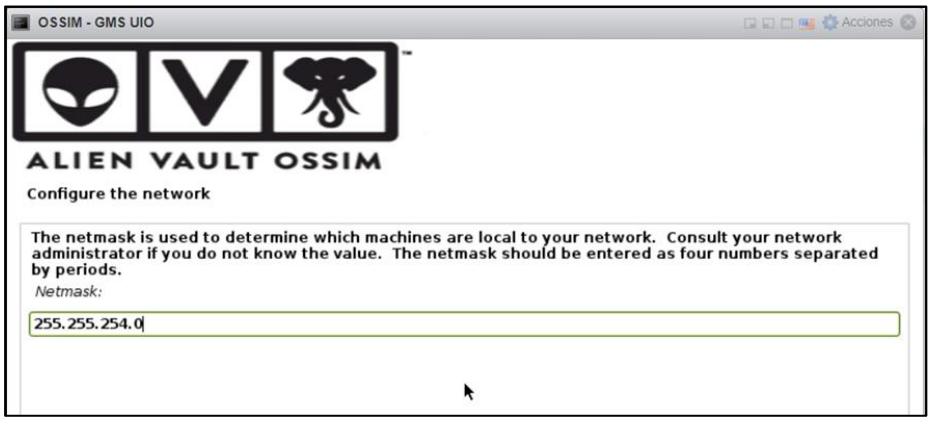


Figura 2.16. Configuración de máscara de red

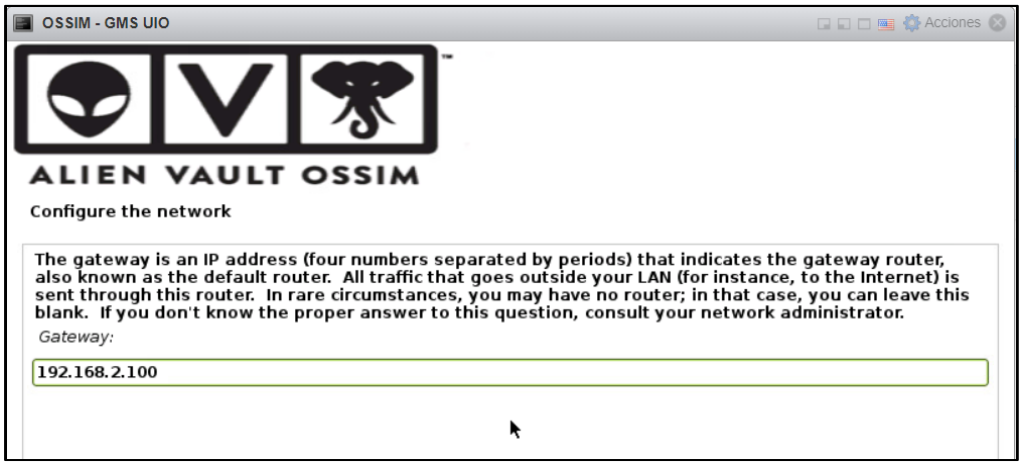


Figura 2.17. Configuración de gateway

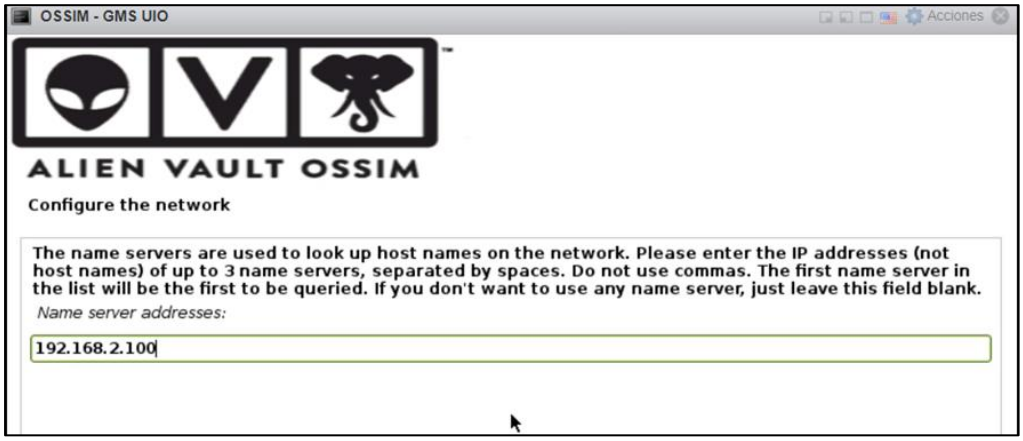


Figura 2.18. Configuración de DNS

2.5.2.4 Configuración de contraseña y región horaria

Se estableció la contraseña de administración de la plataforma web, la cual será también utilizada para el acceso al modo consola como se observa en Figura 2.19

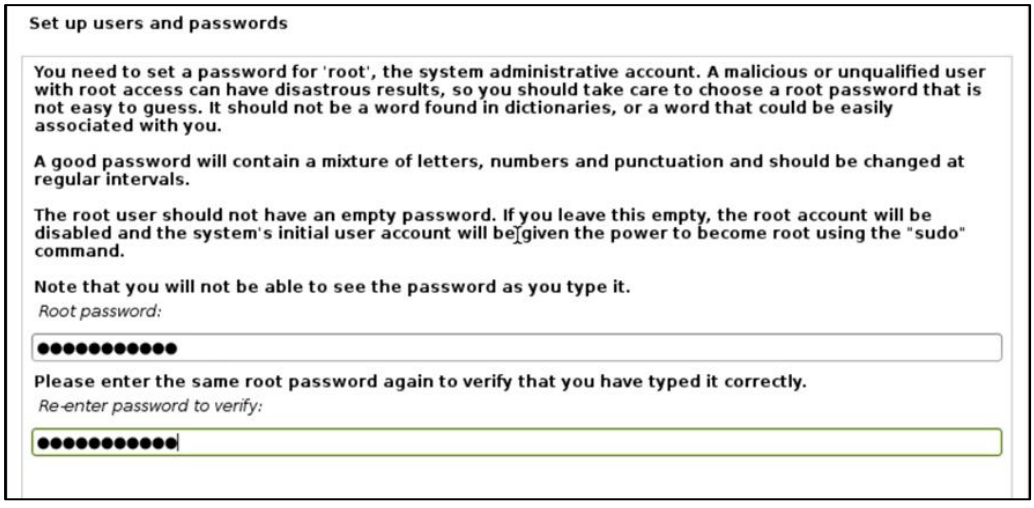


Figura 2.19. Configuración de usuario root

La región seleccionada para la hora es la de Guayaquil (GMT -5) como se indica en Figura 2.20

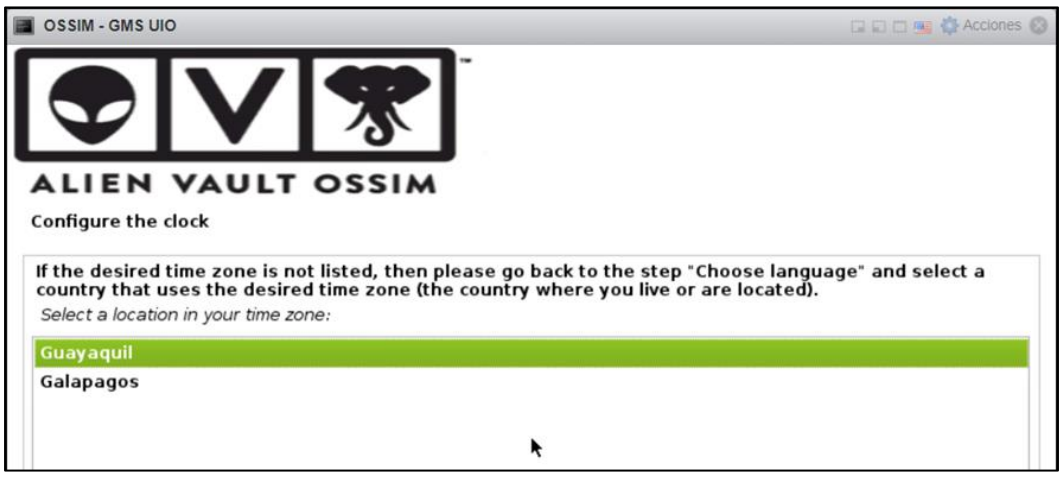


Figura 2.20. Configuración de zona horaria

Una vez que se terminó de establecer los parámetros requeridos por OSSIM, la instalación comenzó como se muestra en Figura 2.21.

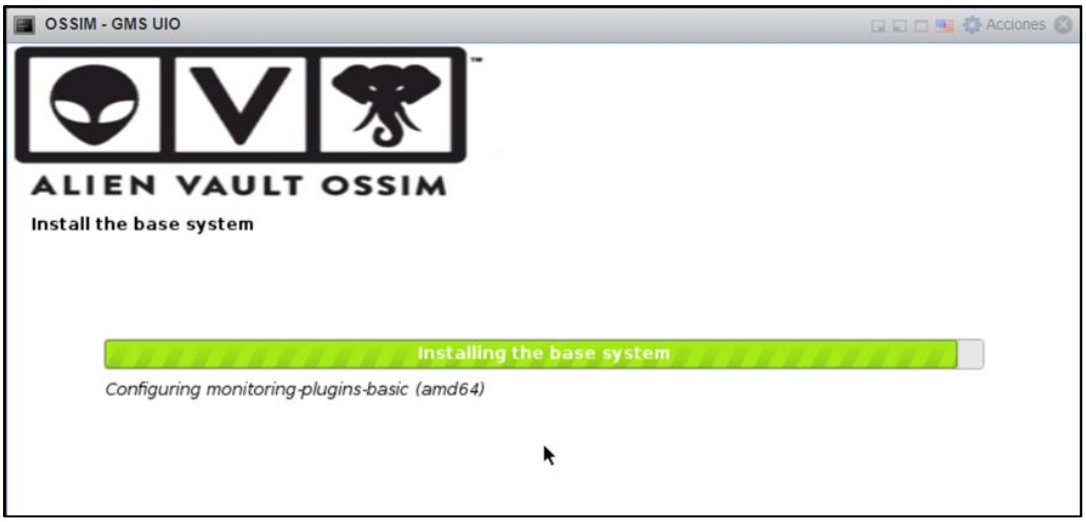


Figura 2.21. Instalación OSSIM

2.5.2.5 Acceso a OSSIM

Una vez que finalizó la instalación, se accedió a la plataforma OSSIM mediante un navegador web a la dirección asignada anteriormente, utilizando el protocolo https. La URL de acceso es la https://192.168.2.3

Después de solicitar las credenciales de acceso web, se muestra un mensaje de bienvenida como se indica en la Figura 2.22, el cual permite realizar la integración de activos al monitoreo de una manera guiada.

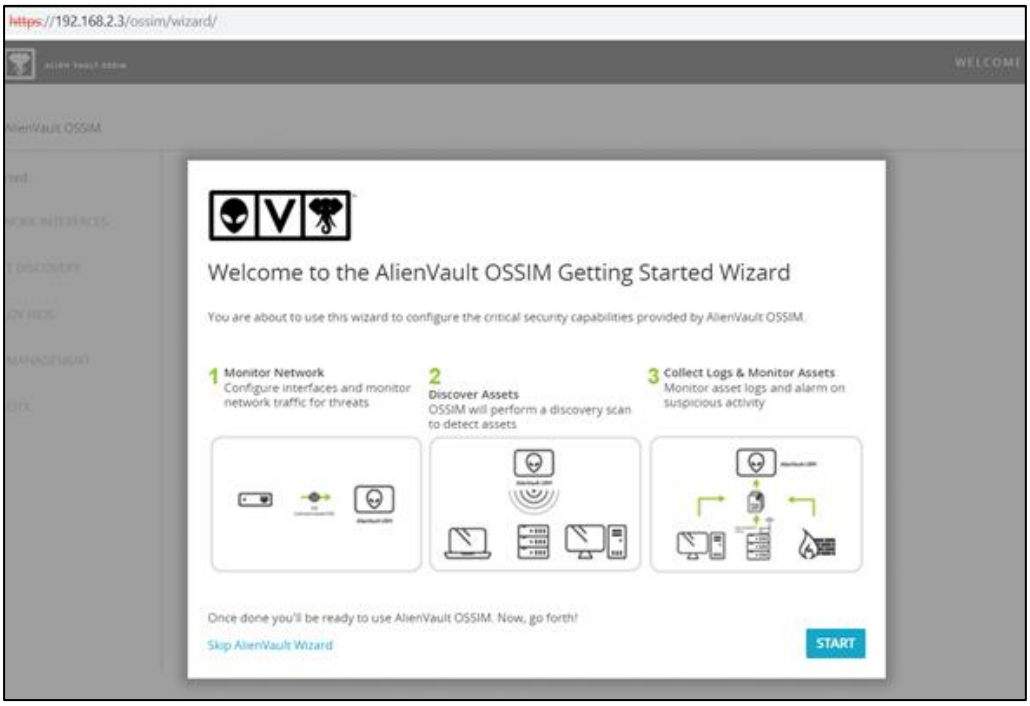


Figura 2.22. Pantalla inicial de OSSIM

2.5.3 INTEGRACIÓN DE ACTIVOS A MONITOREAR

Como se mencionó en 2.3, para realizar el monitoreo de equipos Windows o Linux, es necesario la instalación de un agente OSSEC. Para los equipos perimetrales como firewall, switch, router, etc. Se debe configurar el envío de logs a un servidor remoto utilizando el protocolo syslog UDP/514.

OSSIM necesita tener un inventario de activos a monitorear para la generación de los respectivos agentes Windows y Linux, así como la habilitación de plugins respectivos para la normalización de logs.

El inventario de activos se lo puede encontrar en la parte de ENVIRONMENT > ASSETS & GROUPS como se muestra en la Figura 2.23.

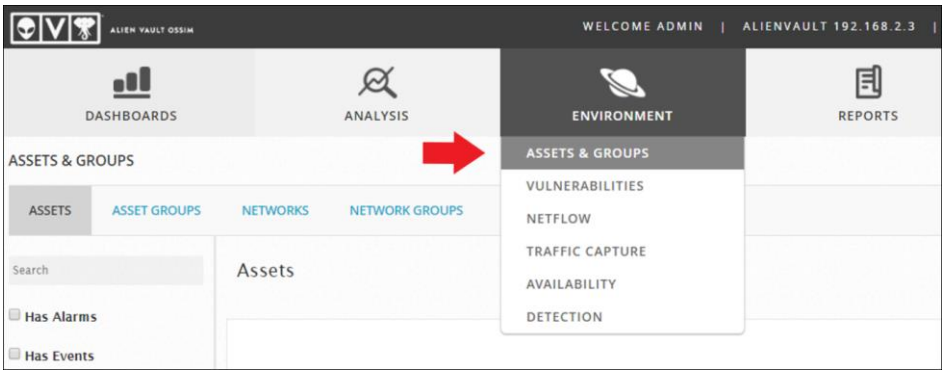


Figura 2.23. Assets & Groups

Para añadir los activos se debe dirigir a la parte de ADD ASSETS, en esta parte se pude elegir entre añadir un activo manualmente, subir un listado de activos mediante un archivo CSV, agregar activos que estén relacionados a eventos presentes en los Eventos SIEM o realizar un escaneo de activos.

Una vez seleccionada la opción, se desplegará los campos necesarios para el ingreso del nuevo activo de monitoreo como se ve en la Figura 2.24.

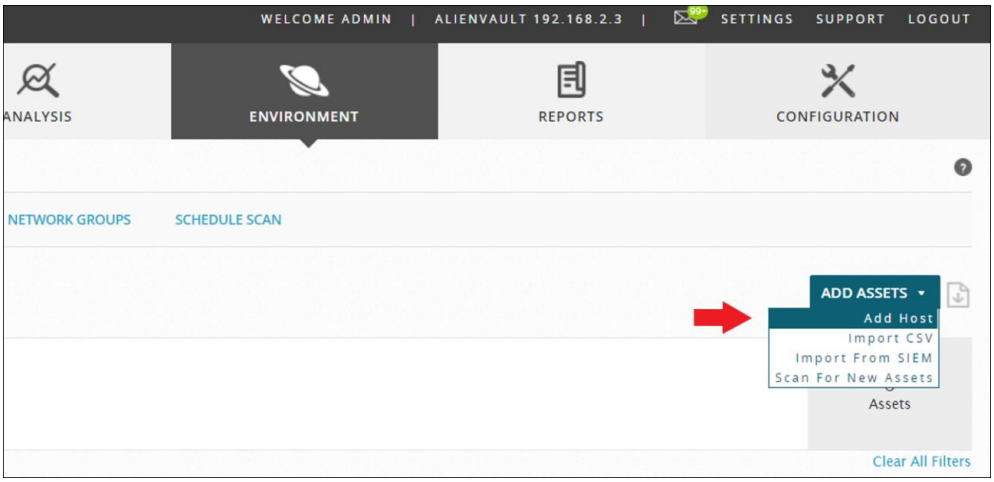


Figura 2.24. Adición de activo al inventario de OSSIM

2.5.3.1 Equipos Windows

Para el monitoreo del activo correspondiente al Active Directory (192.168.2.7), se procedió a añadir el activo al inventario de OSSIM como se muestra la Figura 2.25.

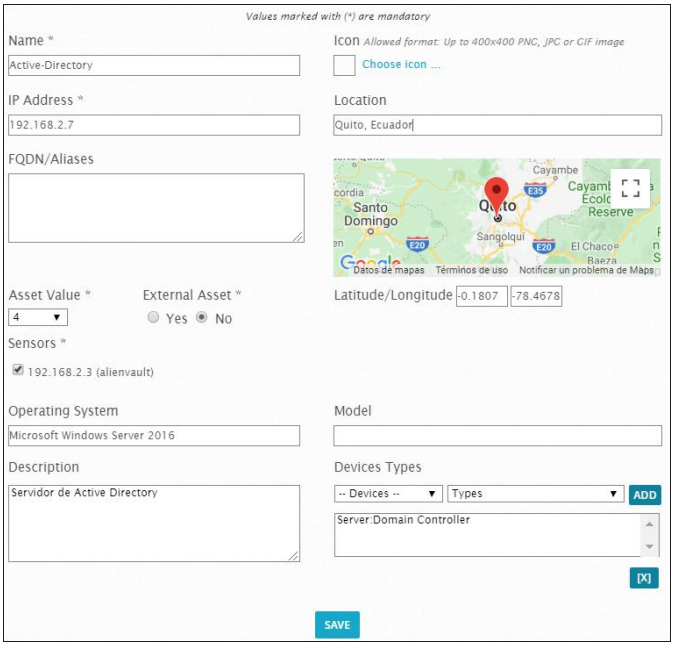


Figura 2.25. Adición de Activo Active Directory

Una vez que el activo se ha añadido al inventario, se debe dirigir a la sección ENVIRONMENT > DETECTION, como se indica en la Figura 2.26

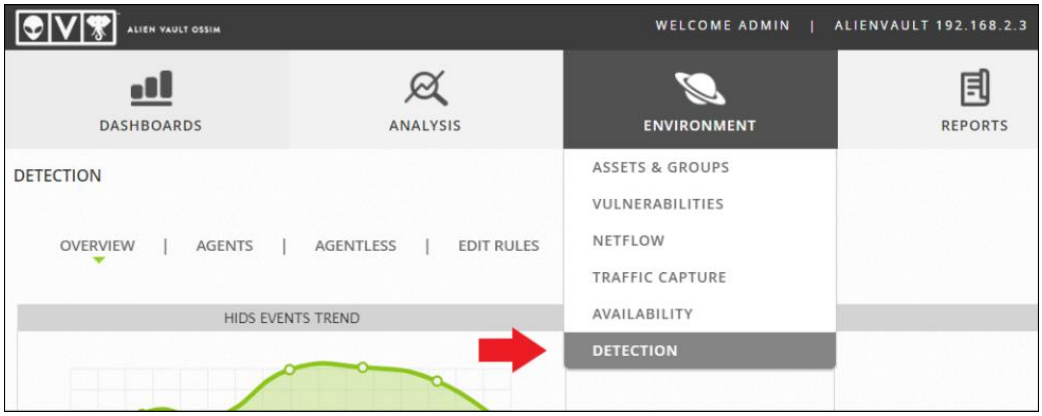


Figura 2.26. Sección Detection - OSSIM

Después, se debe seleccionar la opción de AGENTS y dar clic en la opción ADD AGENT como se indica en la Figura 2.27

Luego, mostrará la opción para la creación del nuevo agente OSSEC, en donde se especificó el activo del cual se requiere crear el agente y campos requeridos como el nombre del agente y si la dirección IP asignada es estática o dinámica como se observa en la Figura 2.28

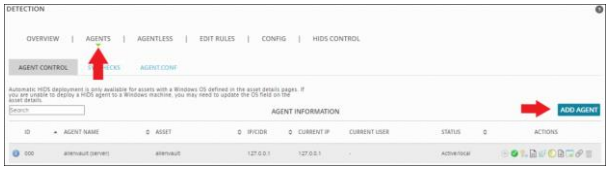


Figura 2.27. Creación de agente OSSEC - Windows

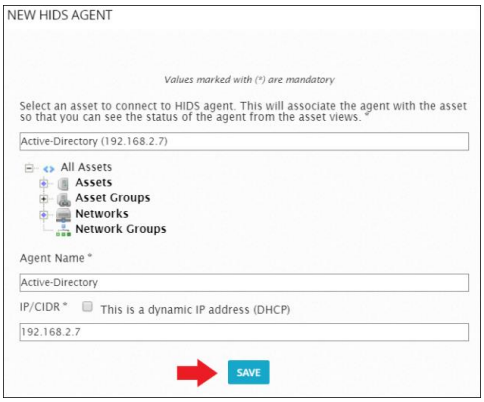


Figura 2.28. Parámetro del agente OSSEC - Windows

Una vez que se finalizó la creación del agente, podremos encontrarlo en el listado de agentes como se muestra en la Figura 2.29. Listado de agentes OSSEC disponiblesFigura 2.29

En las acciones que tenemos disponibles para el agente OSSEC está la de descarga del agente preconfigurado para equipos Windows como se indica en la Figura 2.30

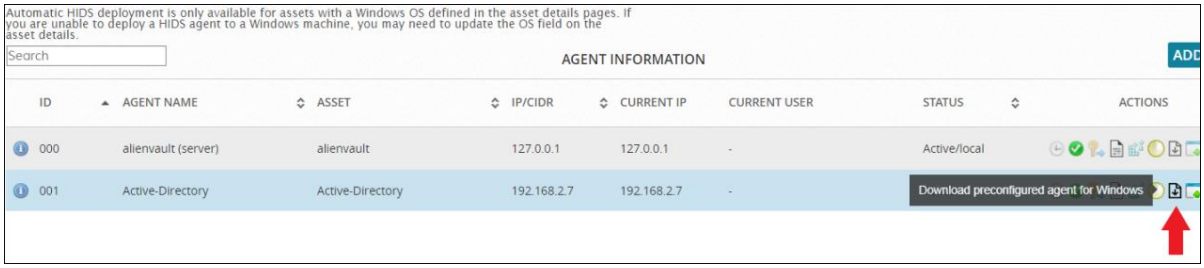


Figura 2.29. Listado de agentes OSSEC disponibles

Se procedió con la descarga del agente OSSEC para el activo 192.168.2.7, el cual generó un archivo .exe como se indica en la Figura 2.30

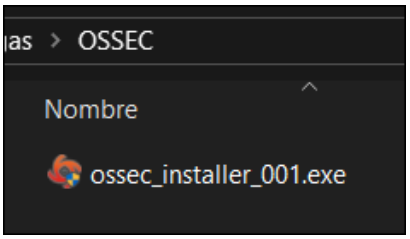


Figura 2.30. Agente OSSEC descargado

A continuación, este agente OSSEC se lo instaló en el equipo Active Directory (192.168.2.7) con permisos de administrador como se puede ver en Figura 2.31

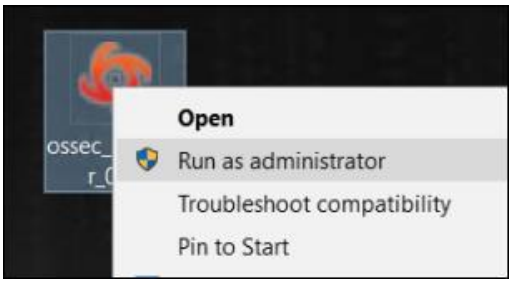


Figura 2.31. Instalación de agente OSSEC en Active Directory

Se validó que el agente se encuentre en ejecución como se ve en la Figura 2.32

Adicionalmente, se verificó que haya comunicación entre el agente OSSEC y el equipo OSSIM. Como se aprecia en la Figura 2.33, se puede ver que el tráfico se encuentra cifrado.

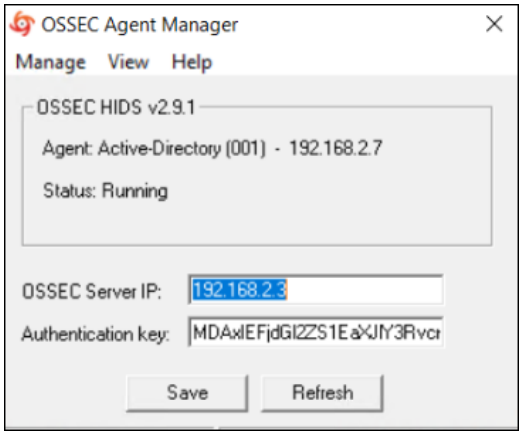


Figura 2.32. Verificación de ejecución de agente OSSEC en Active Directory

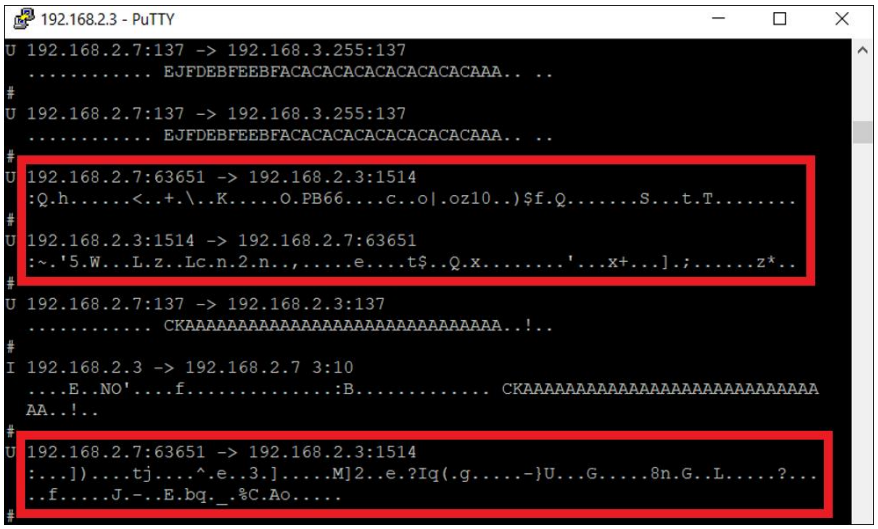


Figura 2.33. Verificación de comunicación de agente OSSEC

Finalizada la conexión, el agente cambia a estado de activo como se puede ver en la Figura 2.34.

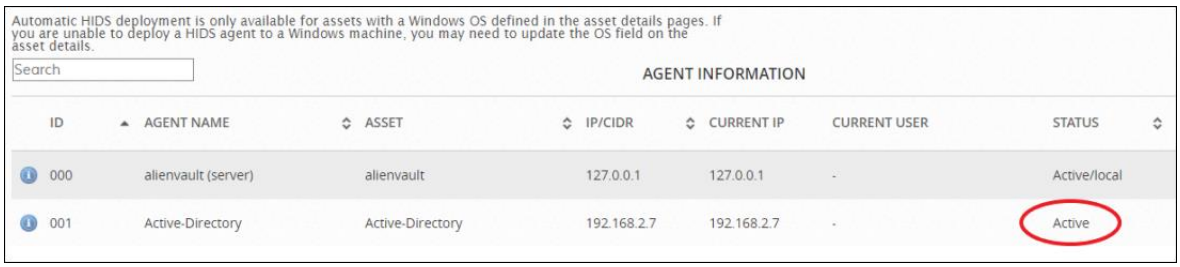


Figura 2.34. Agente OSSEC en estado Activo

Los eventos que se encuentra enviando el agente OSSEC del equipo 192.168.2.7 se los puede visualizar en la sección ANALYSIS -> SECURITY EVENTS (SIEM) como se lo puede ver en la Figura 2.35.

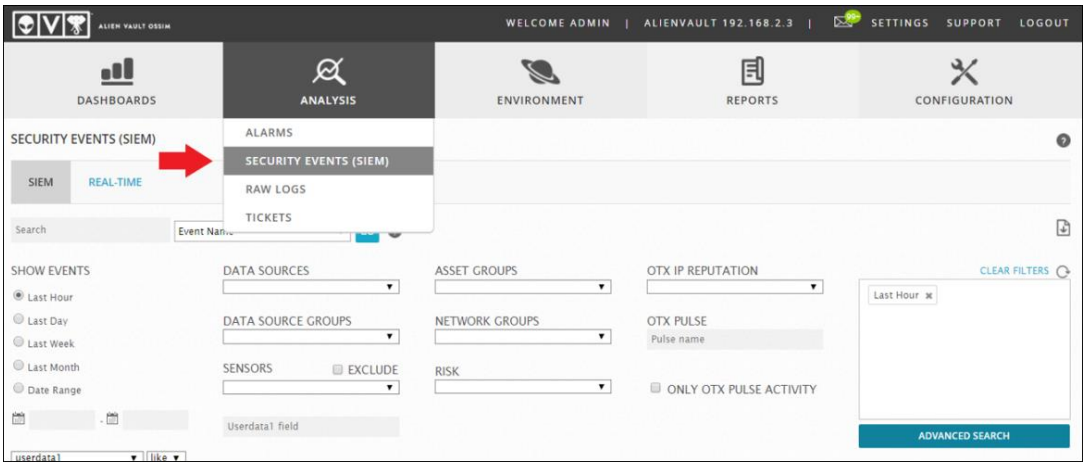


Figura 2.35. Sección Security Events (SIEM)

En esta sección se pueden visualizar todos los logs que se han normalizado a través de los plugins que OSSIM tiene activados por defecto o los que se activaron manualmente. Para el caso de agentes OSSEC, el plugin activado por defecto es el “AlienVault HIDS”.

Se realizó un filtro para visualizar los eventos del Active Directory. Se seleccionó como DATA SOURCES el plugin de OSSEC (AlienVault HIDS) y se estableció como dirección IP fuente (Scr IP) la 192.168.2.7, como se muestra en la Figura 2.36.

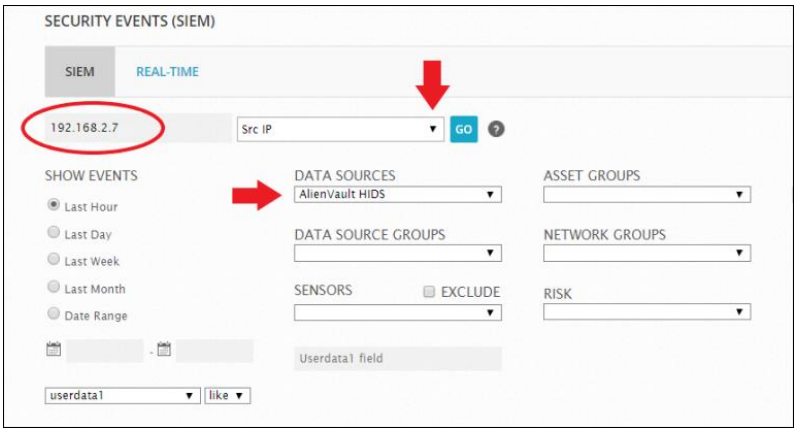


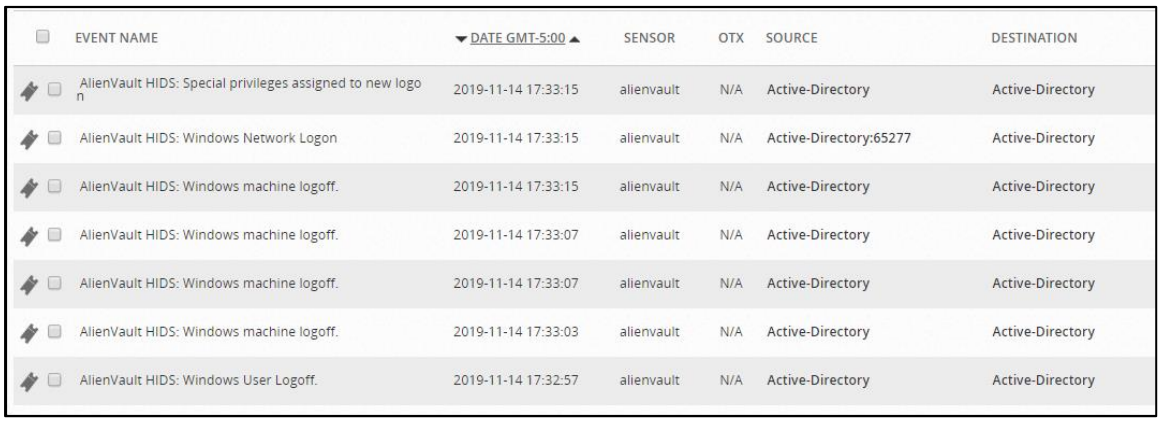
Figura 2.36. Filtro para validar eventos

En la sección mostrada se encuentran todos los eventos que OSSIM reconoció mediante el plugin AlienVault HIDS del Active Directory como se indica en la Figura 2.37.

2.5.3.2 Equipos Linux

Los equipos Linux a monitorear son los siguientes:

- Servidor de Archivos MicroDM - 192.168.2.13
- Central telefonica - 10.0.9.2



EVENT NAME	DATE GMT-5:00	SENSOR	OTX	SOURCE	DESTINATION
AlienVault HIDS: Special privileges assigned to new logo n	2019-11-14 17:33:15	alienvault	N/A	Active-Directory	Active-Directory
AlienVault HIDS: Windows Network Logon	2019-11-14 17:33:15	alienvault	N/A	Active-Directory:65277	Active-Directory
AlienVault HIDS: Windows machine logoff.	2019-11-14 17:33:15	alienvault	N/A	Active-Directory	Active-Directory
AlienVault HIDS: Windows machine logoff.	2019-11-14 17:33:07	alienvault	N/A	Active-Directory	Active-Directory
AlienVault HIDS: Windows machine logoff.	2019-11-14 17:33:07	alienvault	N/A	Active-Directory	Active-Directory
AlienVault HIDS: Windows machine logoff.	2019-11-14 17:33:03	alienvault	N/A	Active-Directory	Active-Directory
AlienVault HIDS: Windows User Logoff.	2019-11-14 17:32:57	alienvault	N/A	Active-Directory	Active-Directory

Figura 2.37. Eventos de Active Directory

El procedimiento que se siguió es similar al utilizado en 2.5.3.1 para la integración del equipo Windows hasta la parte de generación del agente OSSEC. OSSIM no permite la descarga de un agente preconfigurado para sistemas Linux [15]. El agente se lo debe descargar desde la página https://github.com/ossec/ossec-hids/releases

Una vez que se añadió el agente OSSEC de Linux como se muestra en la Figura 2.38, este aparecerá como desconectado en el listado de agentes y con la opción de descarga de agente preconfigurado bloqueada como se puede ver en la Figura 2.39

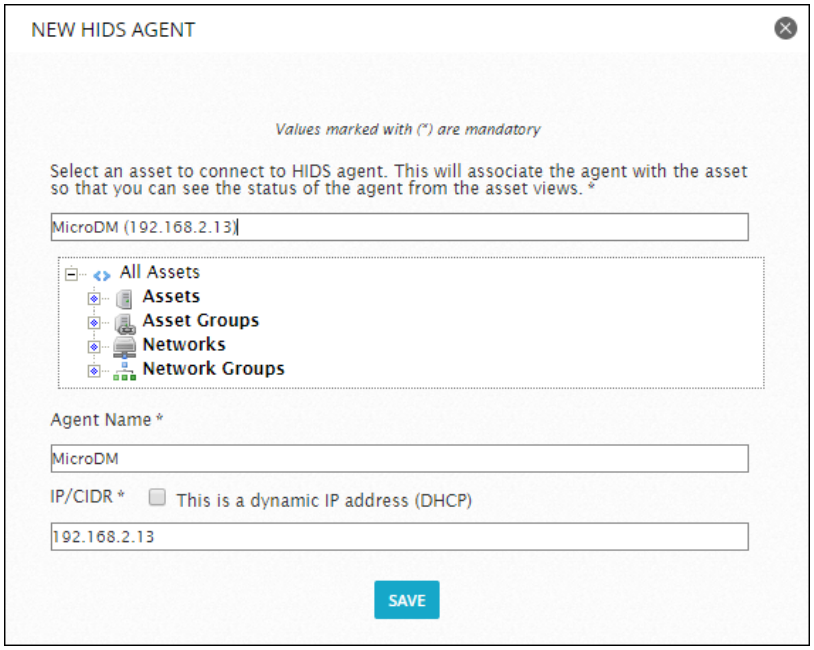


Figura 2.38. Parámetro del agente OSSEC - Linux

Figura 2.39. Agente Linux Desconectado

Para la comunicación entre el agente Linux y OSSIM, es necesario configurar el agente OSSEC con la llave que generó OSSIM como se muestra en la Figura 2.40

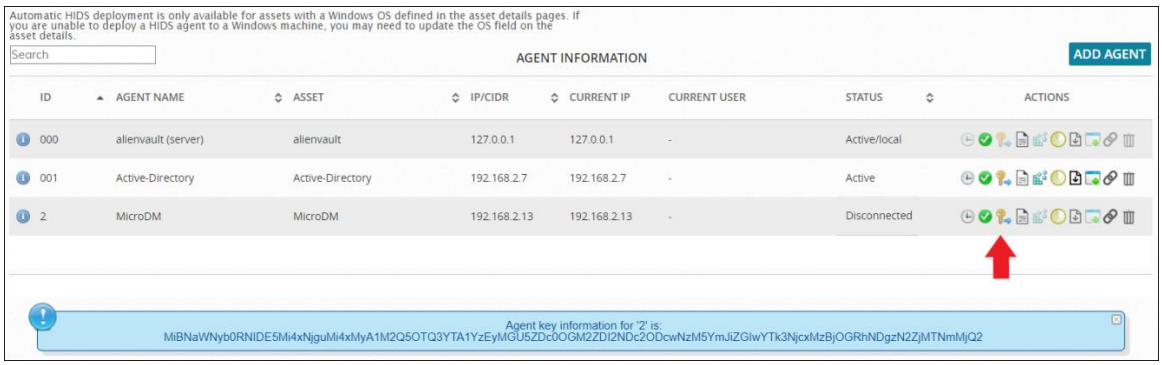


Figura 2.40. Llave de agente Linux

En el equipo Linux se realizó la descarga del agente OSSEC con la versión 2.9.1, con la cual es compatible OSSIM como se indica en la Figura 2.41. Se extrajo el contenido del archivo .tar.gz y se ejecutó el script de instalación install.sh.

El proceso de instalación se lo efectúa de una manera guiada. La primera pantalla que se muestra permite elegir el idioma en el que se mostrarán las opciones de instalación. En este caso el idioma por defecto es el inglés como se puede ver en la Figura 2.42

Figura 2.41. Descarga de agente OSSEC Linux

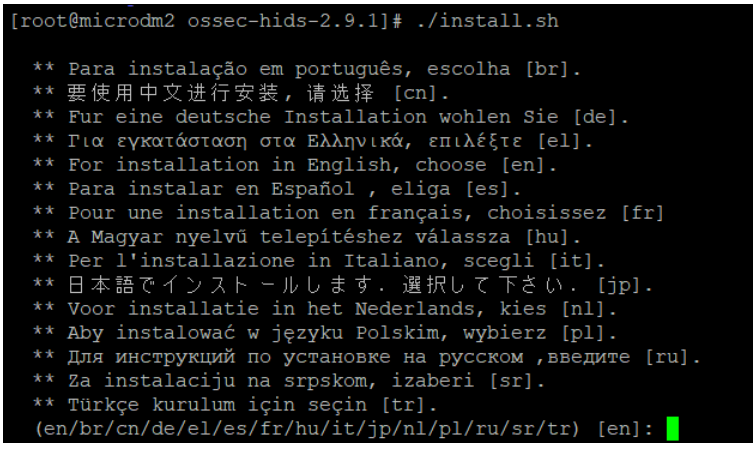


Figura 2.42. Inicio de instalación del agente OSSEC en Linux

A continuación, se informa al usuario las características del equipo como tipo de sistema, tipo de usuario y el host como se puede ver en la Figura 2.43 y se pide para continuar con la instalación presionar la tecla enter.

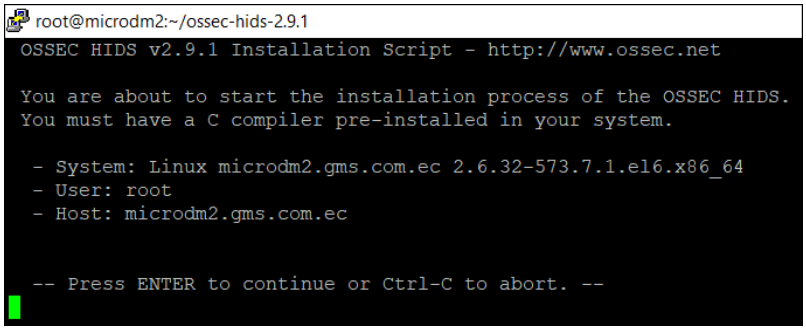


Figura 2.43. Datos del sistema

Después de presionar la tecla enter, se pide al usuario parámetros de instalación como tipo de instalación (en este caso se escoge agente), ruta de instalación (/var/ossec/), dirección IP del servidor OSSIM (192.168.2.3) y la habilitación de servicios adicionales que ofrece OSSEC como se indica en la Figura 2.44

El agente OSSEC presenta a continuación, los archivos de logs de los cuales obtendrá la información a enviar a OSSIM, éstas por defecto son:

- /var/log/messages
- /var/log/secure
- /var/log/maillog
- /var/log/httpd/error_log
- /var/log/httpd/Access_log

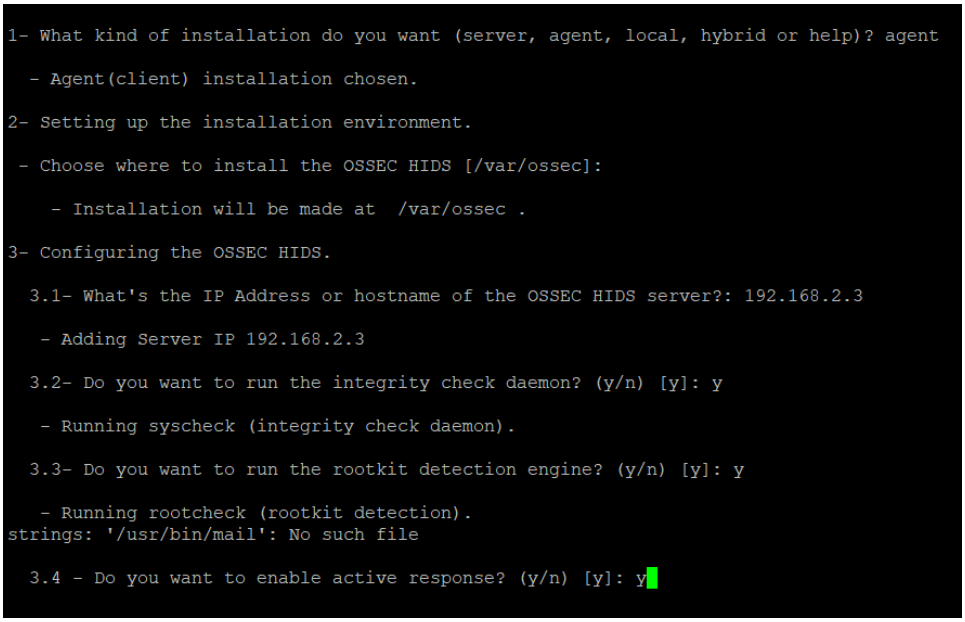


Figura 2.44. Configuración agente OSSEC - Linux

Se tiene la opción de indicarle al agente OSSEC rutas adicionales de las cuales obtener la información, realizando la modificación del archivo de configuración respectivo como se indica en la Figura 2.45.

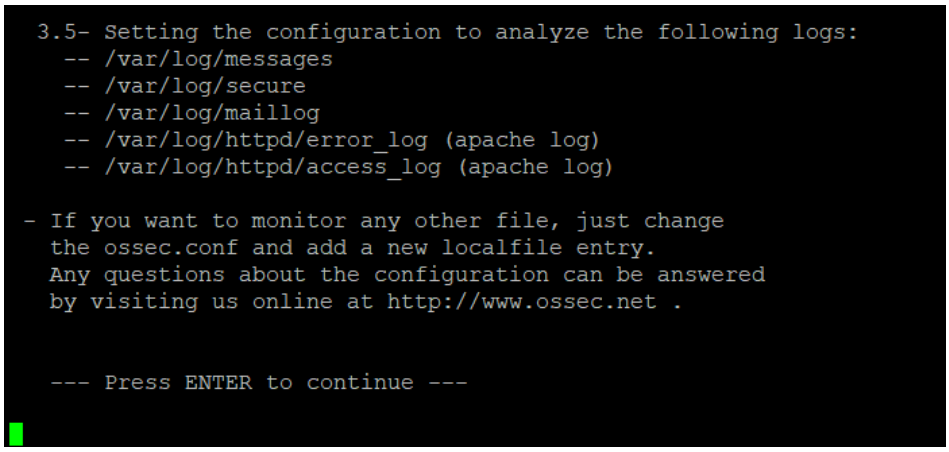


Figura 2.45. Rutas de logs por defecto OSSEC

Una vez que la instalación concluyó, se presenta los comandos para el inicio del agente OSSEC como se indica en la Figura 2.46

Antes de iniciar el agente, se debe añadir la llave generada previamente en la plataforma OSSIM. Para esto se dirigió a la ruta /var/ossec/bin y se ejecutó el script “manage_agents”, el cual permitió permite importar la llave del agente respectivo como se puede ver en la Figura 2.47

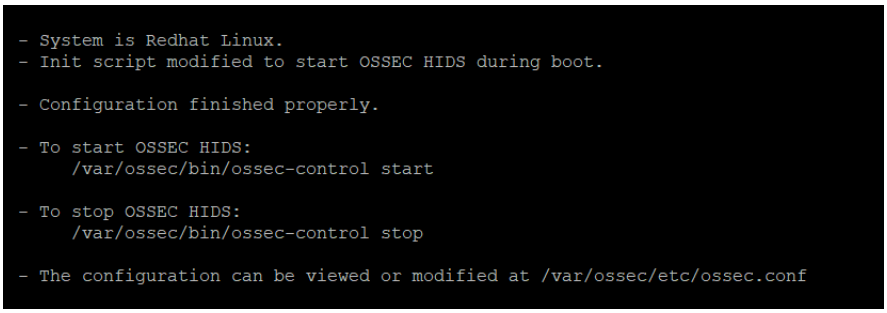


Figura 2.46. Comandos del agente OSSEC - Linux

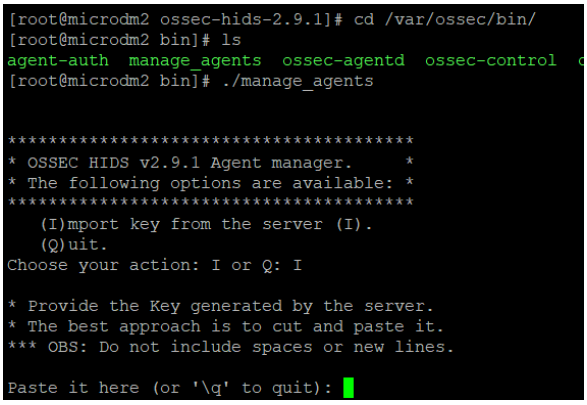


Figura 2.47. Importar llave OSSEC

Una vez seleccionada la opción de importar una llave desde el servidor (I) y se copió la llave que se mostró desde OSSIM en la web. Se mostró en pantalla la información del agente a la cual corresponde la llave introducida y se verificó que corresponda al equipo instalado como se ve en la Figura 2.48. Una vez que se realizó la configuración del agente OSSEC, se procedió a iniciar el agente como se puede ver en la Figura 2.49.

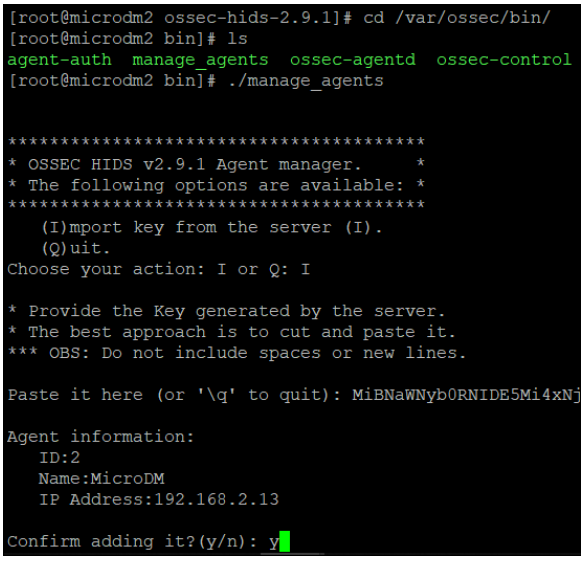


Figura 2.48. Confirmación de OSSEC

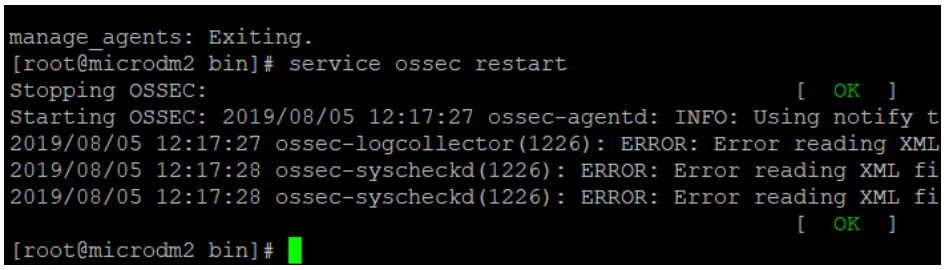


Figura 2.49. Inicio del servicio OSSEC

Finalmente, se valida que el agente OSSEC se encuentre activado como se indica en la Figura 2.50 y se comprueba la recepción de eventos como se observa en la Figura 2.51

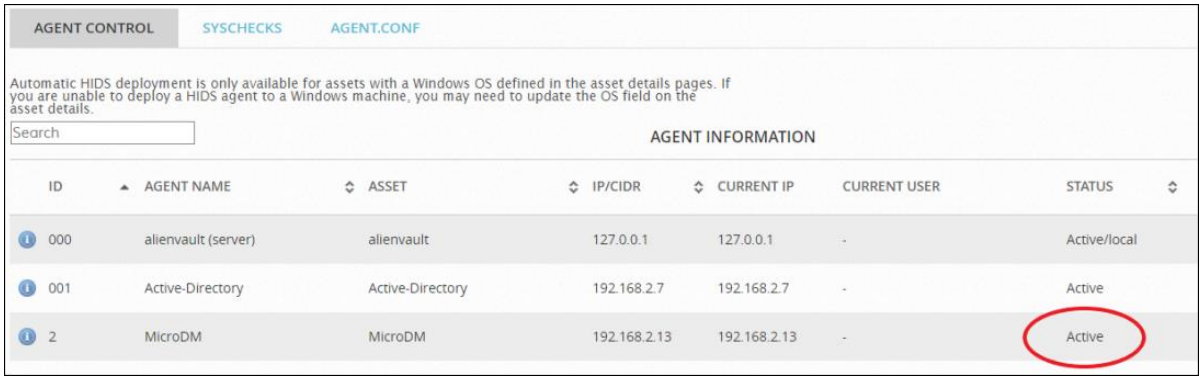


Figura 2.50. Estado Activo del agente OSSEC

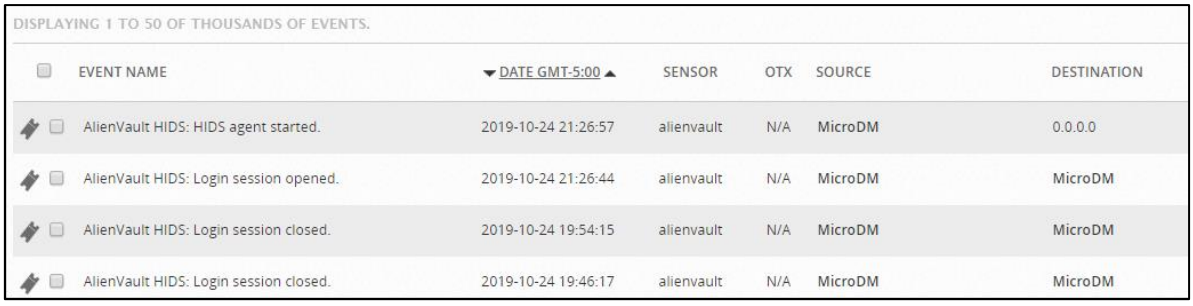


Figura 2.51. Recepción de eventos del agente OSSEC

El proceso descrito se lo replica para la instalación del agente OSSEC en el equipo Linux Central telefonica - 10.0.9.2. Una vez que se instaló el agente OSSEC en el equipo 10.0.9.2, se verificó que el agente se encuentre en estado activado como se indica en la Figura 2.52. Y adicionalmente, se verificó que se tenga recepción de eventos como se muestra en la Figura 2.53.

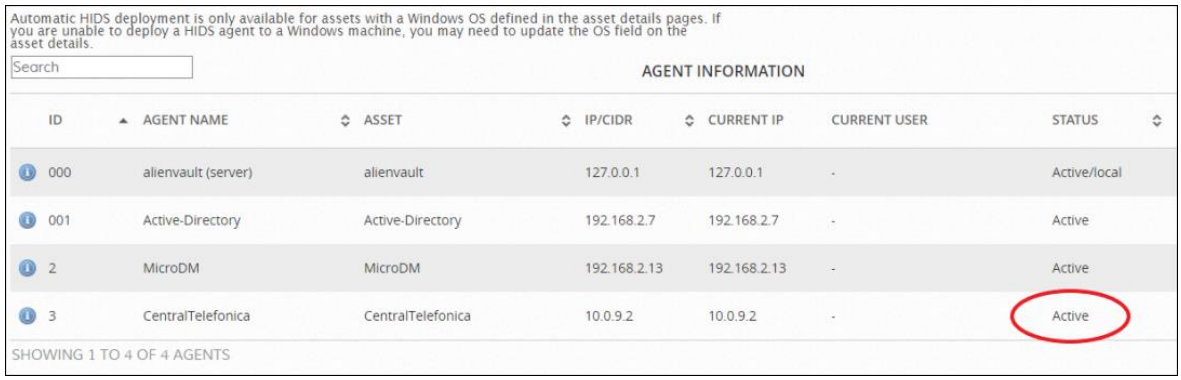


Figura 2.52. Agente OSSEC Central Telefónica

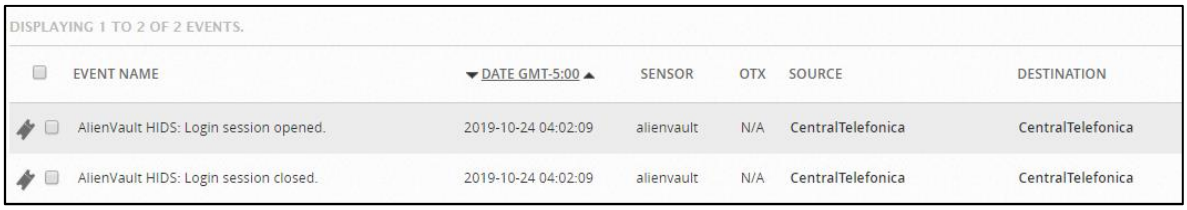


Figura 2.53. Recepción de eventos de la Central Telefónica

2.5.3.3 Equipo Firewall

Para la configuración de envío de logs desde el equipo firewall, se estableció como parámetros la dirección IP del servidor remoto, el puerto utilizado, desde que nivel se deben enviar los logs (Informativo). Como se puede observar en la Figura 2.54

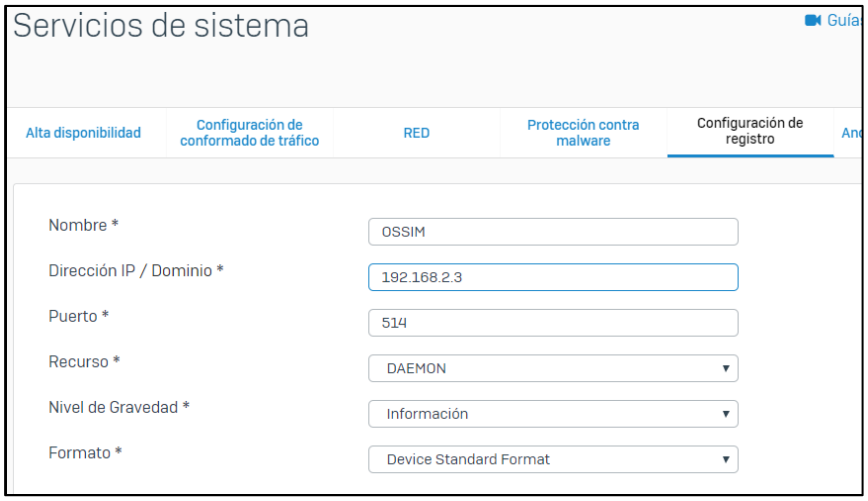


Figura 2.54. Configuración envío de logs - Firewall

Como en el caso de los equipos Linux y Windows, se comenzó con la adición del activo de monitoreo en el inventario de OSSIM como se indica en la Figura 2.55, y este se puede visualizar en el listado como se puede observar en la Figura 2.56.

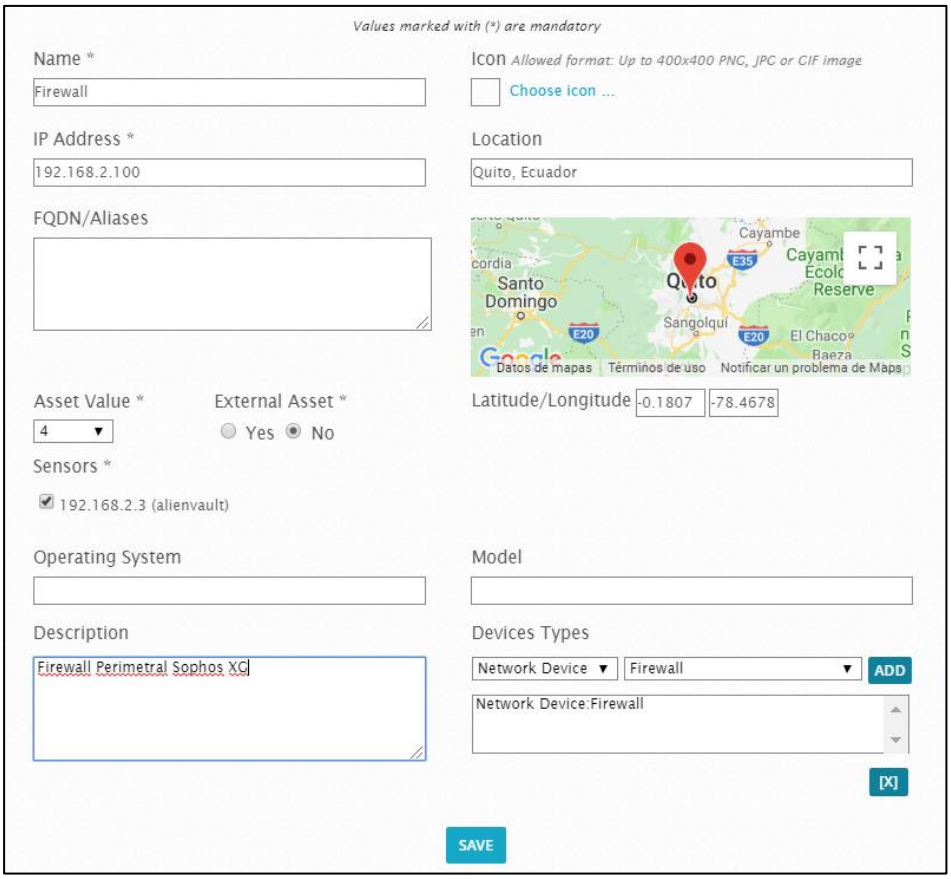


Figura 2.55. Integración del Firewall

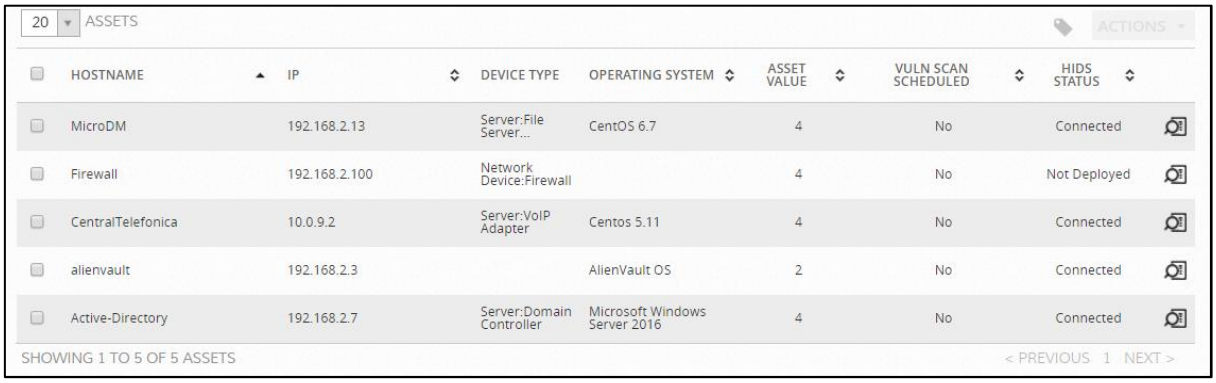


Figura 2.56. Listado de activos

Para la activación del respectivo plugin o para la edición de algún parámetro del activo, se debe dar clic en el ícono con forma de lupa señalado en la Figura 2.57, en la pantalla que se muestra a continuación, se observa toda la información que ha sido configurada en el activo como se ve en la Figura 2.58

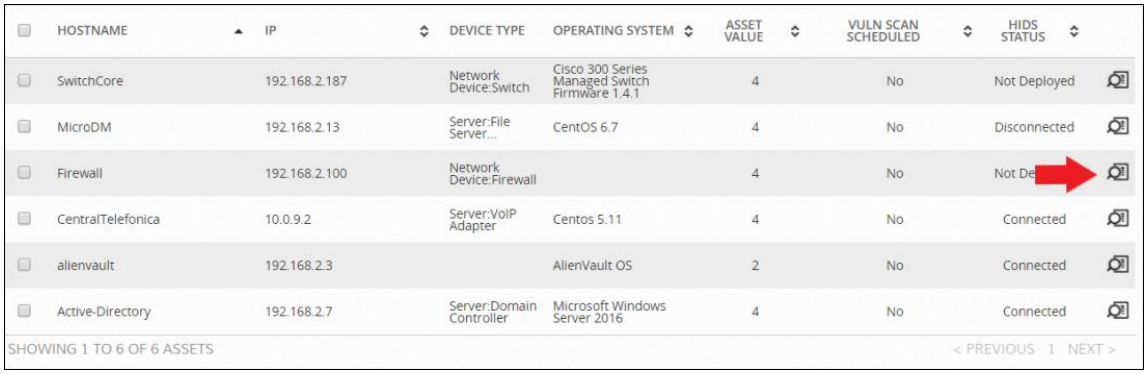


Figura 2.57. Listado de activos - Firewall

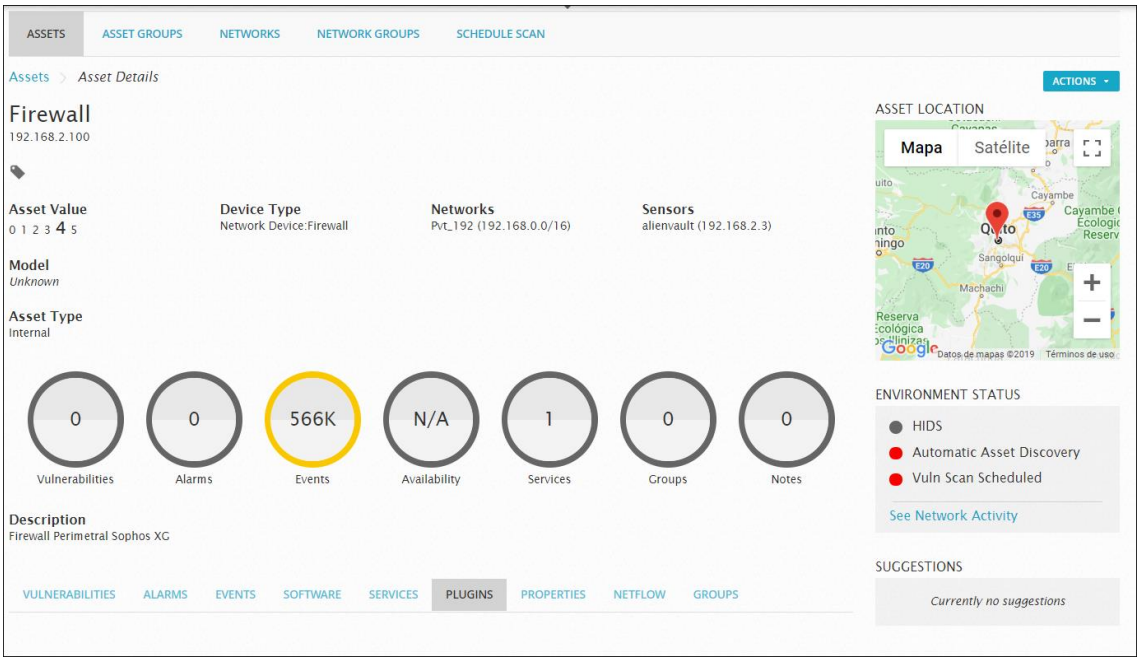


Figura 2.58. Activo Firewall

Para la activación del plugin del firewall Sophos, hay que dirigirse al apartado de PLUGINS y seleccionar EDIT PLUGINS como se ve en la Figura 2.59, A continuación, se despliega una ventana en la que aparecen las marcas compatibles y el modelo de los equipos que son reconocidos. En este caso se selecciona como marca Sophos y el modelo XG como se indica en la Figura 2.60.

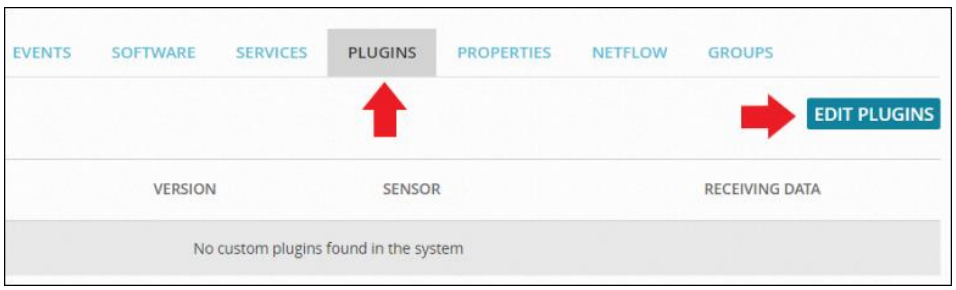


Figura 2.59. Opción para la selección de Plugin

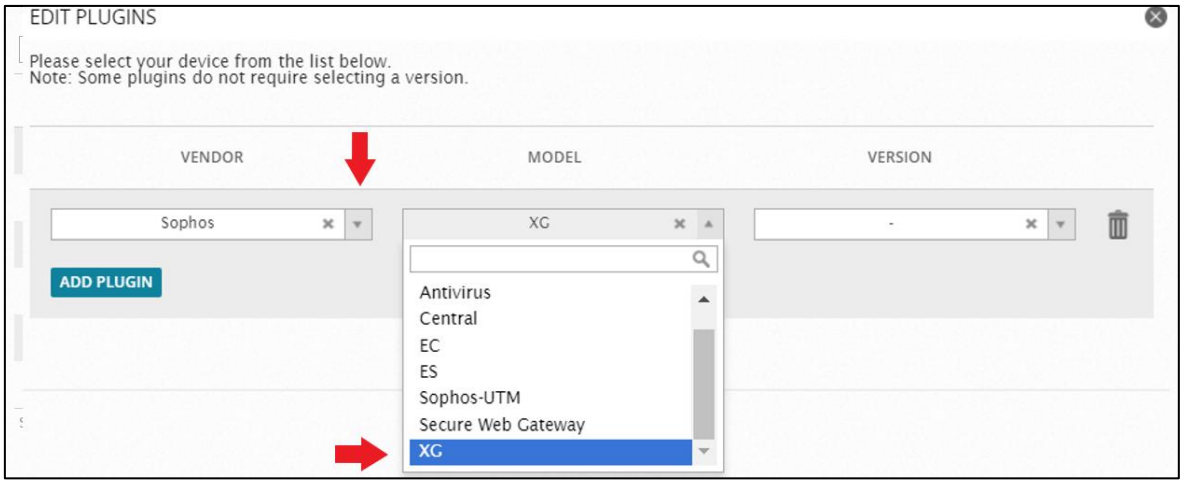


Figura 2.60. Selección de plugin Sophos XG

Se verifica la recepción de eventos como se indica en la Figura X. En DATA SOURCES basta con seleccionar el Sophos

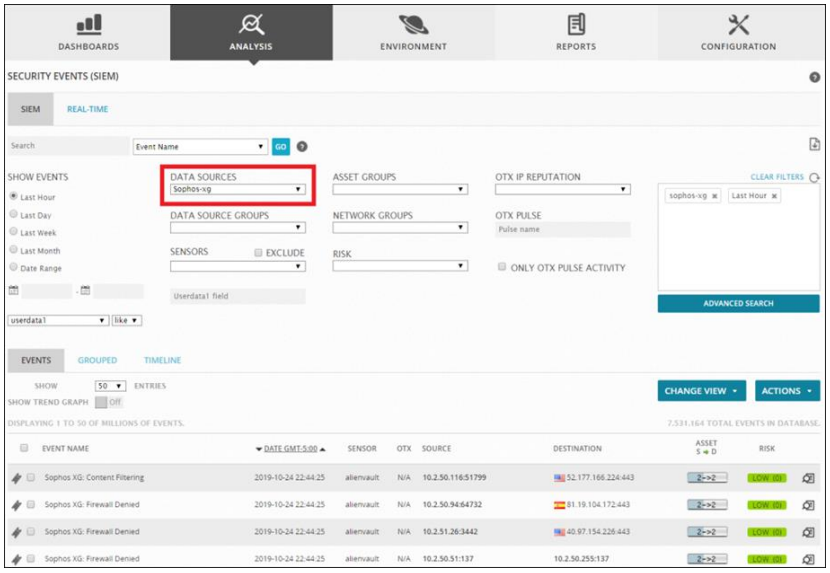


Figura 2.61. Verificación de eventos de Firewall Sophos XG

2.5.3.4 Equipo Virtualizador VMware

La configuración de envío de logs para VMware ESXi 5.1, se la hace siguiendo las especificaciones del protocolo syslog (UDP/514) como se observa en la Figura 2.62 y adicionalmente, se debe configurar el firewall que tiene por defecto VMware para habilitar los permisos necesarios del protocolo syslog como se indica en la Figura 2.63. Configuración firewall syslog

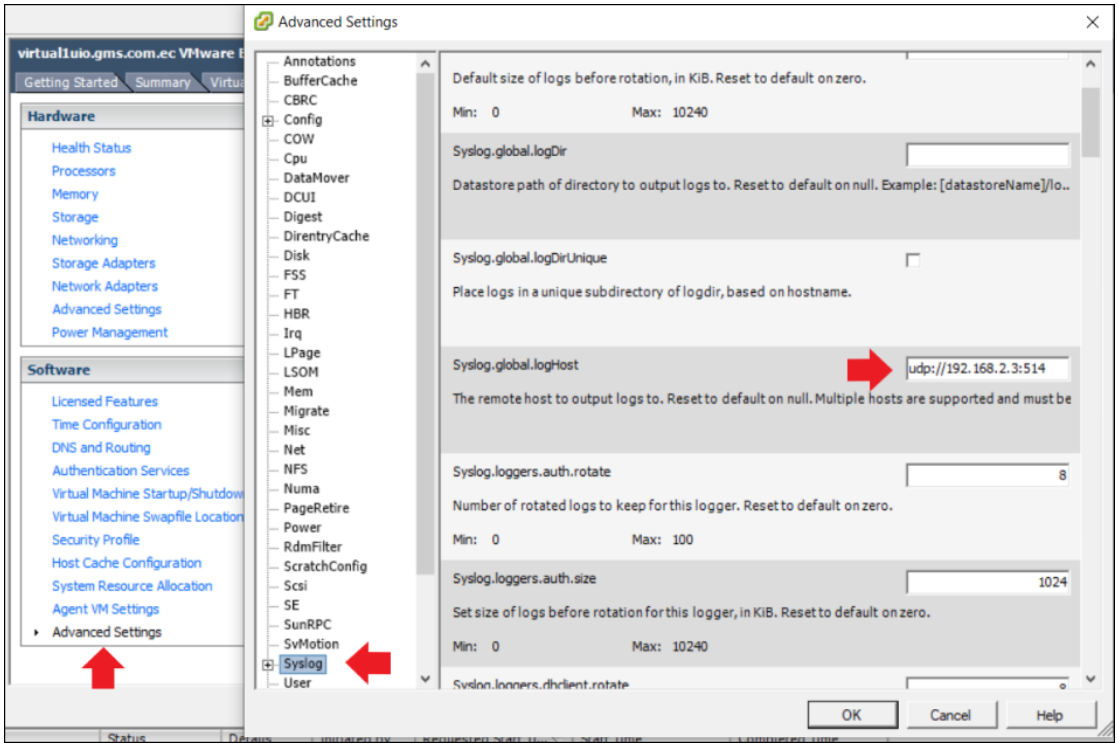


Figura 2.62. Configuración de envío de logs desde VMware

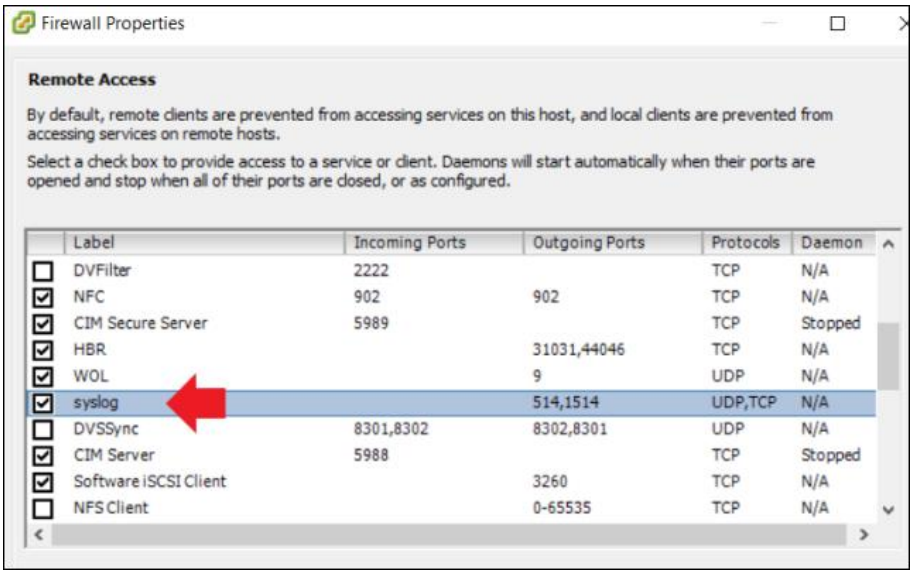


Figura 2.63. Configuración firewall syslog

Se agrega el activo al listado de OSSIM como se observa en la Figura 2.64 y se activa el plugin VMware, ya que es el que tiene compatibilidad con los logs generados para las plataformas VMware ESXi como se indica en la Figura 2.65.

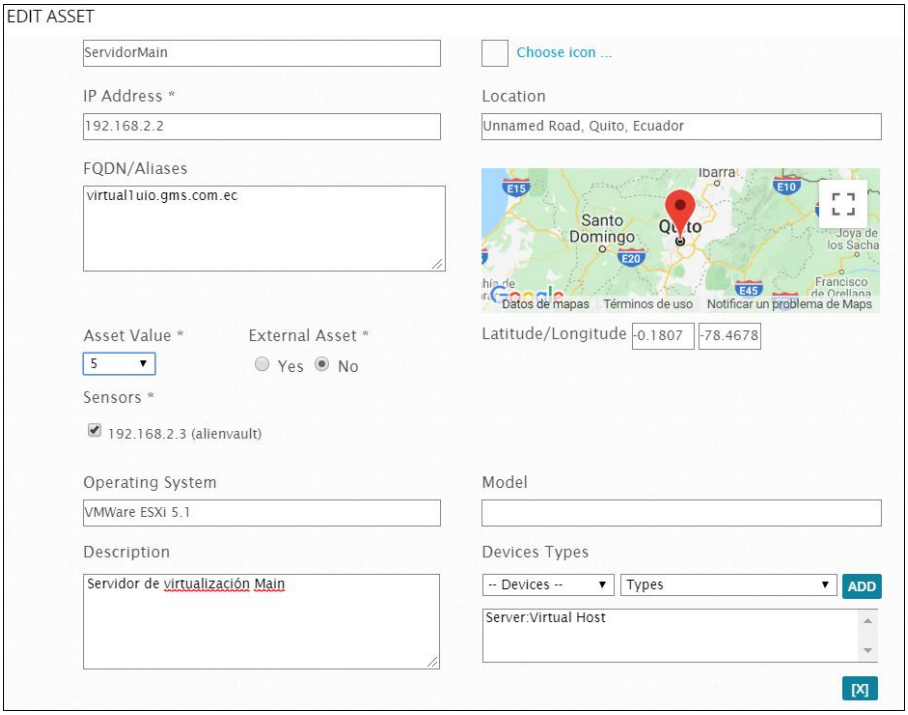


Figura 2.64. Adición de VMware al listado de OSSIM

Figura 2.65. Selección de Plugin Cisco Router

Se verificó la recepción de eventos como se indica en la Figura 2.66

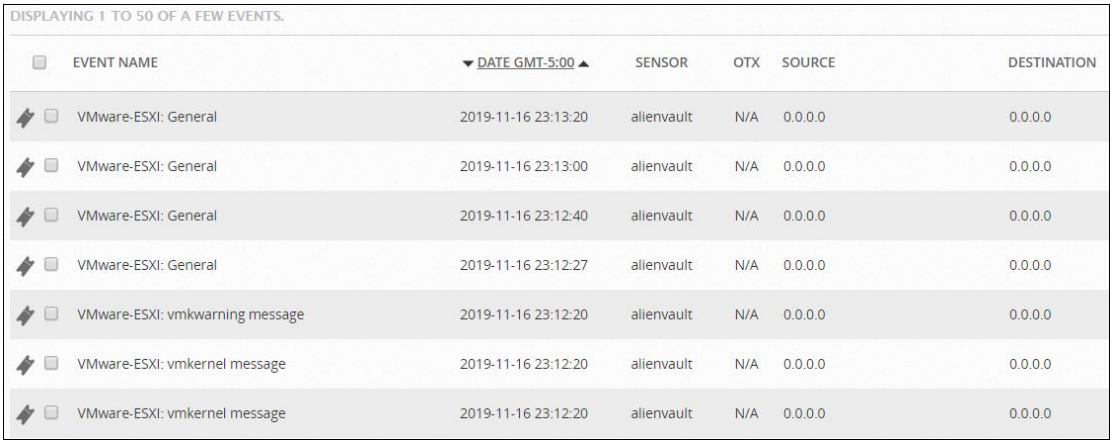


Figura 2.66. Recepción de eventos VMware

2.5.4 ACTIVACIÓN DEL ANALIZADOR DE RED

Una de las características adicionales con la que cuenta OSSIM es el analizador de tráfico de red, este permite detectar anomalías presentes en la red como escaneo de puertos, ataques de denegación de servicio, mediante el motor de Suricata[1] que trae incorporado.

Para la activación del analizador se realizó la activación del plugin correspondiente a "AlienVault NIDS" [7], ubicado en CONFIGURATION > DEPLOYMENT > COMPONENTS > ALIENVAULT CENTER > CONFIGURATION SENSOR como se indica en la Figura 2.67

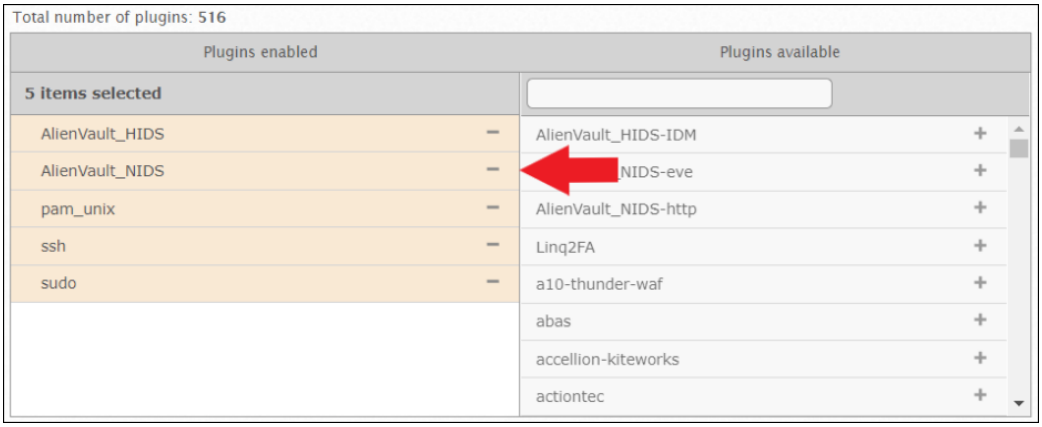


Figura 2.67. Activación de analizador de red

Una vez que se activó el plugin correspondiente, se pudo observar la detección de diferentes anomalías de red como escaneo de puertos, ataques de denegación de servicio.

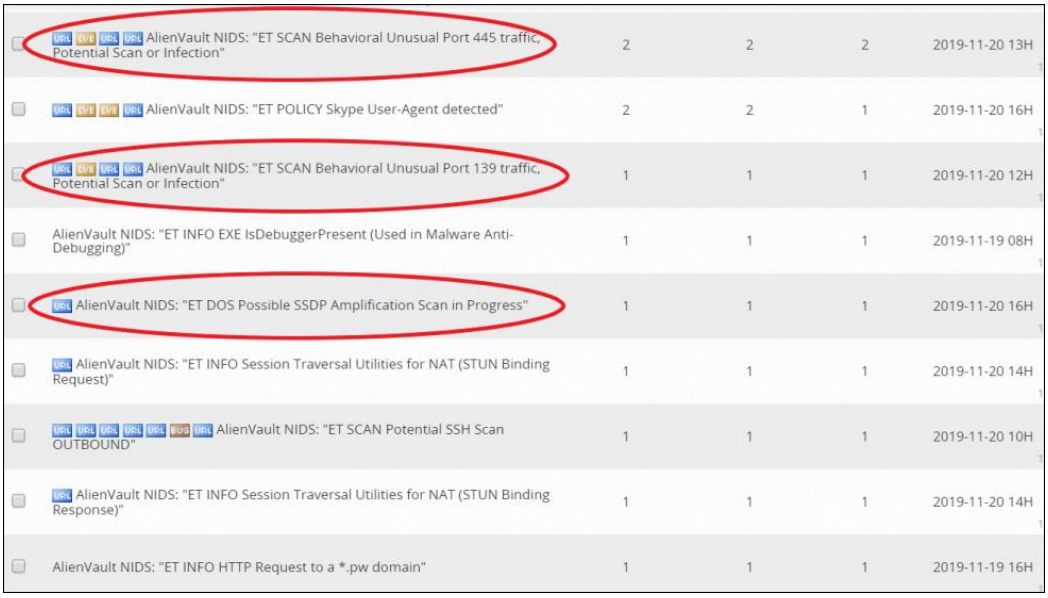


Figura 2.68. Anomalías detectadas por el analizador de red

[1] Suricata: sistema de prevención de intrusos de código abierto

2.6 RECEPCIÓN DE LOGS ESPECÍFICOS DE MONITOREO

Para la generación de las directivas, es necesario conocer los eventos que las van a disparar. Para esto, se realizaron pruebas para determinar los eventos que recolecta OSSIM.

2.6.1 ACCESOS FALLIDOS Y EXITOSOS

Se realizaron pruebas introduciendo en los activos credenciales incorrectas, tanto de usuarios registrados como de no registrados.

2.6.1.1 Equipos Windows

Para que el equipo pueda enviar logs de acceso exitosos y fallidos, fue necesario activar la auditoría de Windows y seleccionar que se auditen los eventos de acceso exitosos y fallidos como se indica en la Figura 2.69 y en la Figura 2.70.

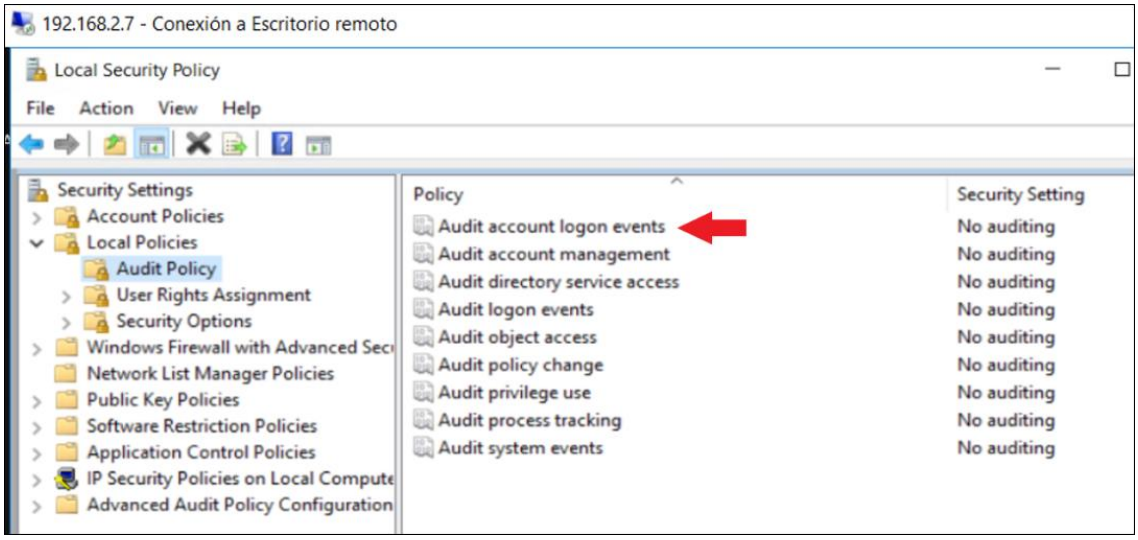


Figura 2.69. Auditoría de eventos de acceso

Con lo realizado anteriormente, se busca obtener los eventos 4624 (Windows successful login event) y 4625 (Windows failed login event).

Adicionalmente, se debe activar los decodificadores necesarios para la detección de los eventos 4624 y 4625 indicados en [15]

Para la activación de los decodificadores necesarios, se debe dirigir a la sección ENVIRONMENT > DETECTION, ingresar al apartado CONFIG y en la pestaña RULES se podrán seleccionar los decodificadores necesarios. En este caso se ha seleccionado el “alienvault-network-login-failure_rules.xml”, como se puede ver en la Figura 2.71 y se procedió con el reinicio del servicio OSSEC como se indica en la Figura 2.72.

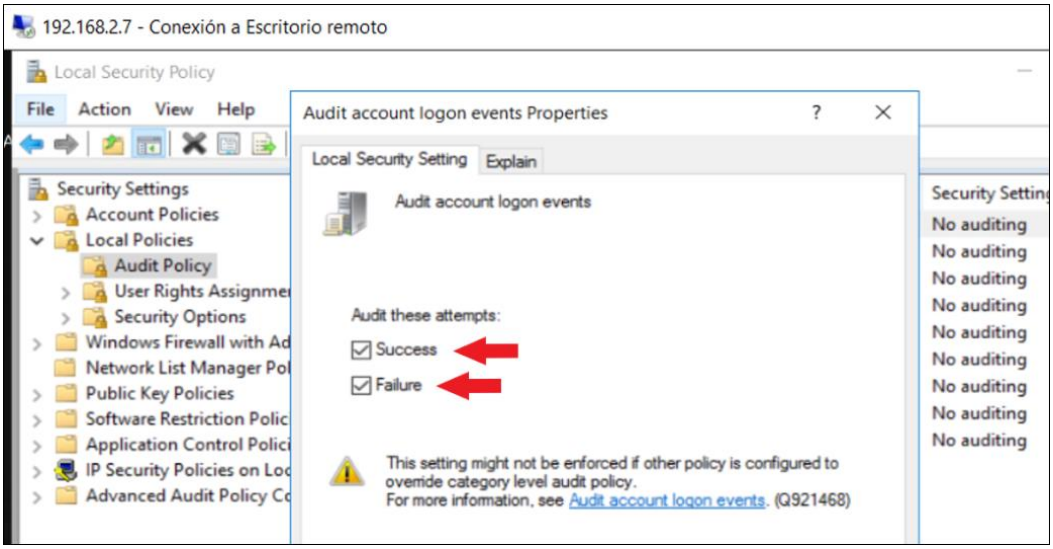


Figura 2.70. Selección de auditoría de accesos exitosos y fallidos

Figura 2.71. Selección del decodificador "alienvault-network-login-failure_rules.xml "

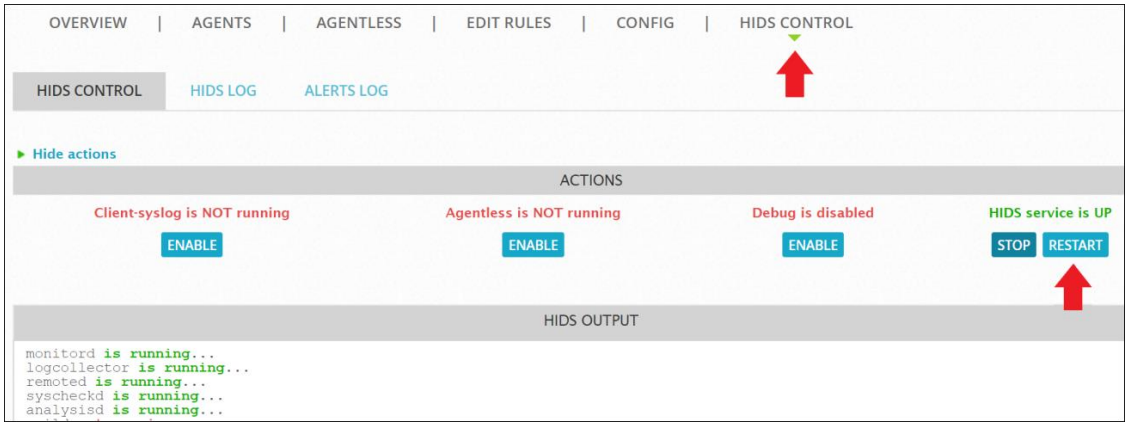


Figura 2.72. Reinicio del servicio OSSEC

2.6.1.1.1 Acceso fallido

Se efectuó un acceso incorrecto de credenciales del usuario “Administrator” como se indica en la Figura 2.73. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. Los campos SOURCE y DESTINATION indican la dirección IP que intentó acceder y la dirección IP del equipo al que se intentó acceder respectivamente.

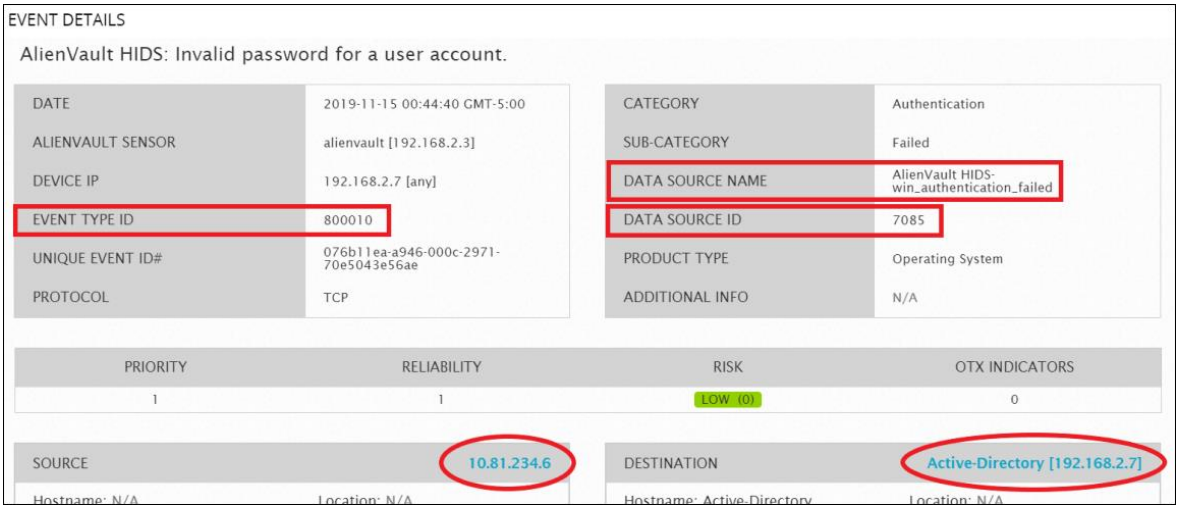


Figura 2.73. Detección de evento de acceso fallido para el usuario Administrator

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.74 se puede ver el nombre del usuario que intentó acceder (Administrator), el ID del evento de Windows (4625), el nombre del equipo que intentó acceder (UIOSOC015A).

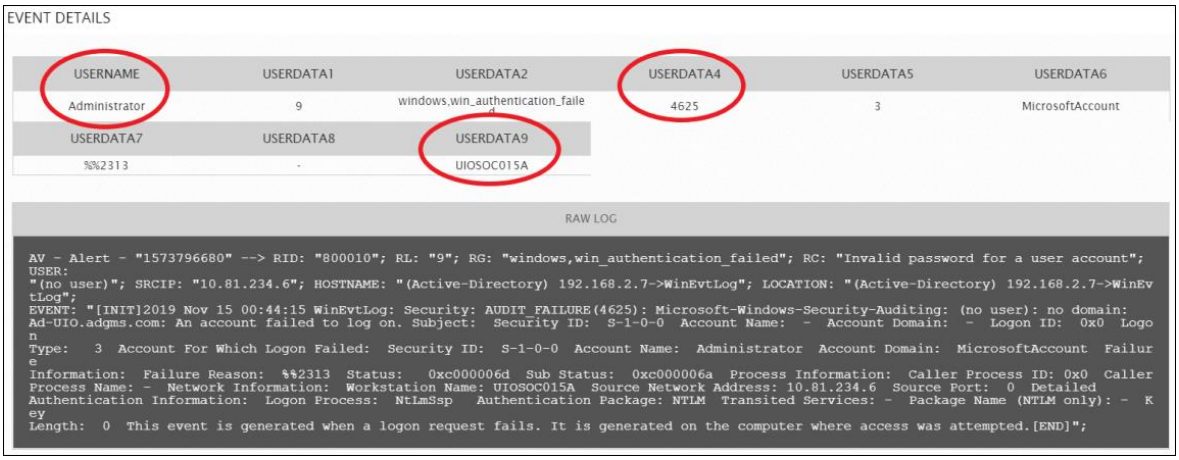


Figura 2.74. Campos adicionales del evento de acceso fallido para el usuario Administrador

Se efectuó un acceso incorrecto de credenciales del usuario no registrado “Prueba” como se indica en la Figura 2.75. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. Los campos SOURCE y DESTINATION indican la dirección IP que intentó acceder y la dirección IP del equipo al que se intentó acceder respectivamente.

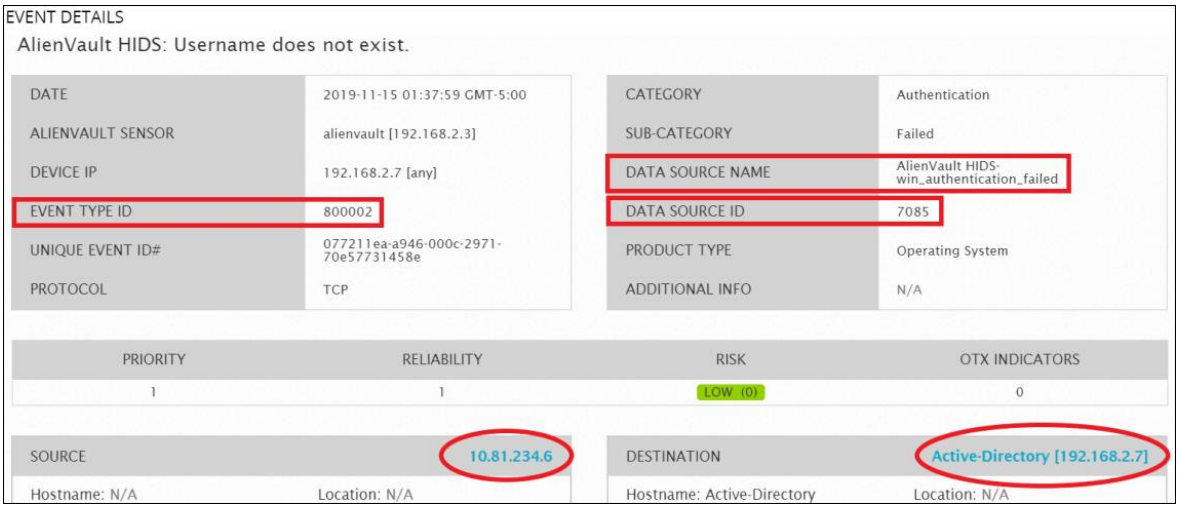


Figura 2.75. Detección de evento de acceso fallido para el usuario Prueba

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.76 se puede ver el nombre del usuario que intentó acceder (Prueba), el ID del evento de Windows (4625), el nombre del equipo que intentó acceder (UIOSOC015A).

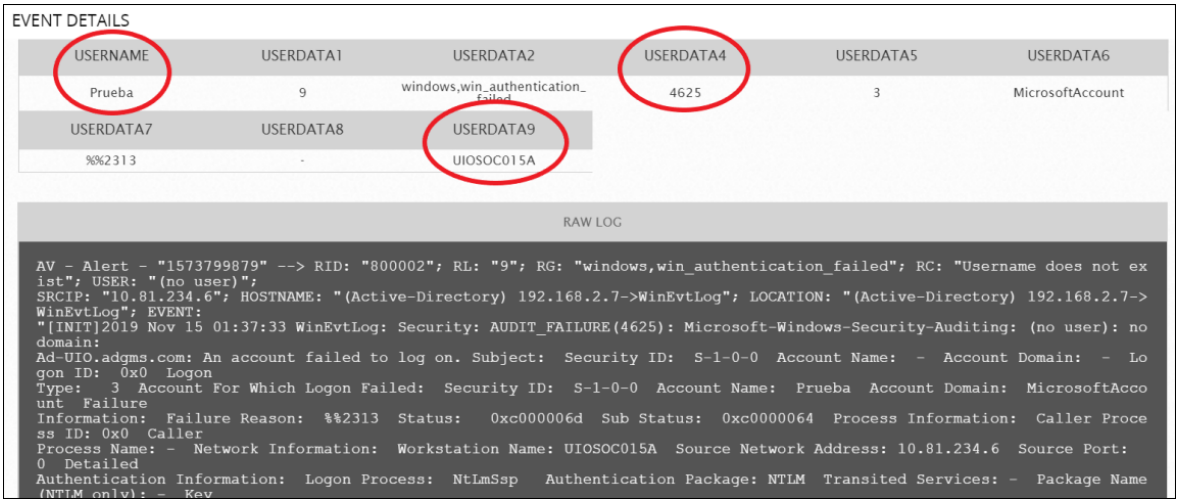


Figura 2.76. Campos adicionales del evento de acceso fallido para el usuario Prueba

2.6.1.1.2 Acceso exitoso:

Se detecta un acceso exitoso de credenciales con el usuario “Administrator” como se indica en la Figura X. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. Los campos SOURCE y DESTINATION indican la dirección IP que intentó acceder y la dirección IP del equipo al que se intentó acceder respectivamente.

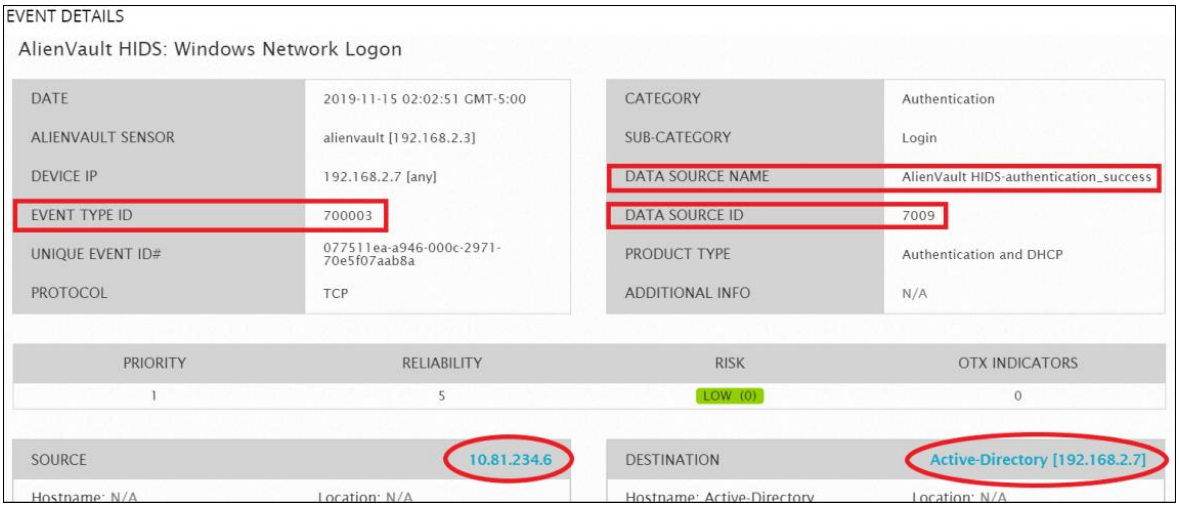


Figura 2.77. Detección de evento de acceso exitoso para el usuario Administrator

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura X se puede ver el nombre del usuario que accedió (Administrator), el ID del evento de Windows (4624), el nombre del equipo que intentó acceder (UIOSOC015A).

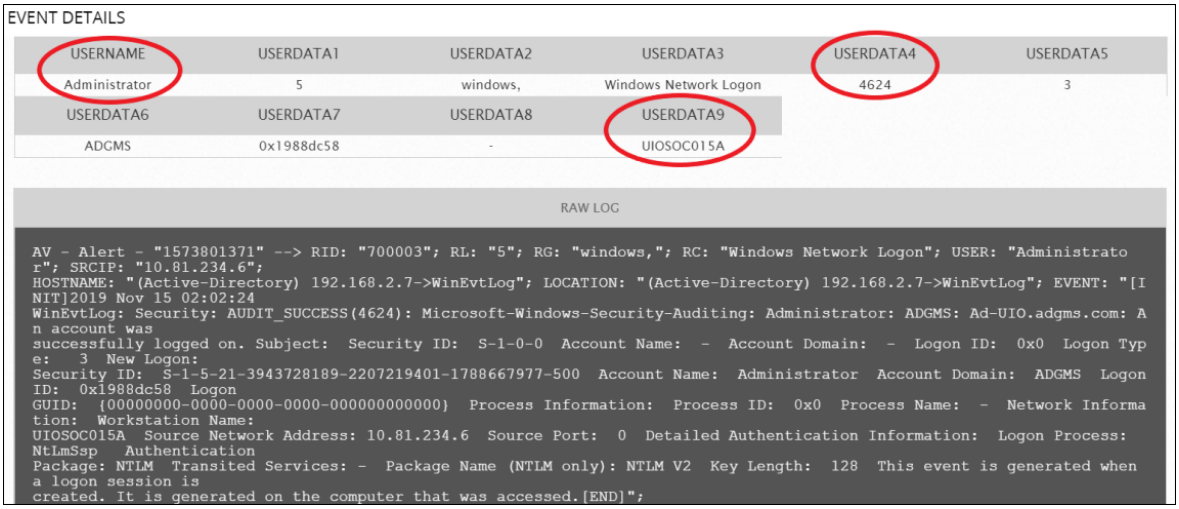


Figura 2.78. Campos adicionales del evento de acceso exitoso para el usuario Administrator

2.6.1.2 Equipos Linux

Para la detección de accesos fallidos, es necesario activar el decodificador “alienvault-linux-pam_rules.xml”, como se indica en [15]. En la Figura 2.79, se puede observar la selección del decodificador mencionado.

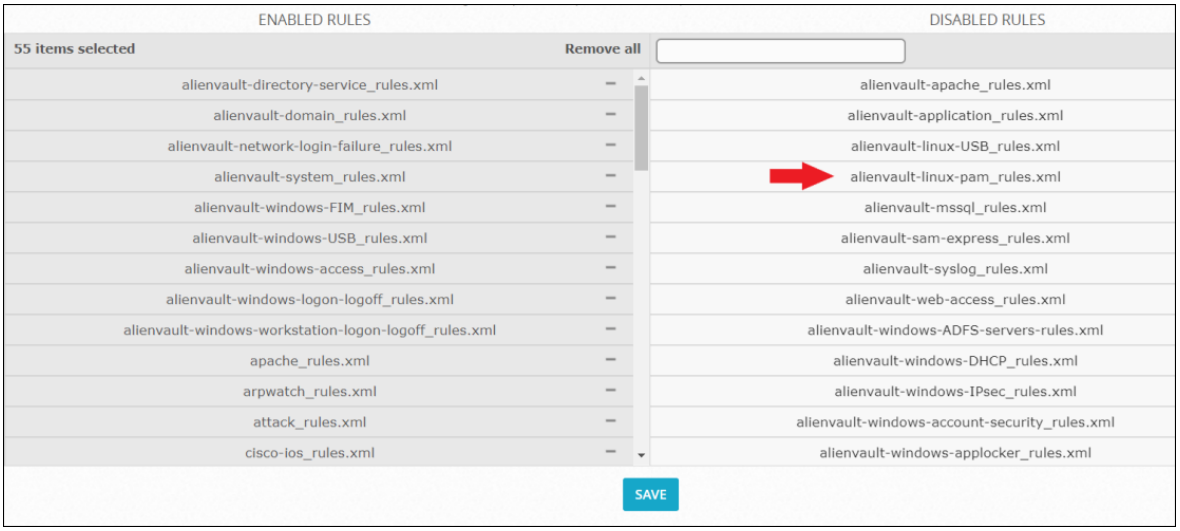


Figura 2.79.Selección del decodificador "alienvault-linux-pan_rules.xml "

Con el decodificador aplicado, se puede reconocer eventos pertenecientes al módulo PAM (Pluggable Authentication Modules) de Linux, el cual es el encargado de manejar los modelos de autenticación en el sistema.

2.6.1.2.1 Acceso fallido

En la Figura 2.80, se tiene la detección de eventos de accesos fallidos para el usuario “root”. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. Los campos SOURCE y DESTINATION indican la dirección IP que intentó acceder y la dirección IP del equipo al que se intentó acceder respectivamente.

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.81 se puede ver el nombre del usuario que intentó acceder (root), la dirección IP desde donde se intentó acceder (10.81.234.6), el nombre del evento (SSHD authentication failed).

Se efectuó un acceso incorrecto de credenciales del usuario no registrado “prueba” como se indica en la Figura 2.82. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. Los

campos SOURCE y DESTINATION indican la dirección IP que intentó acceder y la dirección IP del equipo al que se intentó acceder respectivamente.

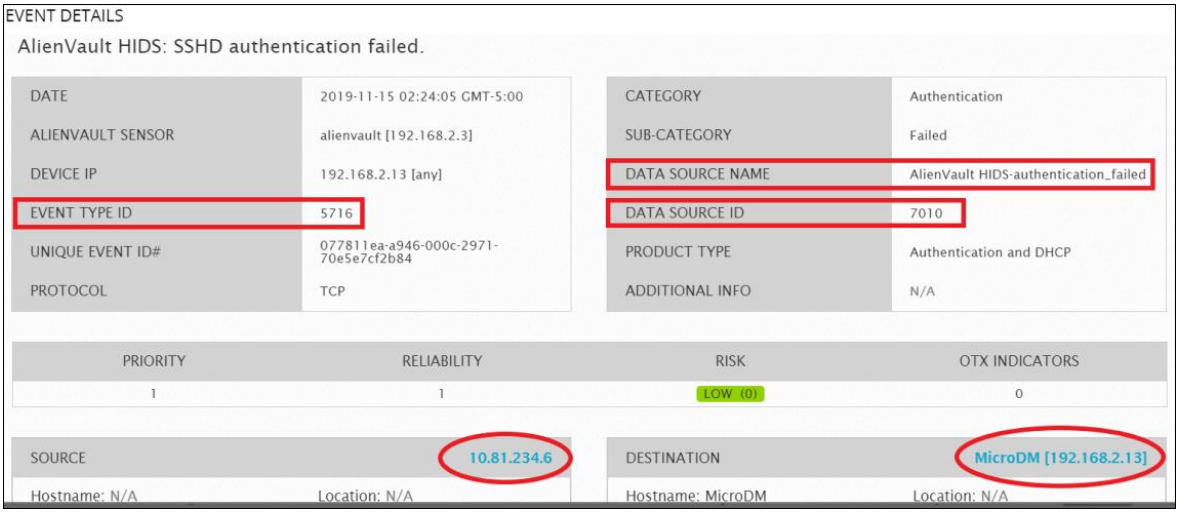


Figura 2.80. Detección de evento de acceso fallido para el usuario root

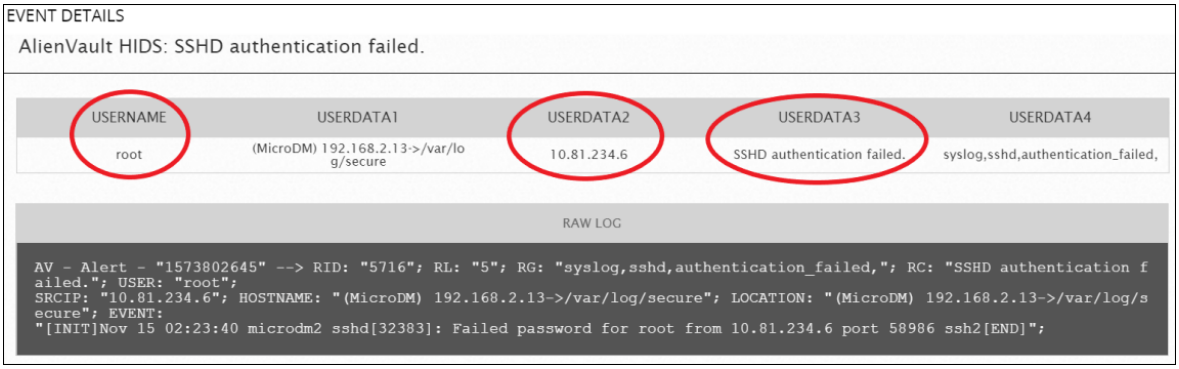


Figura 2.81. Campos adicionales del evento de acceso fallido para el usuario root

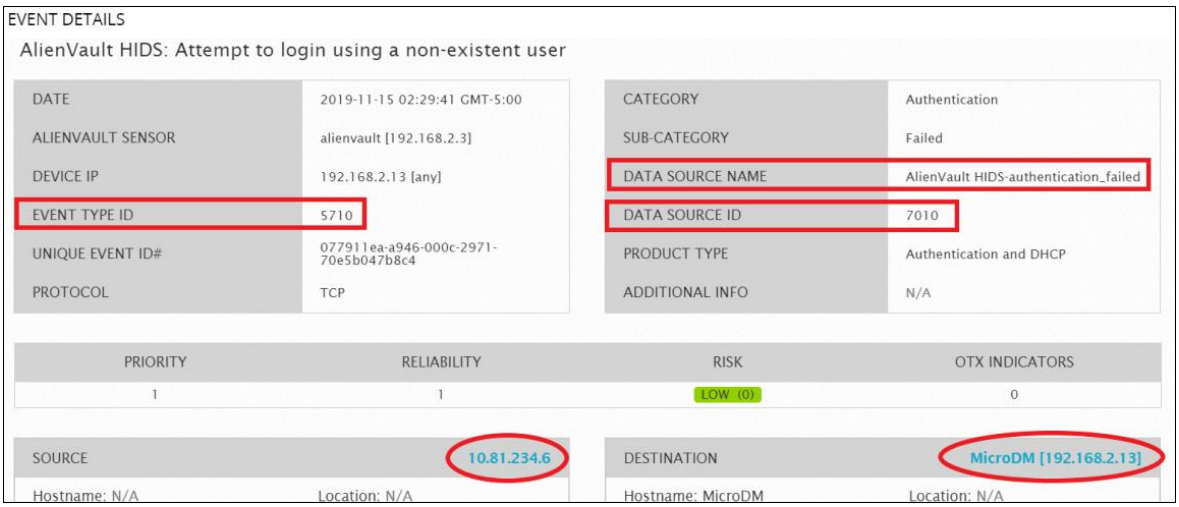


Figura 2.82. Detección de evento de acceso fallido para el usuario prueba

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.83 se puede ver el nombre del usuario que intentó acceder (prueba), la dirección IP desde donde se intentó acceder (10.81.234.6), el nombre del evento (SSHD authentication failed).

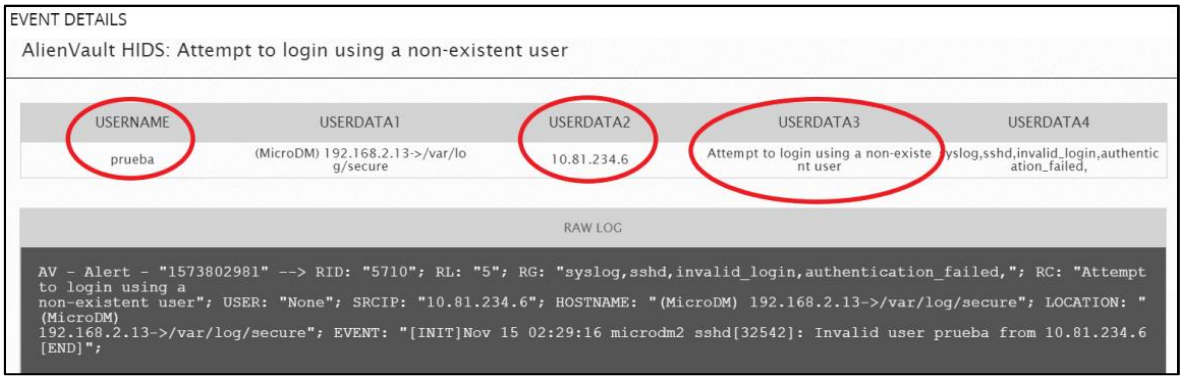


Figura 2.83. Campos adicionales del evento de acceso fallido para el usuario prueba

2.6.1.2.2 Acceso exitoso

Se detecta un acceso exitoso de credenciales con el usuario “root” como se indica en la Figura 2.84. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. Los campos SOURCE y DESTINATION indican la dirección IP que intentó acceder y la dirección IP del equipo al que se intentó acceder respectivamente.

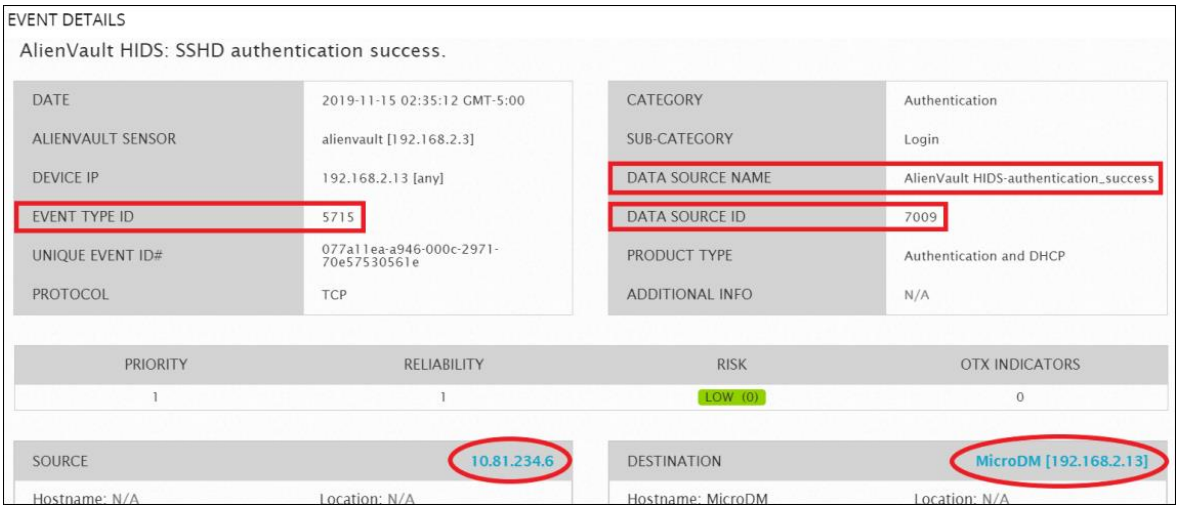


Figura 2.84. Detección de evento de acceso exitoso para el usuario root

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.85 se puede ver el nombre del usuario que intentó acceder

(root), la dirección IP desde donde se intentó acceder (10.81.234.6), el nombre del evento (SSHD authentication success).

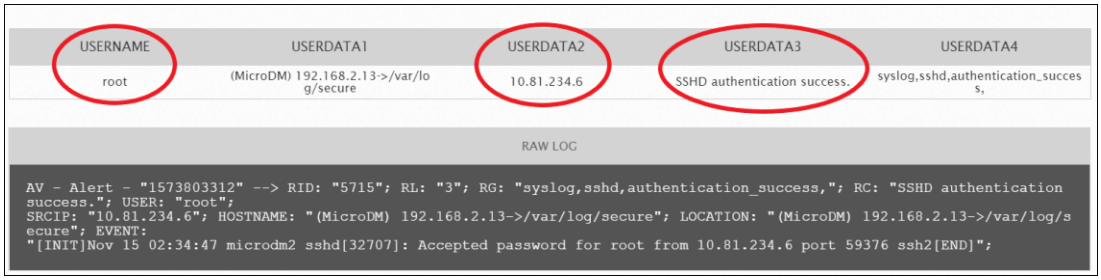


Figura 2.85. Campos adicionales del evento de acceso exitoso para el usuario root

2.6.1.3 Firewall

Para que el firewall Sophos XG envíe logs de accesos es necesario configurar el envío de estos. En este caso se verificó que estén marcadas las opciones que se muestran en la Figura 2.86

Figura 2.86. Configuración logs Firewall

2.6.1.3.1 Acceso fallido - Web

En la Figura 2.87, se tiene la detección de eventos de accesos fallidos para el usuario “alex.quilachamin”. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. El campo SOURCE indica la dirección IP que intentó acceder al firewall.

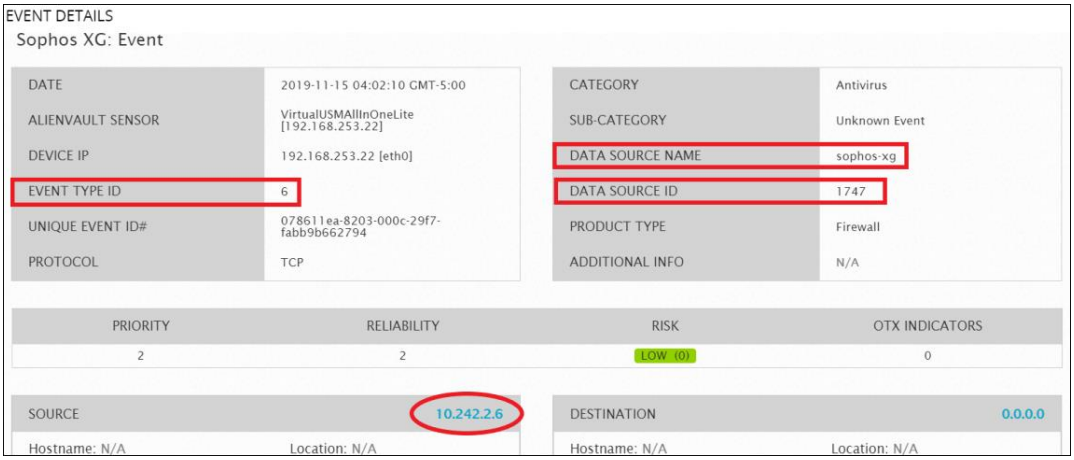


Figura 2.87. Detección de evento de acceso fallido para el usuario alex.quilachamin

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.88 se puede ver que fue un fallo por la web (GUI), el tipo de evento, en este caso de administración (Admin), el estatus del evento (Failed), la prioridad del evento (Notice).

Figura 2.88. Campos adicionales del evento de acceso fallido para el usuario alex.quilachamin

Se efectuó un acceso incorrecto de credenciales del usuario no registrado “prueba” pero el resultado fue el mismo que se obtuvo con un usuario registrado como se indica en la Figura 2.89.

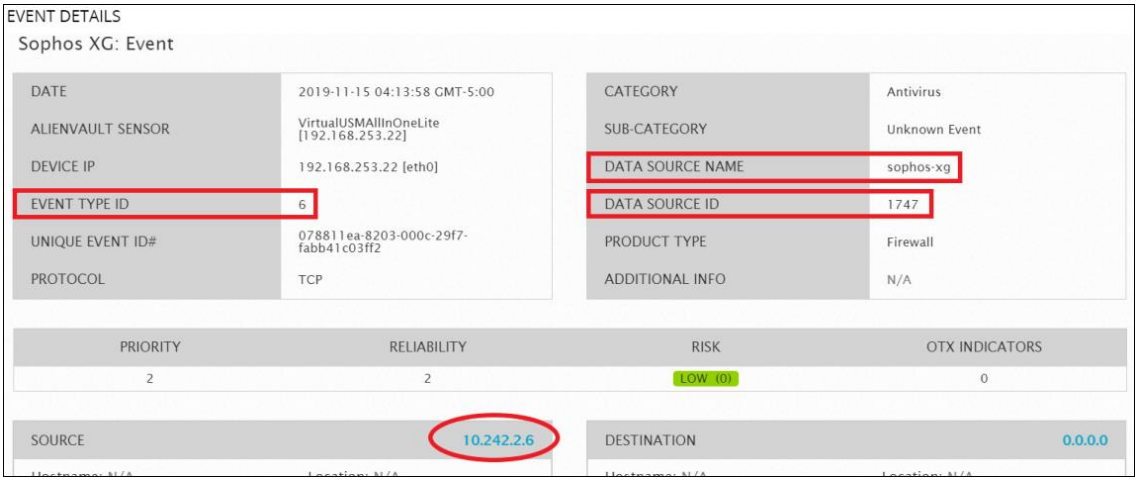


Figura 2.89. Detección de evento de acceso fallido para el usuario prueba

2.6.1.3.2 Acceso fallido – Consola

En la Figura Figura 2.90, se tiene la detección de eventos de accesos fallidos para el usuario “admin”. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. El campo SOURCE indica la dirección IP que intentó acceder al firewall.

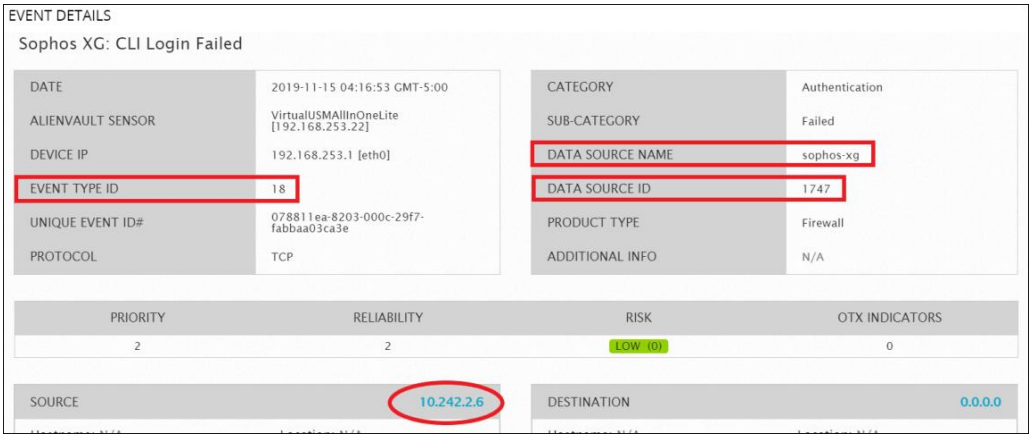


Figura 2.90 Detección de evento de acceso fallido para el usuario admin

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.91 se puede ver el usuario utilizado (admin), que el evento fue un fallo por consola (CLI), el tipo de evento, en este caso de administración (Admin), el estatus del evento (Failed), la prioridad del evento (Notice).

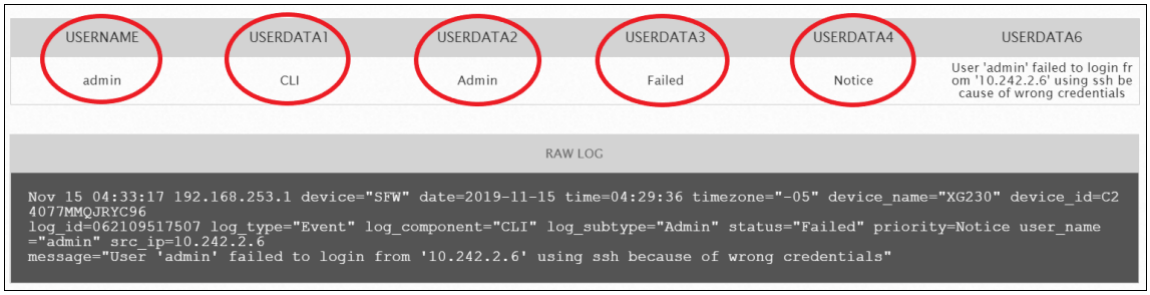


Figura 2.91. Campos adicionales del evento de acceso fallido para el usuario admin

Se efectuó un acceso incorrecto de credenciales del usuario no registrado “prueba” pero el resultado fue el mismo que se obtuvo con un usuario registrado como se indica en la Figura 2.92.

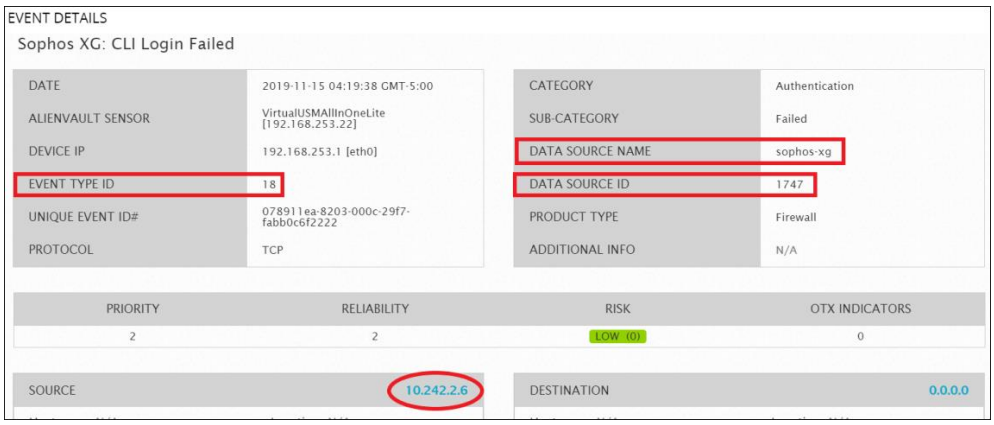


Figura 2.92. Detección de evento de acceso fallido para el usuario prueba

2.6.1.3.3 Acceso exitoso - Web

En la Figura Figura 2.93, se tiene la detección de eventos de accesos exitosos para el usuario “alex.quilachamin”. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. El campo SOURCE indica la dirección IP que intentó acceder al firewall.

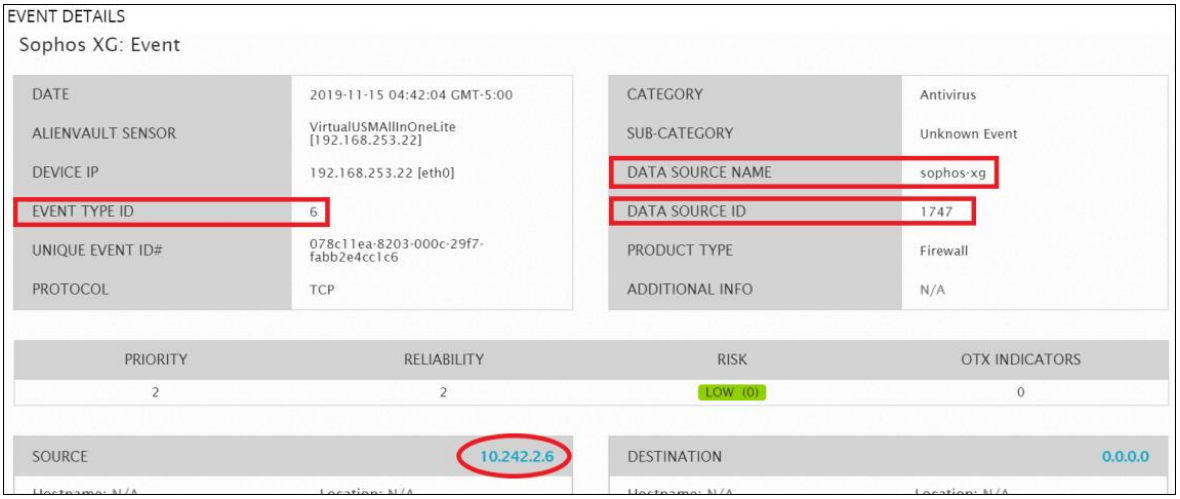


Figura 2.93. Detección de evento de acceso exitoso para el usuario alex.quilachamin

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.94 se puede ver que el evento fue un fallo por la web (GUI), el tipo de evento, en este caso de administración (Admin), el estatus del evento (Successful), la prioridad del evento (Information).

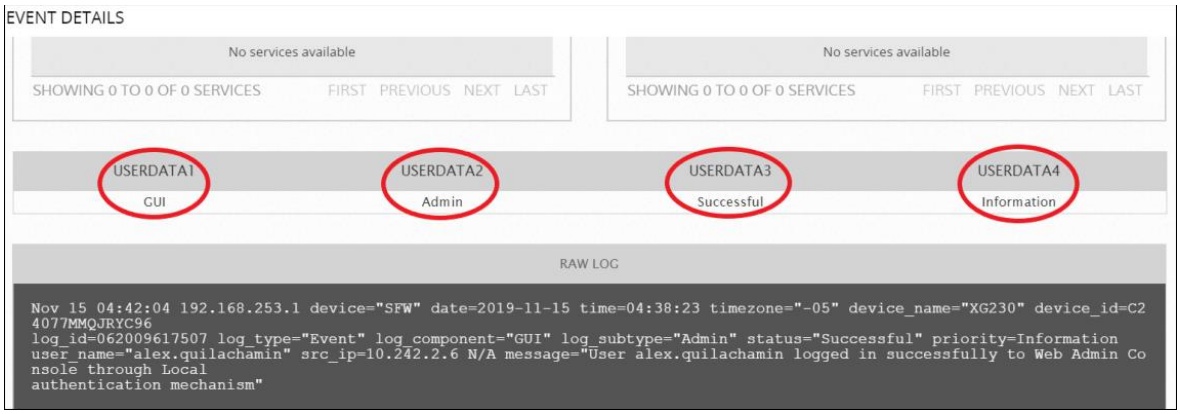


Figura 2.94. Campos adicionales del evento de acceso exitoso para el usuario root

2.6.1.3.4 Acceso exitoso - Consola

En la Figura Figura 2.95, se tiene la detección de eventos de accesos fallidos para el usuario “admin”. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID

identifican a este evento y permiten realizar la implementación de directivas. El campo SOURCE indica la dirección IP que intentó acceder al firewall.

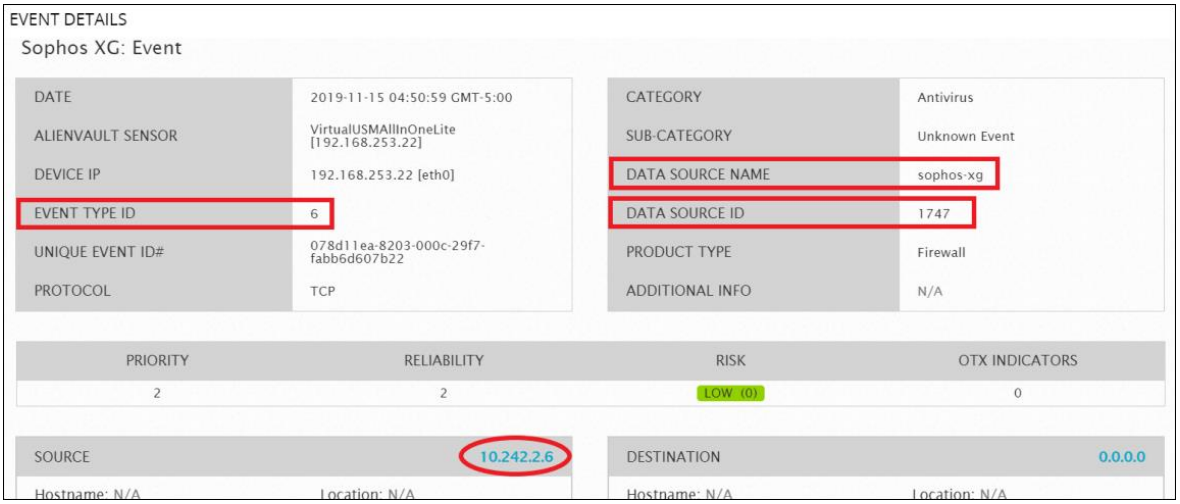


Figura 2.95 Detección de evento de acceso exitoso para el usuario admin

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.96 se puede ver que el evento fue un fallo por consola (CLI), el tipo de evento, en este caso de administración (Admin), el estatus del evento (Successful), la prioridad del evento (Information).

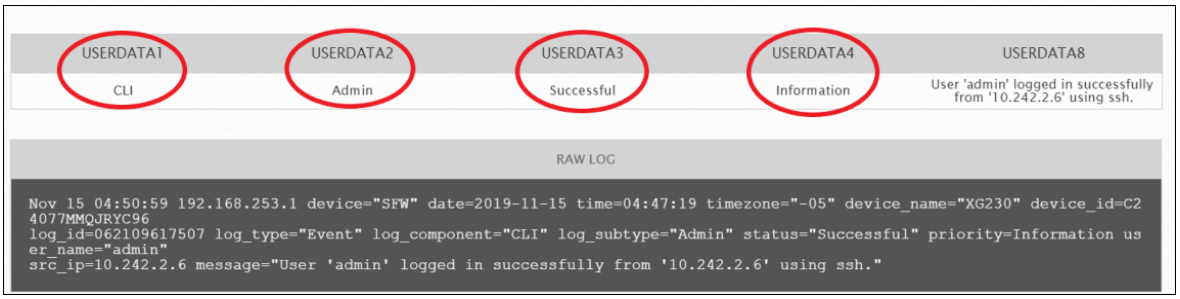


Figura 2.96. Campos adicionales del evento de acceso exitoso para el usuario admin

2.6.1.4 Equipo Virtualizador VMware

Los eventos que se detectaron por el plugin de VMware ESXi mostraron eventos muy genéricos tanto para el acceso fallido como exitoso como se muestra en la Figura 2.97 y la Figura 2.98 respectivamente.

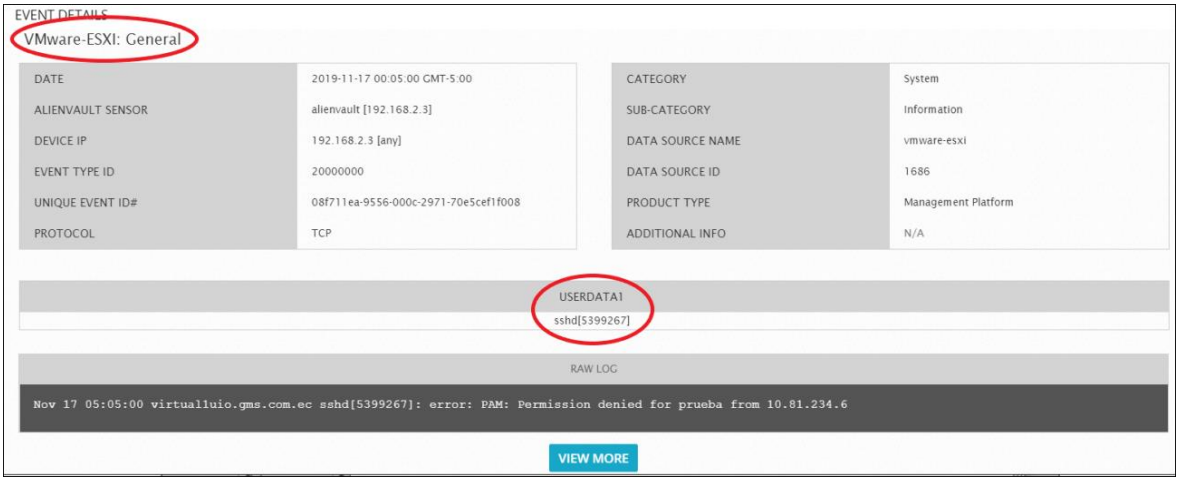


Figura 2.97. Evento de acceso fallido

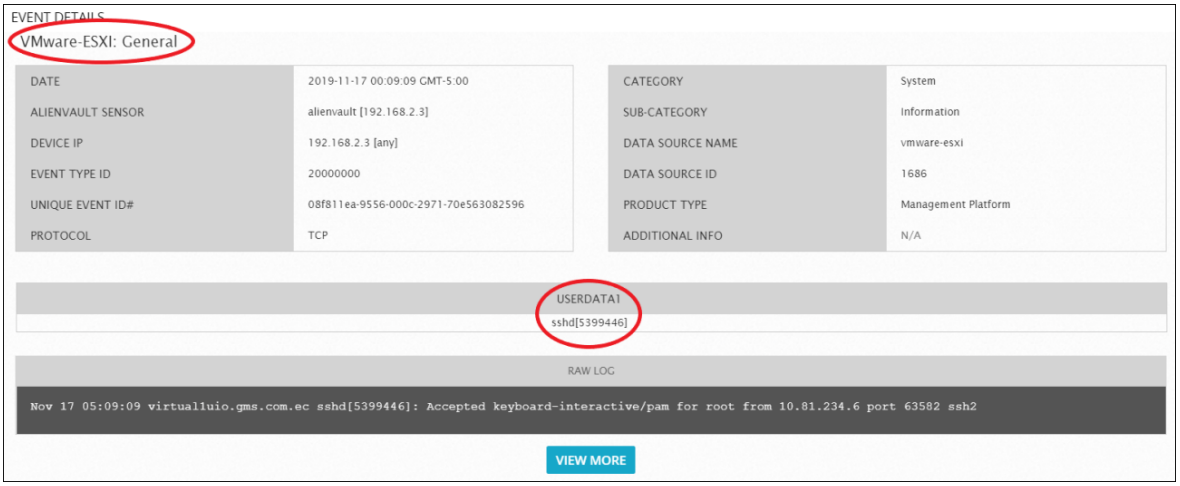


Figura 2.98. Evento de acceso exitoso

Los campos de USERDATA tampoco mostraron datos opcionales para usar en los filtros de las directivas. Por tal motivo se utilizó adicionalmente el plugin de VMware vCenter en el activo 192.168.2.2 como se indica en la Figura 2.99

Figura 2.99. Activación plugin VMware vCenter

2.6.1.4.1 Acceso fallido

En la Figura 2.100, se tiene la detección de eventos de accesos fallidos para el usuario “prueba”. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. El campo SOURCE indica la dirección IP que intentó acceder al VMware.

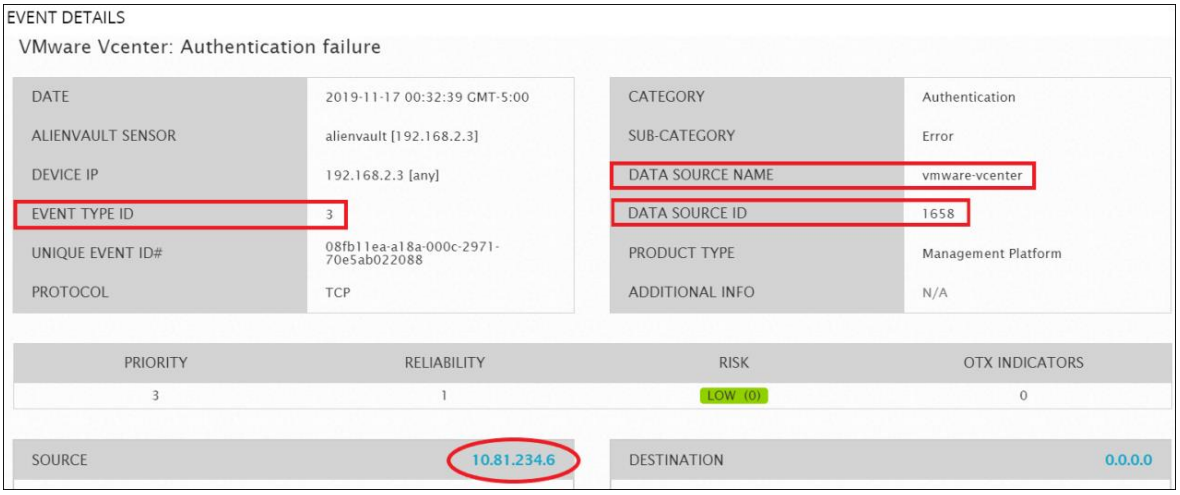


Figura 2.100. Detección de evento de acceso fallido para el usuario prueba

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.101 se puede ver que fue un fallo por la web (GUI), el tipo de evento, en este caso de administración (Admin), el estatus del evento (Failed), la prioridad del evento (Notice).

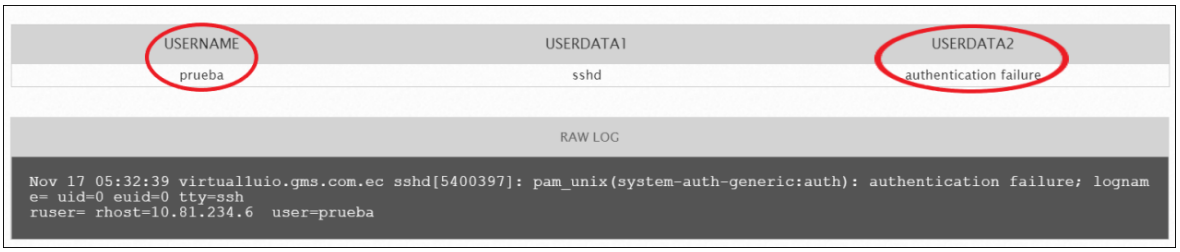


Figura 2.101. Campos adicionales del evento de acceso fallido para el usuario prueba

2.6.1.4.2 Acceso exitoso - Consola

En la Figura 2.102, se tiene la detección de eventos de accesos fallidos para el usuario “admin”. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. El campo SOURCE indica la dirección IP que intentó acceder al firewall.

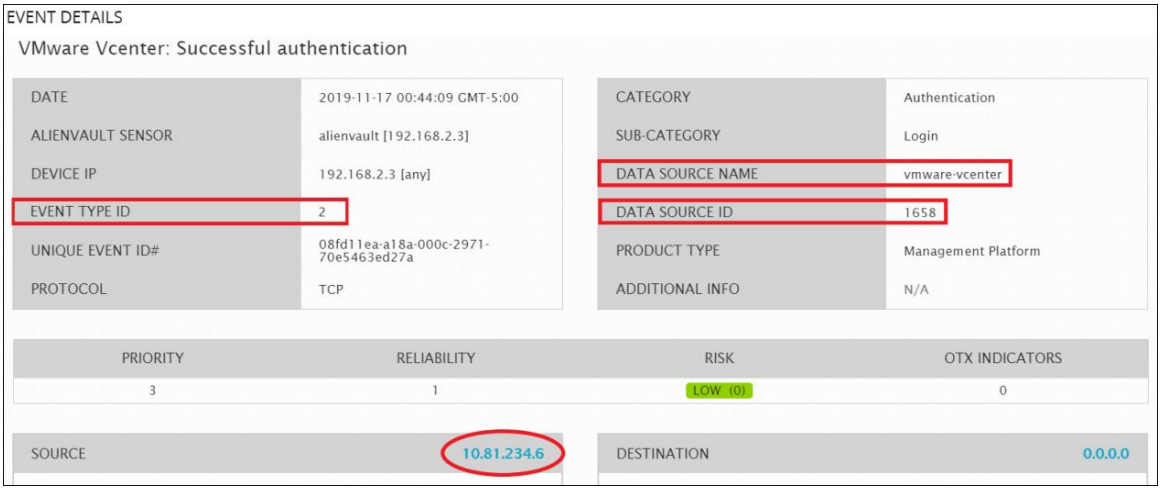


Figura 2.102 Detección de evento de acceso exitoso para el usuario root

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.103 se puede ver que el usuario utilizado es el root.

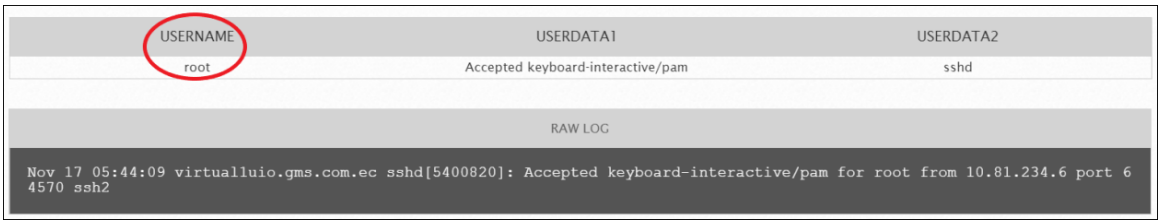


Figura 2.103. Campos adicionales del evento de acceso exitoso para el usuario root

2.6.2 CAMBIOS EN CONFIGURACIONES

En esta sección se identificaron eventos relacionados a la creación, eliminación y modificación de usuarios.

2.6.2.1 Equipos Windows

Para que el equipo pueda enviar logs cuando se efectúe la creación de un usuario, fue necesario activar la auditoría de Windows y seleccionar que se auditen los eventos de administración de cuentas de usuario como se indica en la Figura 2.104 y en la Figura 2.105.

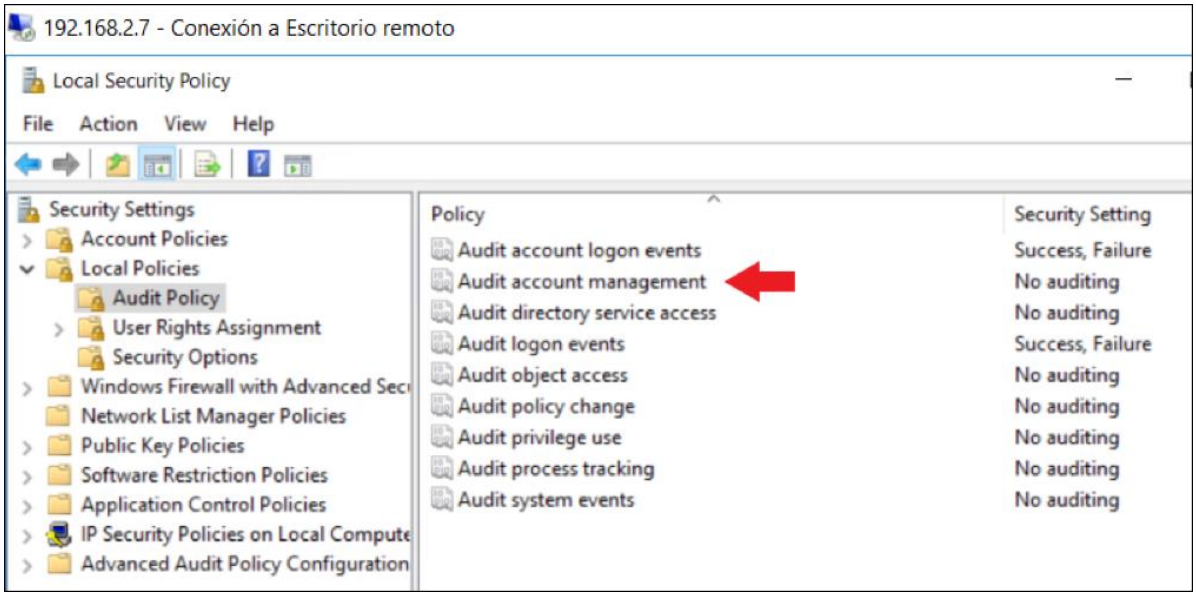


Figura 2.104. Auditoría de eventos de administración de usuario

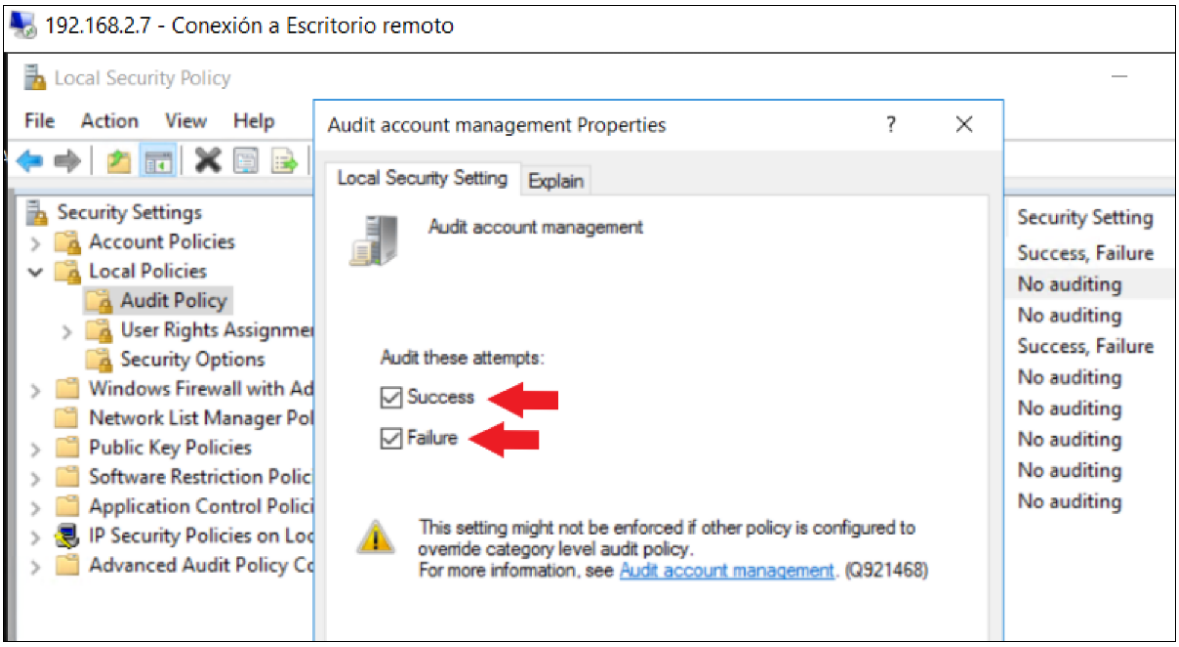


Figura 2.105. Selección de auditoría de administración de usuarios

Con lo realizado anteriormente, se busca obtener el evento 4720 (A user account was created).

2.6.2.1.1 Creación de usuario prueba

Se efectuó la creación del usuario “prueba” como se indica en la Figura 2.106. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. Los campos SOURCE y DESTINATION indican la dirección IP del equipo en el cual se creó el usuario.

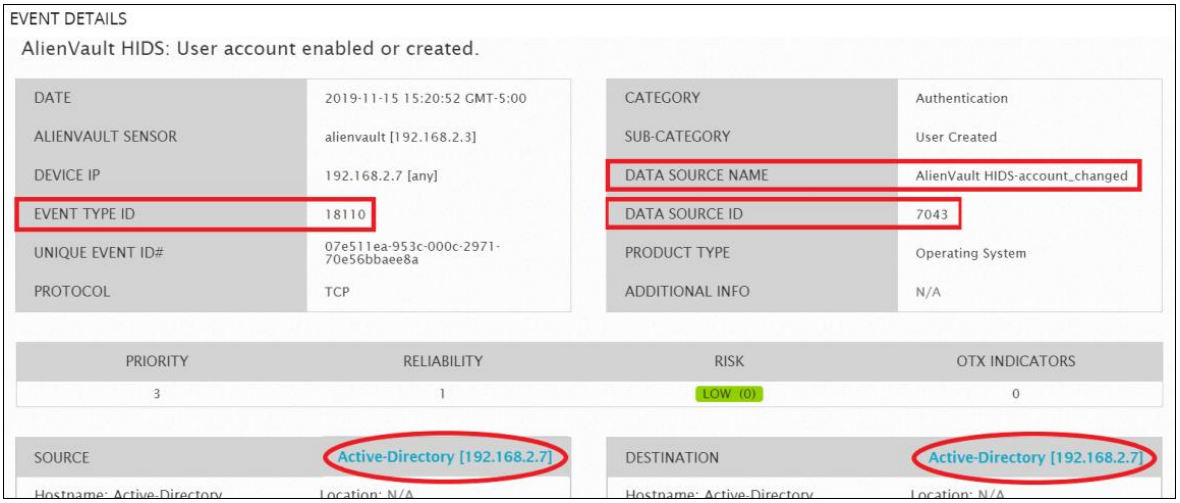


Figura 2.106. Detección de evento de creación del usuario prueba

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.74 se puede ver el nombre del usuario que generó el nuevo usuario (Administrator), el ID del evento de Windows (4720), el nombre del nuevo usuario generado (prueba).

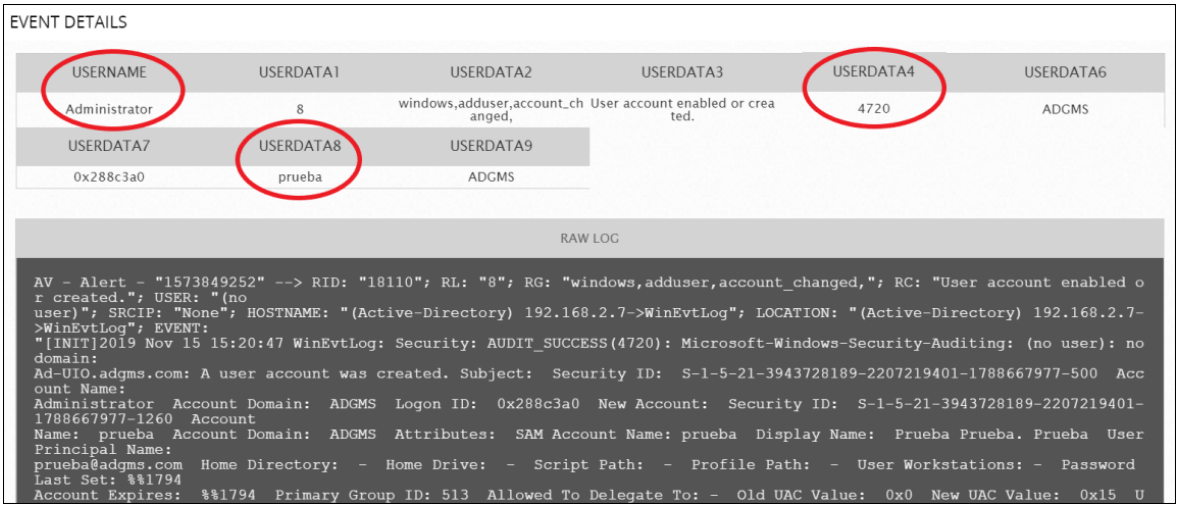


Figura 2.107. Campos adicionales del evento de creación del usuario prueba

2.6.2.2 Equipos Linux

Para la detección de los eventos relacionados a la creación, eliminación y modificación de usuarios, es necesario activar el decodificador “alienvault-system_rules.xml” como se muestra en la Figura 2.108

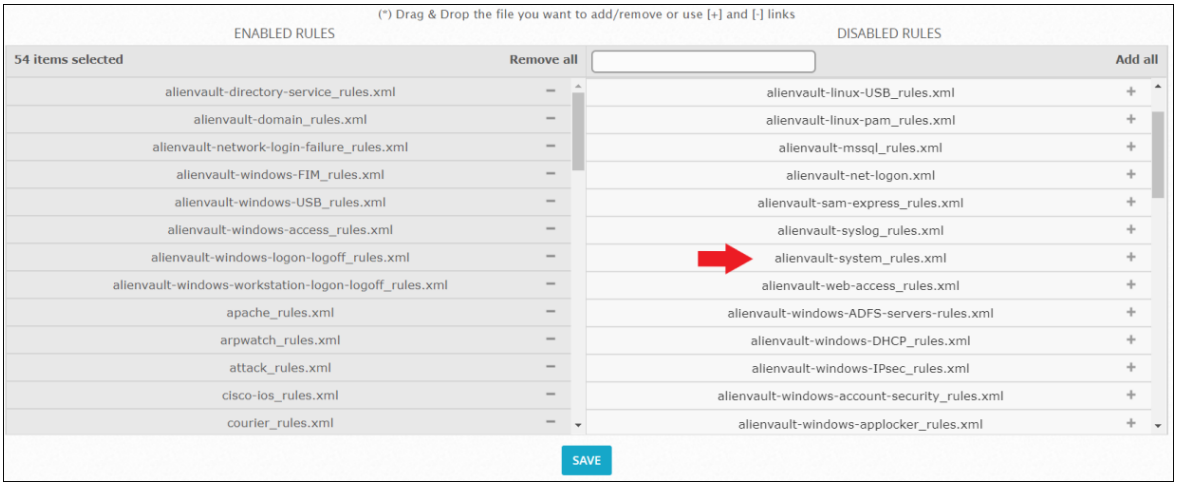


Figura 2.108. Selección del decodificador "alienvault-system_rules.xml "

2.6.2.2.1 Creación de usuario prueba

Se efectuó la creación del usuario “prueba” como se indica en la Figura 2.109. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. El campo SOURCE indica la dirección IP del equipo en el cual se creó el usuario.

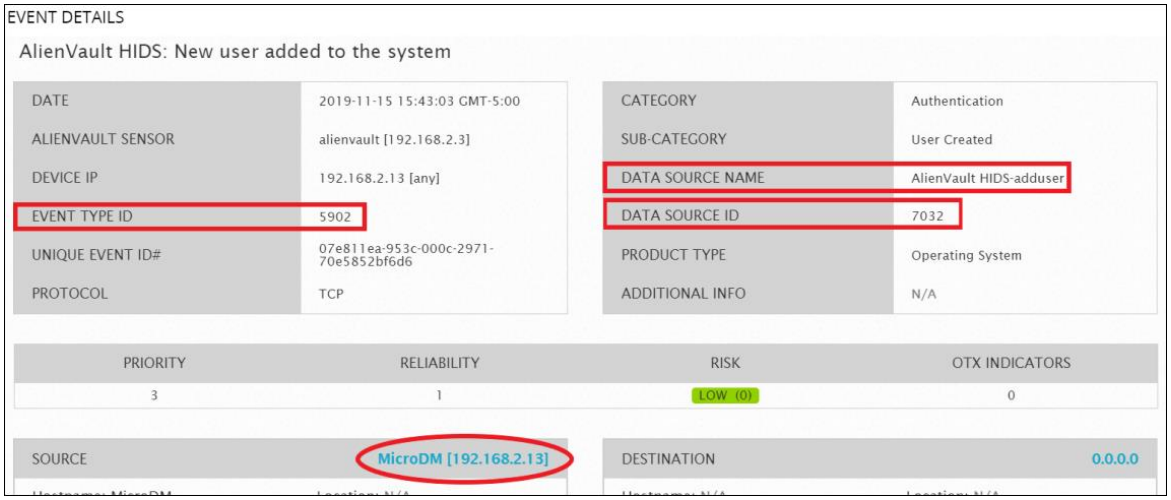


Figura 2.109. Detección de evento de creación del usuario prueba

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.110 se puede ver el nombre del usuario generado (prueba).

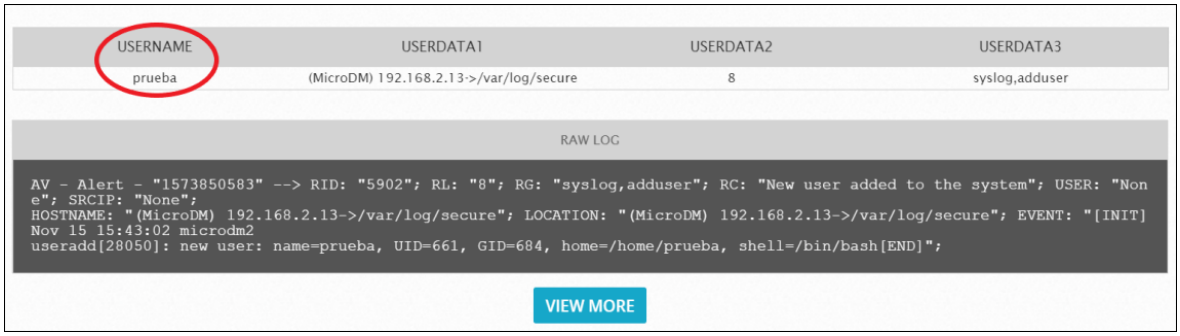


Figura 2.110. Campos adicionales del evento de creación del usuario prueba

2.6.2.3 Firewall

2.6.2.3.1 Creación de usuario prueba

Se efectuó la creación del usuario “prueba” como se indica en la Figura 2.111. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. El campo SOURCE indica la dirección IP del equipo en el cual se creó el usuario.

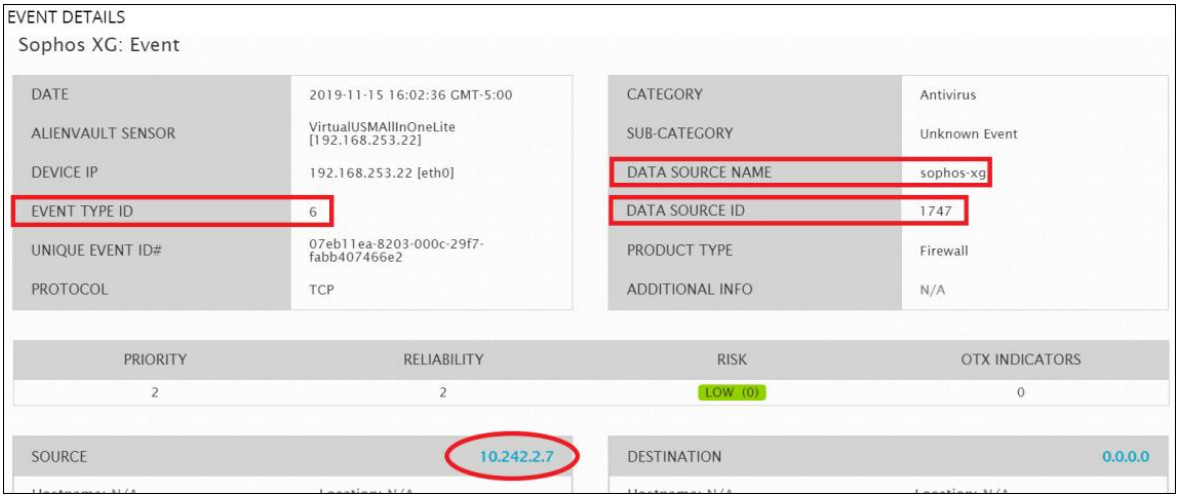


Figura 2.111. Detección de evento de creación del usuario prueba

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.112 se puede ver que el evento fue un fallo por web (GUI), el tipo de evento, en este caso de administración (Admin), el estatus del evento (Successful), la prioridad del evento (Information).

Figura 2.112. Campos adicionales del evento de creación del usuario prueba

2.6.2.4 Equipo Virtualizador VMware

2.6.2.4.1 Creación de usuario prueba

Se efectuó la creación del usuario “prueba” como se indica en la Figura 2.113. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas.

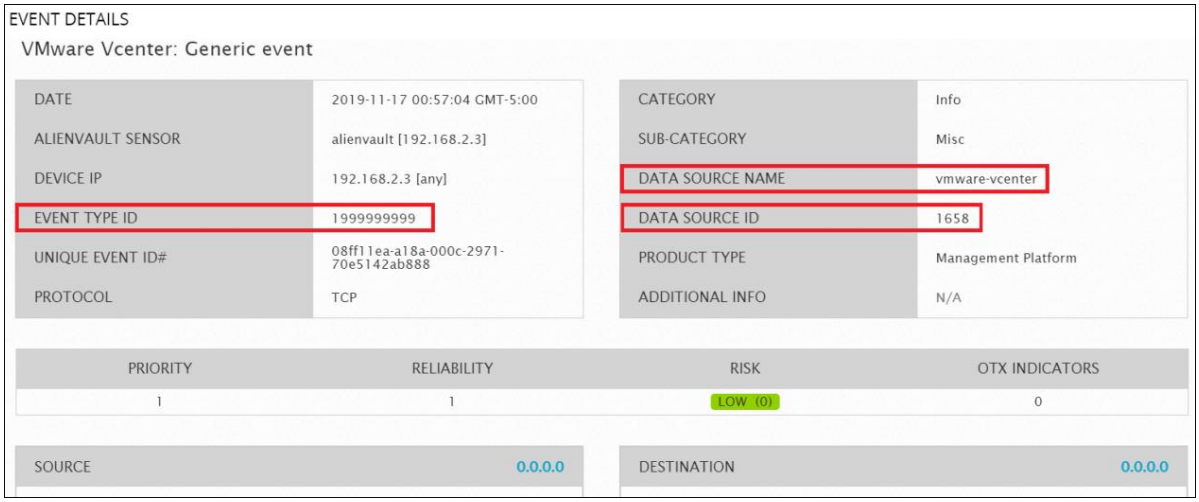


Figura 2.113. Detección de evento de creación del usuario prueba

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.114 se puede ver el campo USERDATA1 contiene el dato “passwd”, este se utilizará para distinguir el evento de otros y se usará en la creación de la directiva.

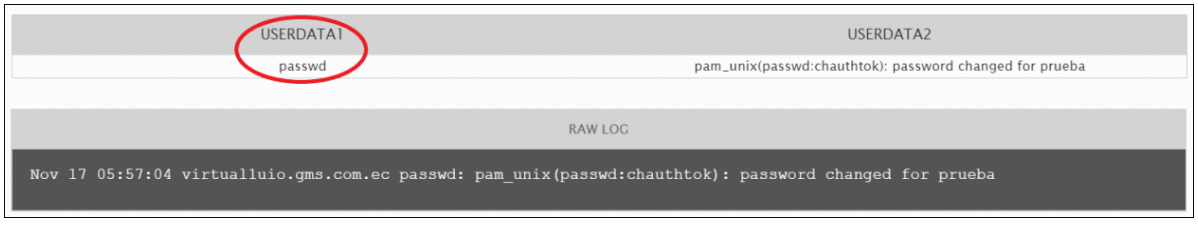


Figura 2.114. Campos adicionales del evento de creación del usuario prueba

2.6.3 CONEXIONES PERMITIDAS EN EL FIREWALL

Se detectó el evento de conexiones permitidas hacia internet como se indica en la Figura 2.115. Los datos DATA SOURCE NAME, DATA SOURCE ID y EVENT TYPE ID identifican a este evento y permiten realizar la implementación de directivas. El campo SOURCE indica la dirección IP del equipo el cual estableció la comunicación y el campo DESTINATION indica la dirección IP a la cual se accedió.

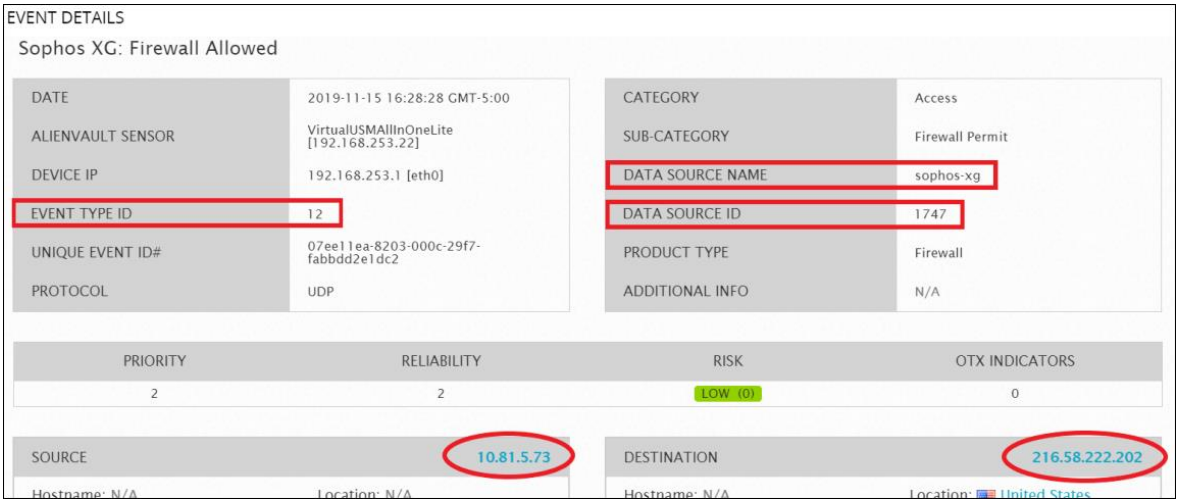


Figura 2.115. Detección de evento de creación del usuario prueba

Campos adicionales que entrega el evento, se los puede encontrar en los USERDATA que OSSIM maneja. En la Figura 2.116 se puede ver que el evento tiene el estatus de permitido (Allow).

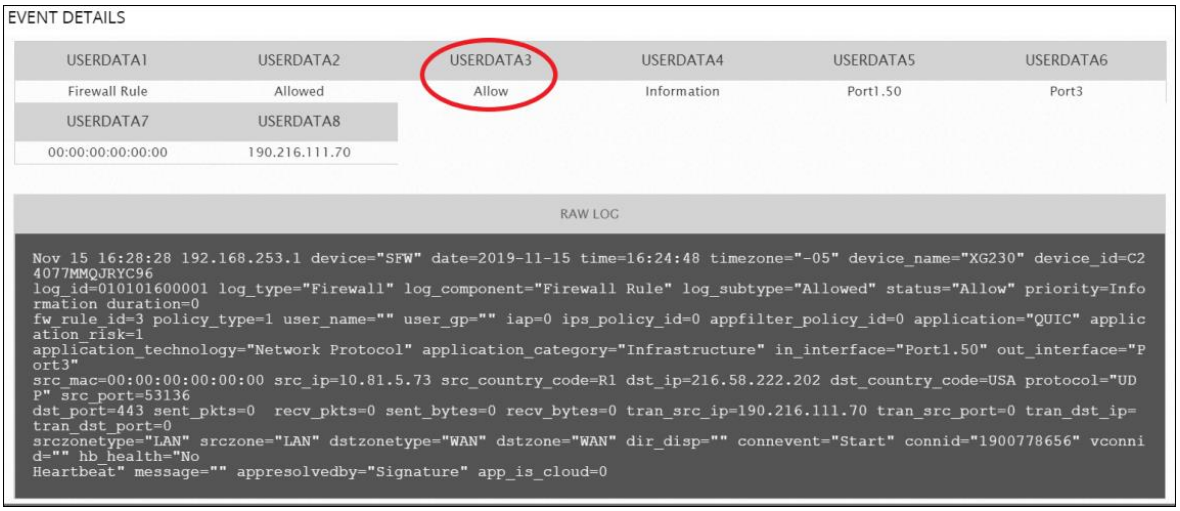


Figura 2.116. Campos adicionales del evento de creación del usuario prueba

2.7 CONFIGURACIÓN DE DIRECTIVAS DE CORRELACIÓN

De acuerdo con [16], la generación de alarmas se basa en el riesgo que se genere por uno o la sucesión de eventos. El riesgo se representa en 3 niveles como se indica en la Tabla 2.14

Tabla 2.14. Niveles de riesgo OSSIM

Nivel	Valor de riesgo
Bajo	1
Medio	2
Alto	Mayor o igual a 3

Los eventos o alarmas que se presentan en OSSIM van a tener a asociados 4 parámetros como se indica en la Figura 2.117

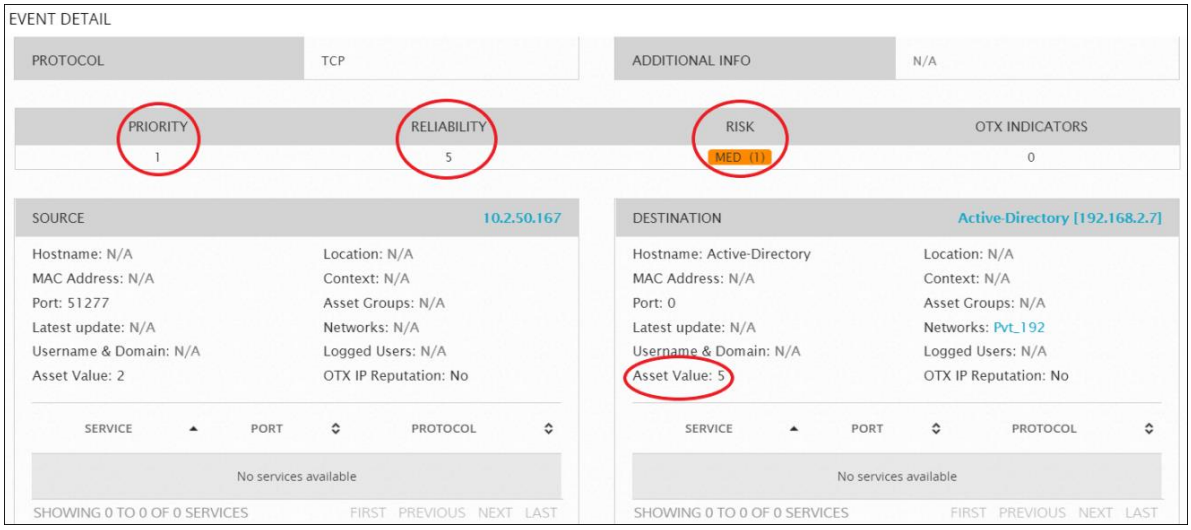


Figura 2.117. Parámetros de eventos

La guía de OSSIM [16] especifica lo siguiente:

- **Valor del activo:** Importancia de un activo o criticidad. Varía de 0 a 5
- **Confiabilidad del evento:** Especifica la probabilidad de que el evento sea exacto. Varía de 0 a 10
- **Prioridad del evento:** Define con qué urgencia se debe investigar el evento. Varía de 0 a 5

Estos parámetros son personalizables y dependerán de la configuración que se le dé a cada evento como se indica en [16] a excepción del riesgo, el cual se calcula mediante la ecuación 2.1:

$$\text{Riesgo} = \frac{(\text{Valor del activo}) \text{ x } (\text{Confiabilidad del evento}) \text{ x } (\text{Prioridad del evento})}{25} \quad (2.1)$$

Entonces, si se tiene un activo con un valor de 3 y el evento tiene valores de confiabilidad y prioridad de 4 y 5 respectivamente, el riesgo sería el resultado de la ecuación

$$\text{Riesgo} = \frac{(3) \text{ x } (4) \text{ x } (5)}{25} = 2{,}4$$

El resultado sería un valor de 2,4 el cual se redondea a 2 generado una alarma de nivel medio de acuerdo con la Tabla 2.14.

El valor de los activos a monitorear se lo tiene establecido con base en la valoración de activos realizada en 2.1.1.2.

Para el valor de prioridad de las alarmas se utilizará el valor más alto que es de 5. Esto permite utilizar el valor de confiabilidad como un valor de control para definir el riesgo final que tendrá la alarma, ya que los valores de los equipos a monitorear tienen un valor de activo igual a 5. Reemplazando en la ecuación 1.1 se tiene lo siguiente:

$$\text{Riesgo} = \frac{(5) \text{ x } (\text{Confiabilidad del evento}) \text{ x } (5)}{25}$$

$$\text{Riesgo} = \text{Confiabilidad del evento}$$

2.7.1 DETECCIÓN DE ATAQUE DE FUERZA BRUTA

Para la creación de las directivas, se utilizó como referencia los eventos detectados en la sección 2.6. Esto permite establecer los eventos que iniciarán las directivas y los cuales son necesarios para la generación de la alarma.

2.7.1.1 Equipos Windows

Se debe dirigir a la sección CONFIGURATION > THREAT INTELLIGENCE > DIRECTIVES y dar clic en “New Directives”. Aparecerá un cuadro para el ingreso de datos en la nueva directiva como se muestra en la Figura 2.118. Los pasos que seguir se muestran a continuación:

A. Nombre de la directiva: Ataque de fuerza bruta - Windows

B. Intento: Delivery & Attack

C. Strategy: Bruteforce Authenticaction

D. Method: Ataque de fuerza bruta - Windows

E. Prioridad: 5 (Definido en la sección 2.7 para el cálculo del riesgo de la alarma)

F. Clic en Next

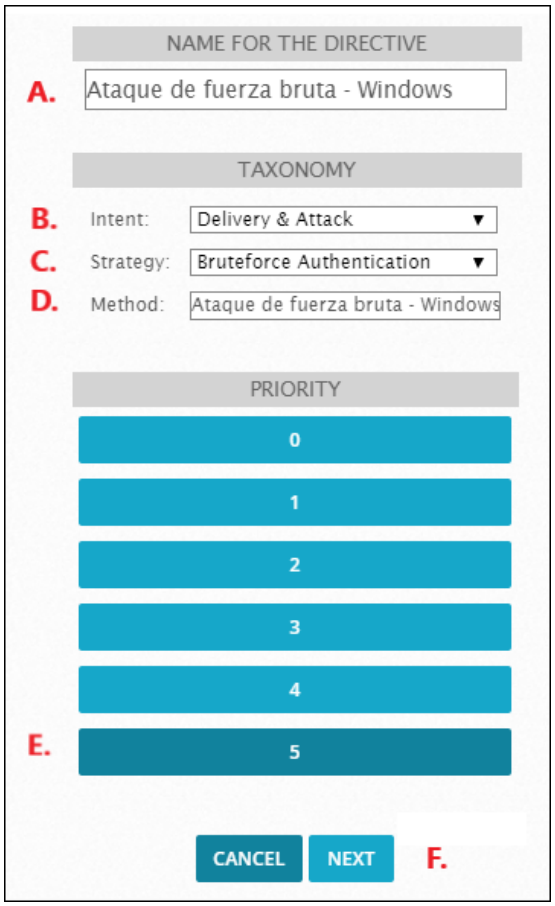


Figura 2.118. Creación de directiva para fuerza bruta nivel 1

G. La siguiente ventana pide el ingreso del nombre de la primera regla de correlación que se está creando como se indica en Figura 2.119. Esta iniciará es la que dará inicio a la directiva. Se coloca como nombre “Acceso Fallido”

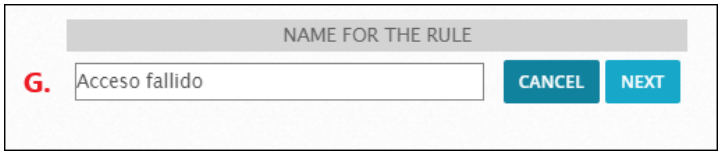


Figura 2.119. Primer nivel de correlación Fuerza Bruta - Windows

H. Se selecciona el tipo de evento detectado en 2.6.1.1.1, el cual permite reconocer eventos de accesos fallidos en Windows.

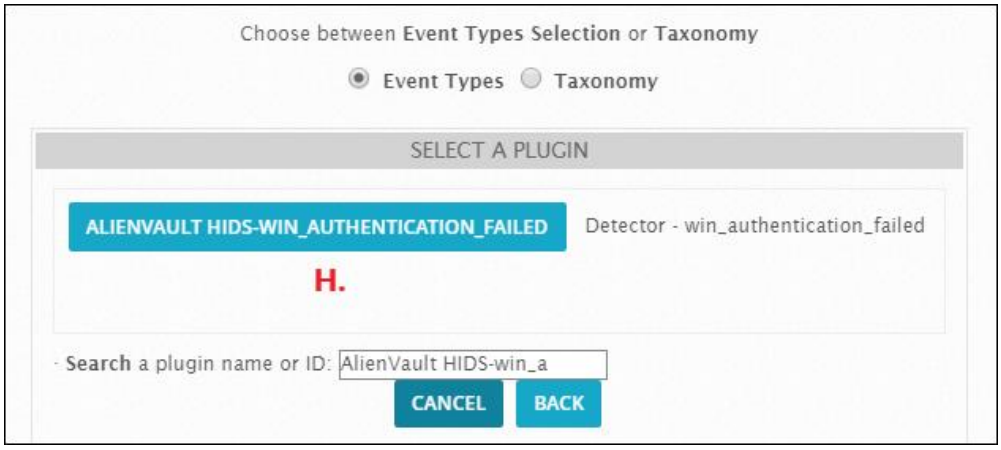


Figura 2.120. Evento de acceso fallido Windows

I. Luego, se seleccionan los subeventos detectados en 2.6.1.1.1, como se muestra en Figura 2.121. Estos eventos representan el acceso incorrecto tanto de una cuenta registrada como de una que no.

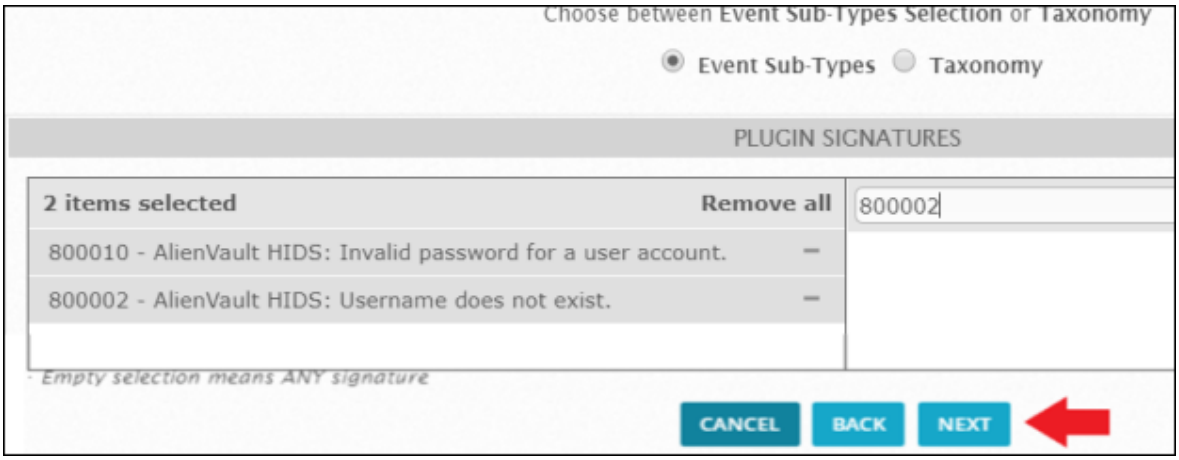


Figura 2.121. Subeventos de accesos fallidos - Windows

J. Después se solicitará, si es necesario, definir parámetros específicos para los eventos configurados como dirección IP origen o destino, puertos utilizados, etc. En este caso, no es necesario definir ninguna dirección IP destino o fuente ni ningún puerto específico, ya que el acceso puede ser producido desde una dirección IP cualquiera. Se da clic en el botón NEXT de la ventana de Configuración Red como se ve en la Figura 2.122

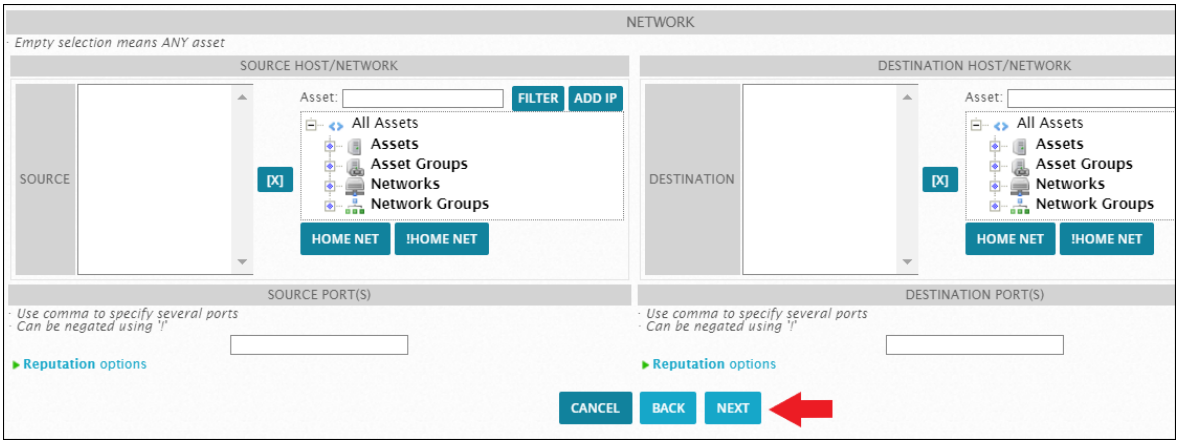


Figura 2.122. Configuración de red directiva

K. De acuerdo con el diseño de la directiva en 1213, se selecciona como confiabilidad (reliability) el valor de 0 como se indica en la Figura 2.123 porque no se requiere que se genere una alarma en el primer acceso fallido. A continuación, se da clic en FINISH

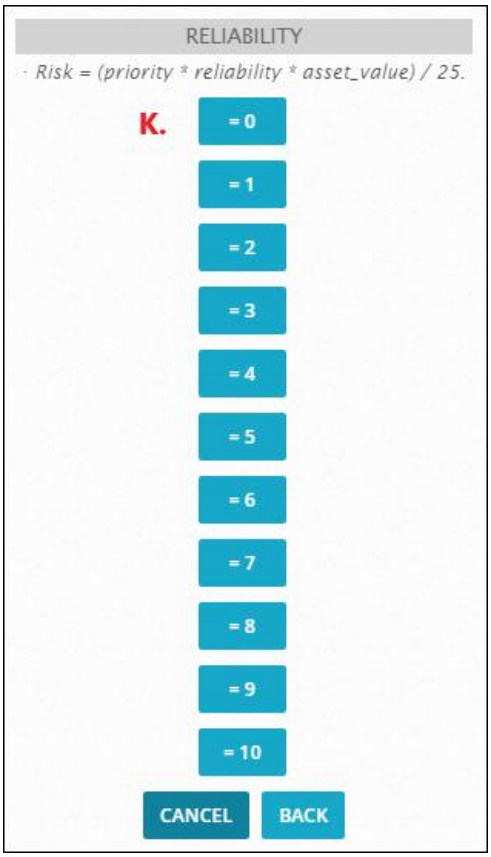


Figura 2.123. Confiabilidad primer acceso fallido

L. La nueva directiva será mostrada en la sección de “User Contributed” como se indica en la Figura 2.124

Figura 2.124. Listado de directivas

M. Para agregar más niveles de correlación, se debe dar clic en el signo + como se observa en la Figura 2.125

Figura 2.125. Agregación de niveles de correlación

N. Para el segundo nivel de correlación es necesario la creación de 2 reglas, una permitirá la detección del evento de acceso correcto y la segunda si hubo más accesos fallidos hacia la misma dirección IP destino. La regla de detección del acceso correcto lleva el nombre de “Acceso exitoso” como se ve en la Figura 2.126

Figura 2.126. Segundo nivel de correlación Acceso exitoso

O. Para la detección de eventos de acceso correcto se selecciona el detector “Alienvault hids-authentication_success” de acuerdo con lo detectado en 2.6.1.1.2 como se observa en la Figura 2.127 y el subevento seleccionado es el 700004 correspondiente al acceso exitoso como se puede ver en la Figura 2.128

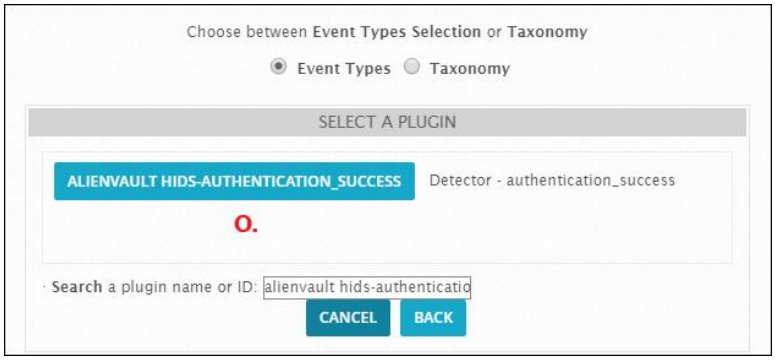


Figura 2.127. Evento de acceso exitoso

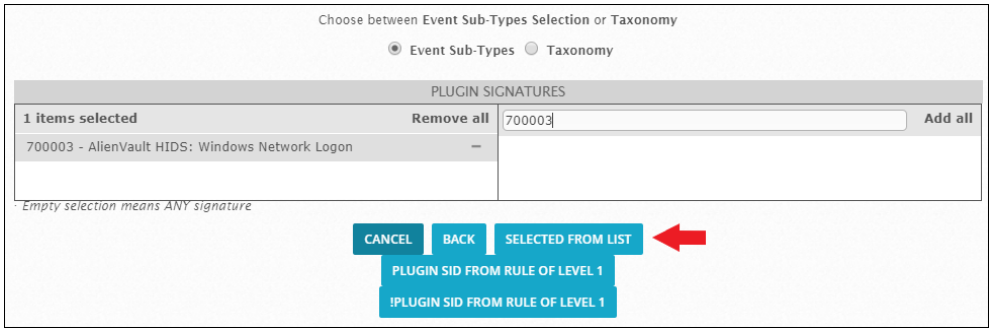


Figura 2.128. Subevento de acceso exitoso

P. Para la parte de configuración de red de este nivel de correlación, se selecciona que solo se tome eventos que tengan como dirección IP destino la misma que se detectó en el primer nivel de correlación como se ve en la Figura 2.129

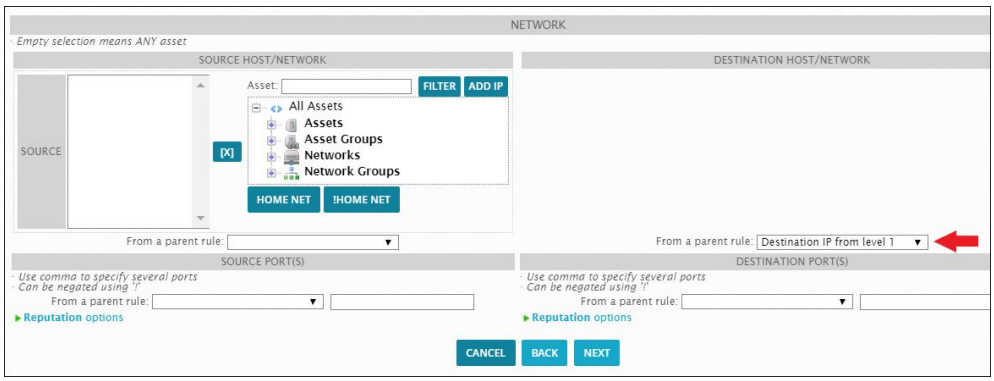


Figura 2.129. Configuración de red IP destino

Q. Como valor del evento de acceso correcto, se establece el valor de 0 como se puede ver en la Figura 2.130 ya que se considera como un falso positivo.

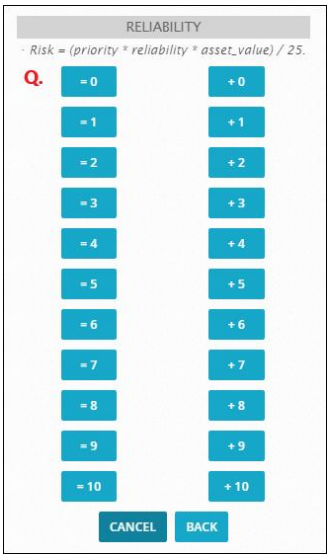


Figura 2.130. Confiabilidad de evento de acceso exitoso

R. Una vez terminada la regla de acceso exitoso, esta aparece como un nivel inferior a la primera que se creó. Se establece el valor de tiempo de correlación en el valor de 20 segundos como se indica en la Figura 2.131.

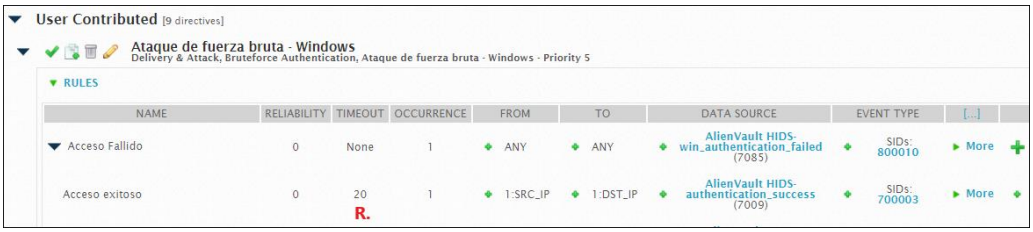


Figura 2.131. Configuración de tiempo Acceso exitoso

S. Luego, se crea la segunda regla correspondiente a la detección de accesos fallidos superiores a 10 con un tiempo de duración de 20 segundos y los mismos subeventos del primer nivel de correlación como se puede ver en la Figura 2.132

Figura 2.132. Regla de accesos fallidos superiores a 10 intentos

T. Se agregan los siguientes niveles, tomando en cuenta los parámetros de tiempo de duración de cada nivel, dirección IP destino y tipo de subeventos como se muestra en la Figura 2.133

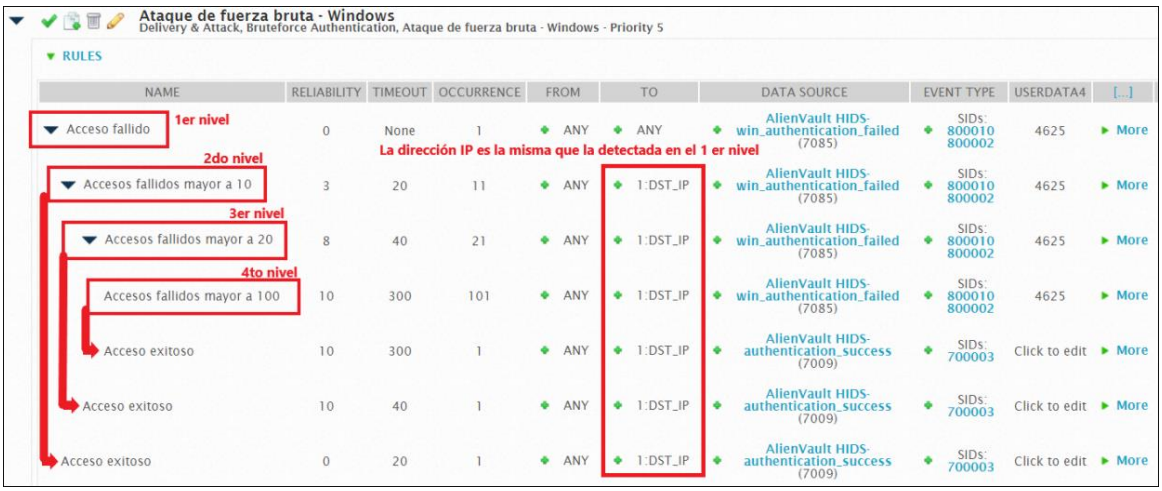


Figura 2.133. Directiva de detección de Ataque de Fuerza bruta Windows

U. Como paso final, es necesario realizar la recarga de las directivas para que estas tomen efecto como se indica en la Figura 2.134

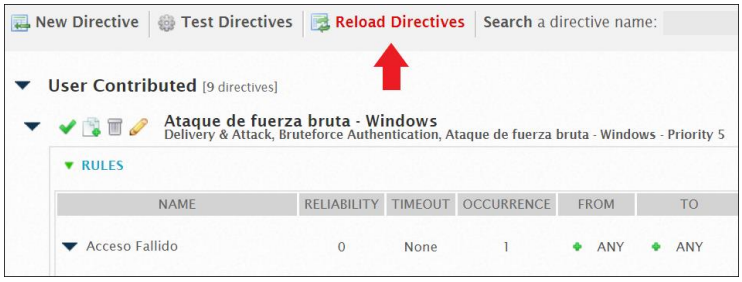


Figura 2.134. Recarga de directivas de correlación

2.7.1.2 Equipos Linux

Se siguió el mismo procedimiento que el hecho en la directiva de detección de ataque de fuerza bruta para Windows 2.7.1.1. La directiva final se la puede ver en la Figura 2.135, se han utilizado los eventos detectados en 2.6.1.2

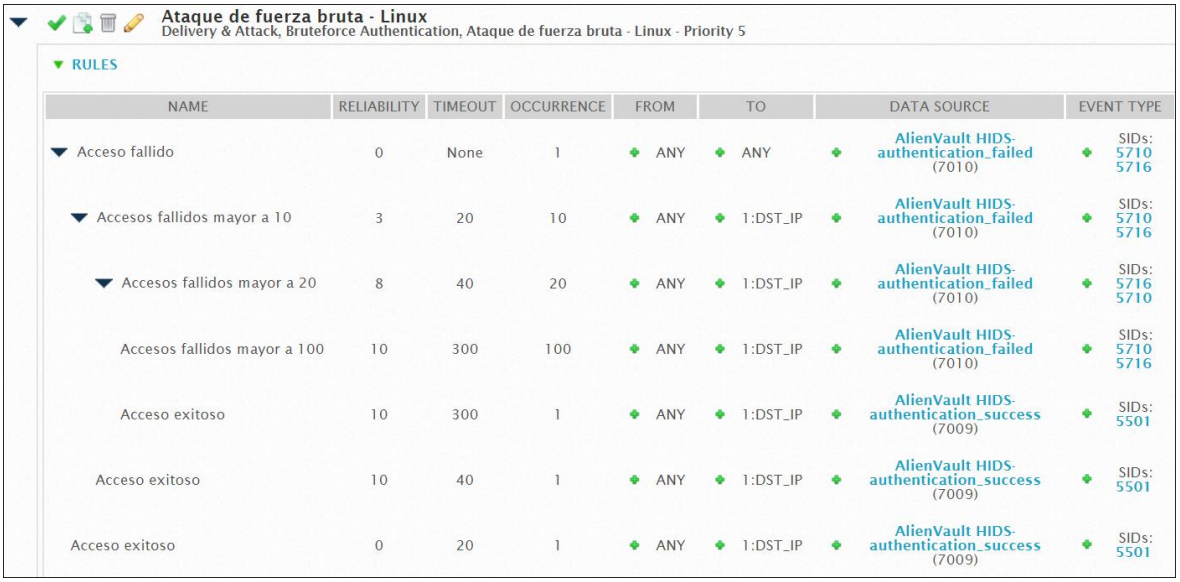


Figura 2.135. Directiva ataque de fuerza bruta - Linux

2.7.1.3 Firewall

Se siguió el mismo procedimiento que el hecho en la directiva de detección de ataque de fuerza bruta para Windows 2.7.1.1. La directiva final se la puede ver en la Figura 2.136, se ha utilizado los eventos detectados en 2.6.1.3

Figura 2.136. Directiva ataque de fuerza bruta – Firewall

El evento de acceso exitoso es el mismo que se genera cuando se genera un cambio de configuración como se vio en 2.6.2.3, por tal motivo se realiza la configuración del campo USERDATA1 para que únicamente se detecte cuando tenga el valor de “CLI” como se ve en la Figura 2.137, con esto se garantiza que el evento sea generado por la consola.

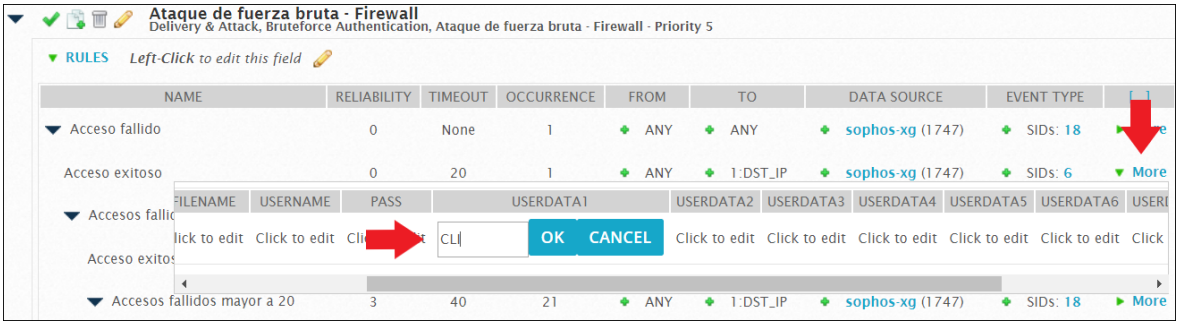


Figura 2.137. Configuración del campo USERDATA1 -CLI

2.7.1.4 Equipo Virtualizador VMware

Se siguió el mismo procedimiento que el hecho en la directiva de detección de ataque de fuerza bruta para Windows 2.7.1.1. La directiva final se la puede ver en la Figura 2.138, se han utilizado los eventos detectados en 2.6.1.4

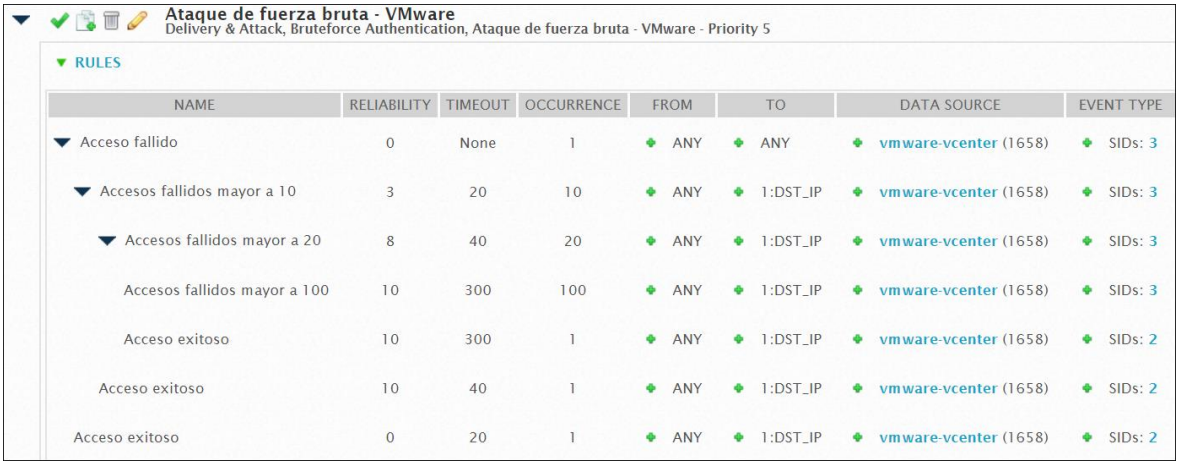


Figura 2.138. Directiva ataque de fuerza bruta –vmware

2.7.2 DETECCIÓN DE CAMBIOS DE CONFIGURACIÓN

2.7.2.1 CREACIÓN DE USUARIOS

2.7.2.1.1 Equipos Windows

Para la creación de la directiva para la detección de cambios de configuración en Windows se siguió el procedimiento de 2.7.1.1 tomando en consideración que la directiva tendrá un nivel de correlación y se usará el evento detectado en 2.6.2.1 como se muestra en la Figura 2.139

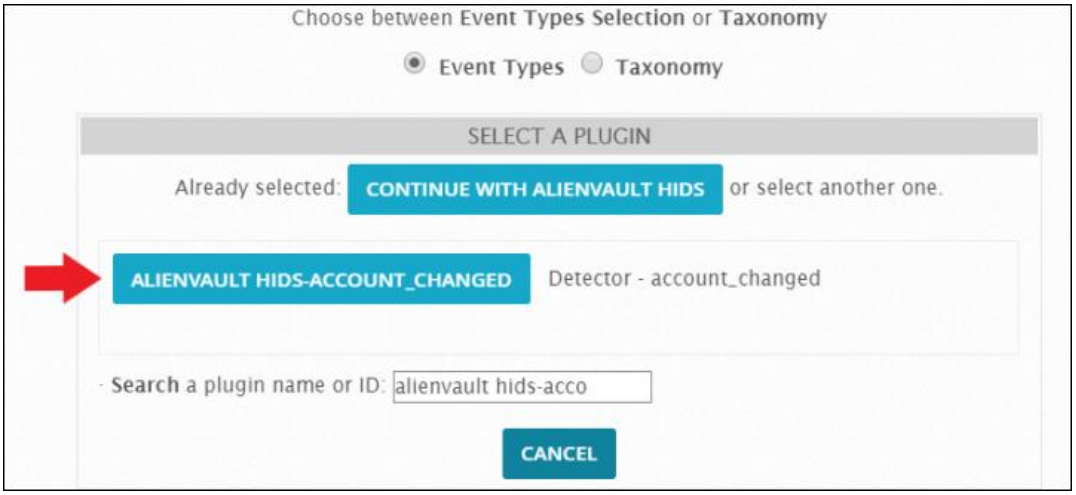


Figura 2.139. Evento detección de modificación de configuración

Para el evento se seleccionó el 18110, correspondiente a la creación o habilitación de una cuenta como se ve en la Figura 2.140

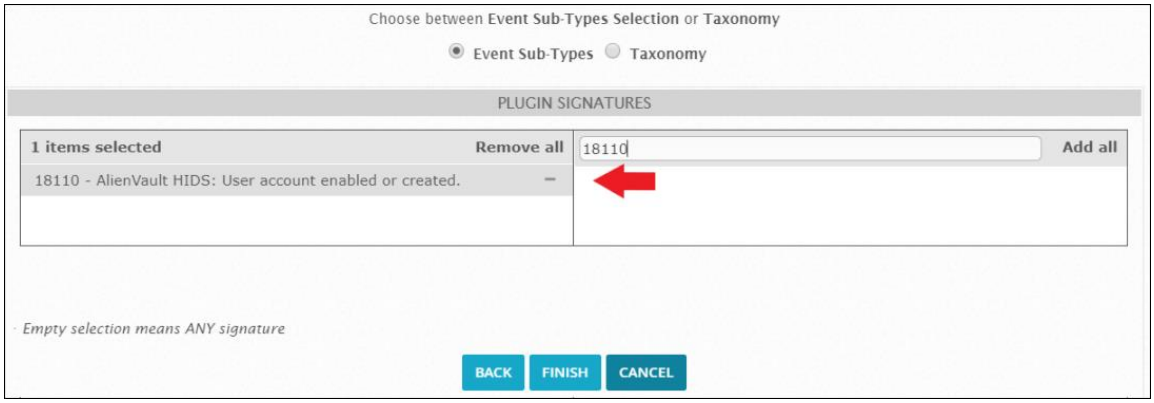


Figura 2.140. Evento de creación de cuenta

De acuerdo con el diseño de la directiva definida en 2.4.2.1, es necesario generar 2 tipos de alarmas basado en el usuario que creó al nuevo usuario. Una alarma debe tener valor de 2 cuando el usuario que creó al nuevo usuario es del grupo de administradores y debe tener un valor de 8 cuado no pertenezca al grupo. Para esto fue necesario crear 2 directivas, una va a detectar si el usuario se encuentra en el listado de administradores como se ve en la Figura 2.141, añadiendo cada uno de los usuarios administradores separados por comas en el campo de USERNAME.

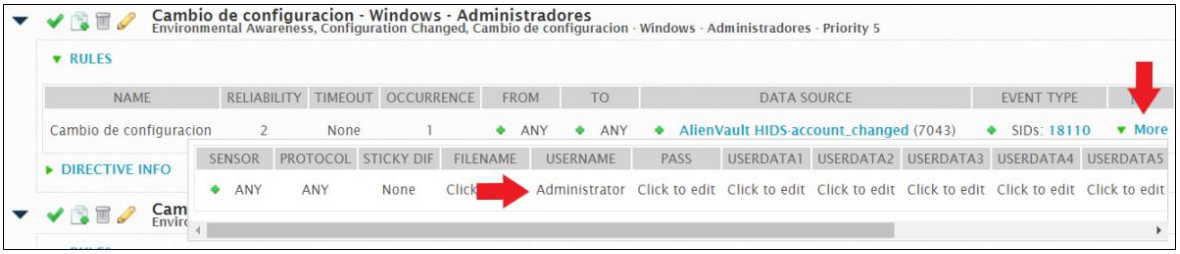


Figura 2.141. Listado de usuarios administradores

Se usa la condición de negación (!) para declarar que, si se usa un usuario diferente a los listados, se genere una alarma con valor de 8 como se muestra en la Figura 2.142

Figura 2.142. Directiva detección de usuario desde un usuario que o es administrador

2.7.2.1.2 Equipos Linux

Para la creación de la directiva para la detección de cambios de configuración en Linux, se siguió el procedimiento para crear directivas de 2.7.1.1 tomando en consideración que la directiva tendrá un nivel de correlación y se usará el evento detectado en 2.6.2.2 como se muestra en la Figura 2.143

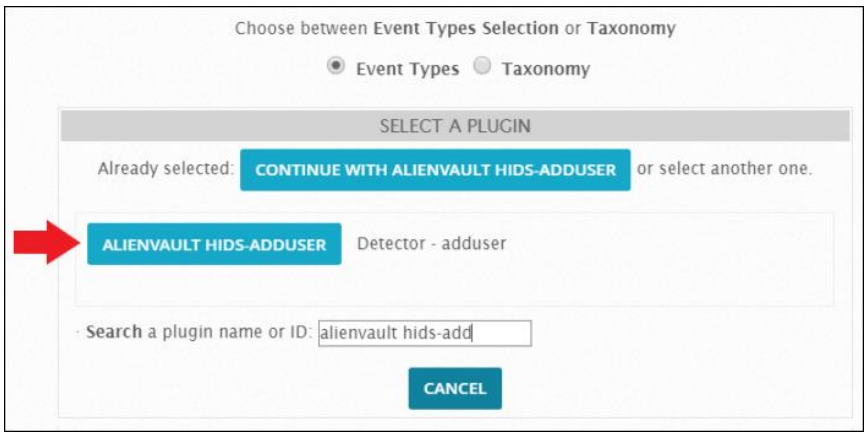


Figura 2.143. Evento creación de usuario - Linux

Para la detección de creación de usuarios, se seleccionó el subevento 5902, correspondiente a la creación de una cuenta como se ve en la Figura 2.144

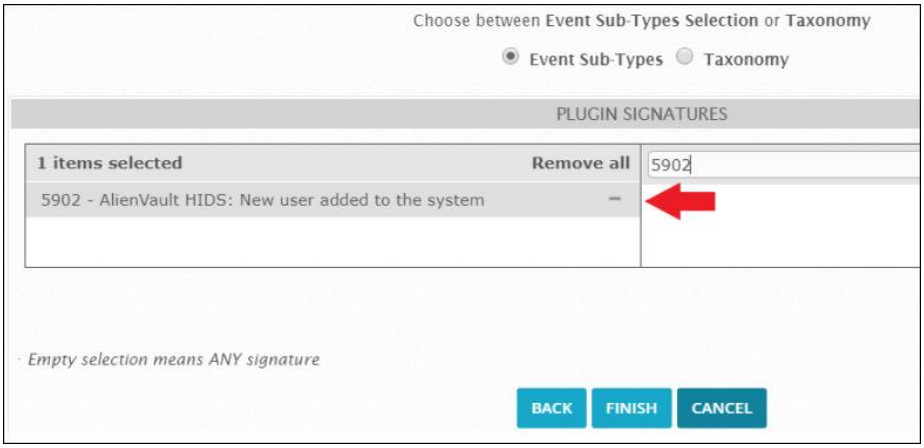


Figura 2.144. Evento de creación de cuenta

De acuerdo con el diseño de la directiva definida en 2.4.2.1, es necesario generar 2 tipos de alarmas basado en el usuario que creó al nuevo usuario. Sin embargo, en los eventos no hay un campo específico que permita ser utilizado para este fin, por lo que se crea una sola directiva con el valor de riesgo de 8 como se indica en la Figura 2.145

Figura 2.145. Directiva detección cambio de configuración Linux

2.7.2.1.3 Firewall

Para la creación de la directiva para la detección de cambios de configuración en el firewall Sophos, se siguió el procedimiento para crear directivas de 2.7.1.1 tomando en consideración que la directiva tendrá un nivel de correlación y se usará el evento detectado en 2.6.2.3 como se muestra en la Figura 2.146

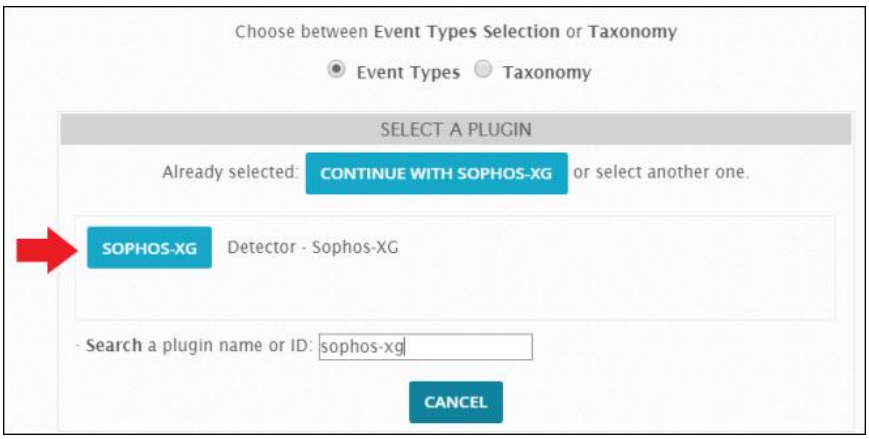


Figura 2.146. Evento creación de usuario – Firewall

Para la detección de creación de usuarios, se seleccionó el subevento 6, correspondiente al detectado en la sección 2.6.2.3, correspondiente a la creación de una cuenta como se ve en la Figura 2.147

Figura 2.147. Evento de creación de cuenta

De acuerdo con el diseño de la directiva definida en 2.4.2.1, es necesario generar 2 tipos de alarmas basado en el usuario que creó al nuevo usuario. Sin embargo, en los eventos no hay un campo específico que permita ser utilizado para este fin, por lo que se crea una sola directiva con el valor de riesgo de 8 como se indica en la Figura 2.148

Figura 2.148. Directiva detección cambio de configuración Firewall

2.7.2.1.4 Equipo Virtualizador VMware

Para la creación de la directiva para la detección de cambios de configuración en VMware, se siguió el procedimiento para crear directivas de 2.7.1.1 tomando en consideración que la directiva tendrá un nivel de correlación y se usará el evento detectado en 2.6.2.4 como se muestra en la Figura 2.149

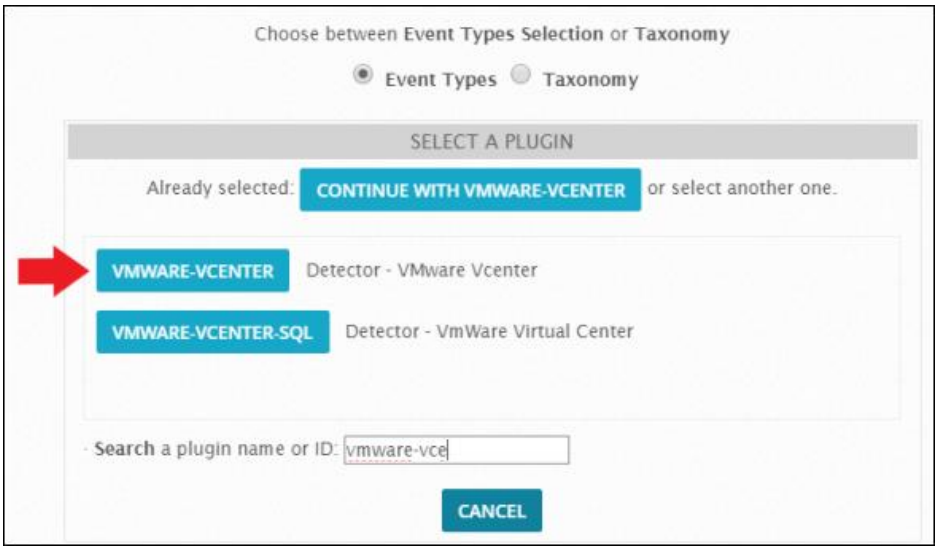


Figura 2.149. Evento creación de usuario – VMware

Para la detección de creación de usuarios, se seleccionó el subevento 1999999999, correspondiente al detectado en la sección2.6.2.4 como se ve en la Figura 2.147

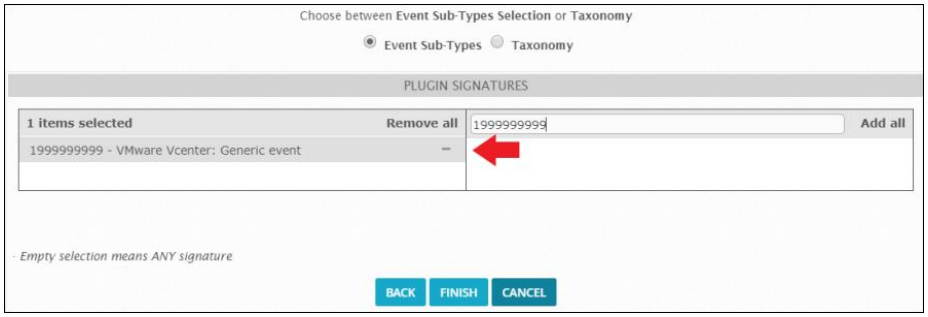


Figura 2.150. Evento de creación de cuenta

De acuerdo con el diseño de la directiva definida en 2.4.2.1, es necesario generar 2 tipos de alarmas basado en el usuario que creó al nuevo usuario. Sin embargo, en los eventos no hay un campo específico que permita ser utilizado para este fin, por lo que se crea una sola directiva con el valor de riesgo de 8 como se indica en la Figura 2.151 y para que este sea diferenciado a otros eventos genéricos se añade en el campo USERDATA1 el texto "passwd" que representa la creación de nuevo usuario.

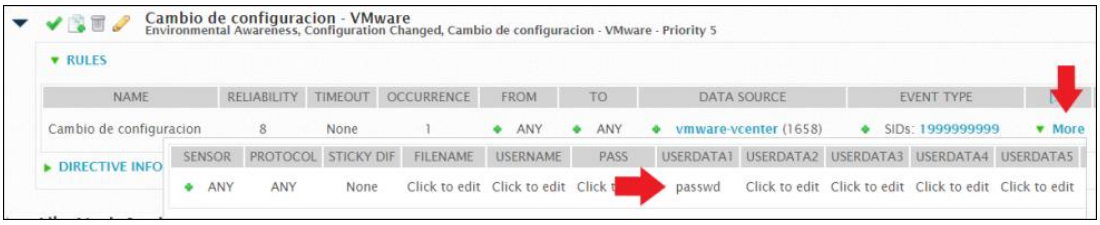


Figura 2.151. Directiva detección cambio de configuración VMware

2.7.2.2 MODIFICACIÓN DE ARCHIVOS

Para la creación de la directiva para la detección de modificación de archivos, se siguió el procedimiento para crear directivas de 2.7.1.1 tomando en consideración que la directiva tendrá un nivel de correlación. Se selecciona el plugin "AlienVault hids-syscheck" como se indica en la Figura 2.152

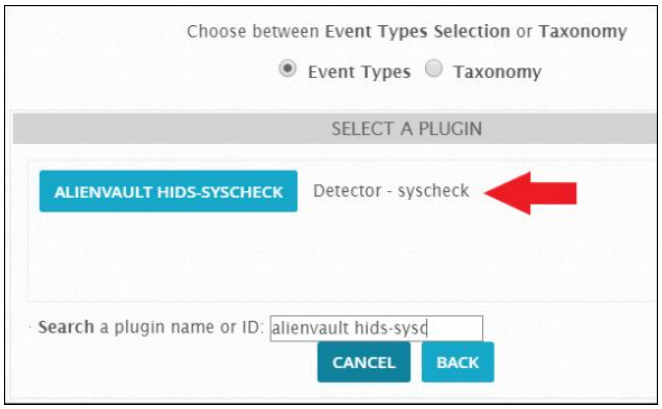


Figura 2.152. Plugin detector de integridad

Para la detección de cambios de integridad, se seleccionó el subevento 550 correspondiente a cambios detectados de integridad como se indica en la Figura 2.153

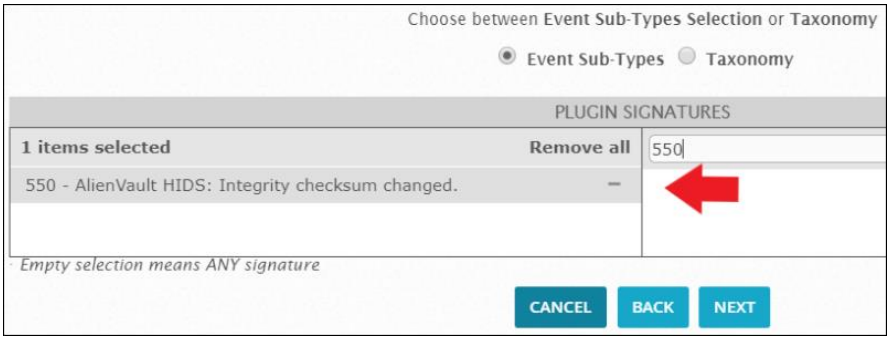


Figura 2.153. Detección de cambios de integridad

2.7.3 DETECCIÓN DE CONEXIONES HACIA IP MALICIOSA

Para la creación de la directiva para la detección de conexión hacia IP detectadas como maliciosas en el firewall Sophos XG se utiliza el plugin de Sophos como se indica en la Figura 2.154, y se usa el subevento 12, correspondiente a eventos conexiones permitidas como se puede ver en la Figura 2.155

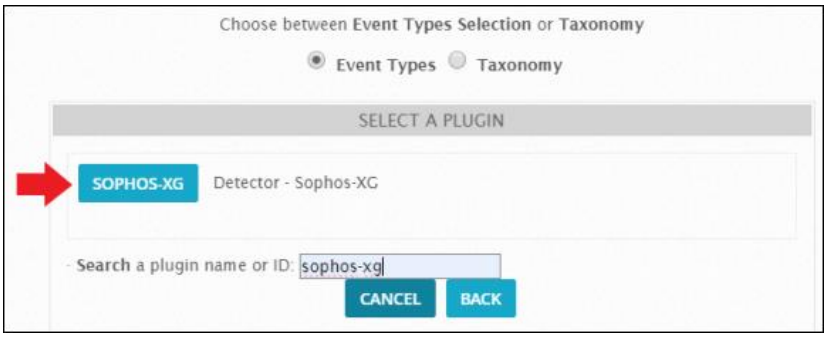


Figura 2.154. Plugin Sophos XG

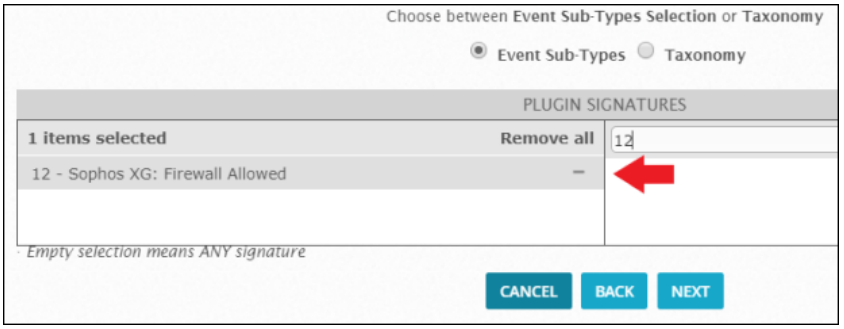


Figura 2.155. Evento de conexiones permitidas

En la configuración de parámetros de red en la regla, se marca la opción de verificar la reputación en OTX a “YES” como se indica en la , y se selecciona como parámetros de

prioridad y confiabilidad de la reputación de la IP destino como alertamiento desde los valores de 1 como se puede ver en la Figura 2.156 y la alarma generada va a tener una confiabilidad de 10 como se ve en la Figura 2.157

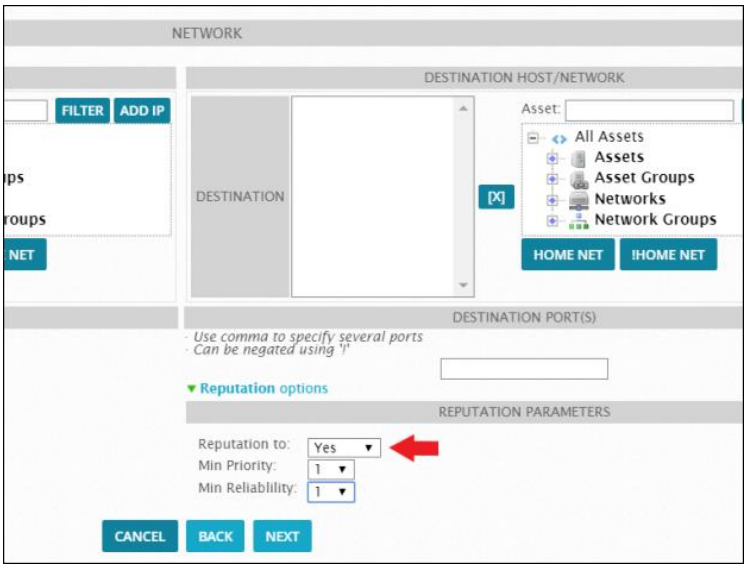


Figura 2.156. Verificación de reputación de IP destino en OTX

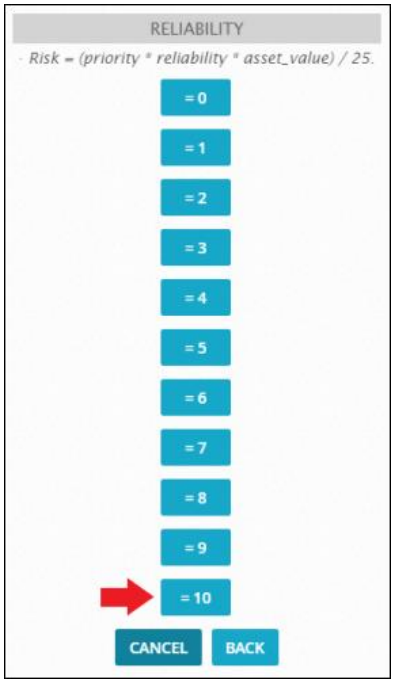


Figura 2.157. Confiabilidad 10

En la Figura 2.158 se puede visualizar la directiva final para el propósito de generar alarmas cuando una IP interna establezca comunicación hacia una dirección IP maliciosa.

Figura 2.158. Directiva detección de conexión permitida hacia IP maliciosa

3. RESULTADOS Y DISCUSIÓN

3.1 PRUEBAS DE ACCESO PARA DETECCIÓN DE ATAQUES DE FUERZA BRUTA

Para las pruebas de ataque de fuerza bruta se utilizó la herramienta hydra, la cual viene preinstalada en la distribución de pentesting Kali Linux, sin embargo, el uso de esta herramienta para efectuar el ataque al equipo Windows no pudo ser utilizada porque no tiene compatibilidad para sistemas Windows 2016

3.1.1 EQUIPOS WINDOWS

Se realizó una simulación de ataque manual, teniendo en cuenta la cantidad de accesos fallidos necesarios a efectuar para que el comportamiento sea similar al de una herramienta automatizada. Se efectuó como primer escenario, un ataque de fuerza bruta no exitoso con la cantidad de 22 eventos, dando a lugar una alarma de riesgo 3 como se indica en la Figura 3.1

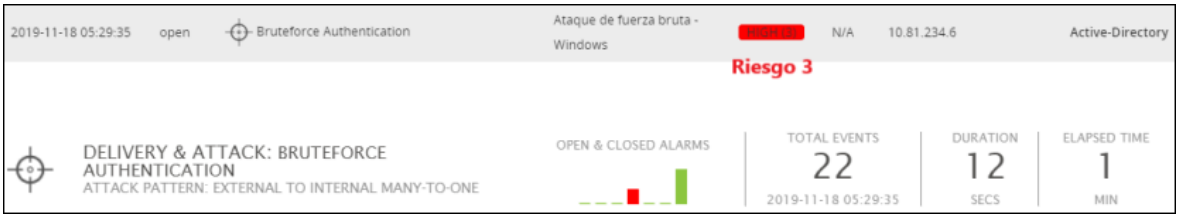


Figura 3.1. Windows - Ataque de fuerza bruta no exitoso

Luego se realizó un nuevo escenario de ataque en el cual se introdujeron las credenciales correctas de acceso para la simulación de un ataque de fuerza bruta exitoso, lo cual genera una alarma de riesgo 4 como se puede ver en la Figura 3.2

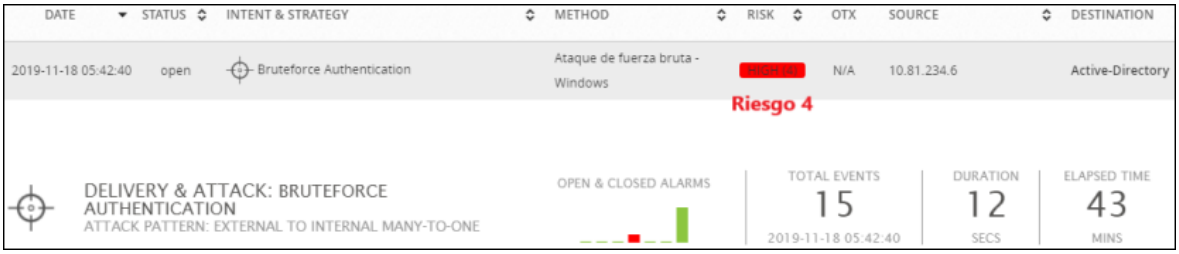


Figura 3.2. Windows - Ataque de fuerza bruta exitoso

La alarma que se observó en la Figura 3.2, tiene como nivel de riesgo 4 y no 10 como se había establecido en el diseño de la directiva. Se verificó el inconveniente y se observa que el valor de activo que OSSIM está estableciendo al activo es de 2 como se observa en la Figura 3.3.

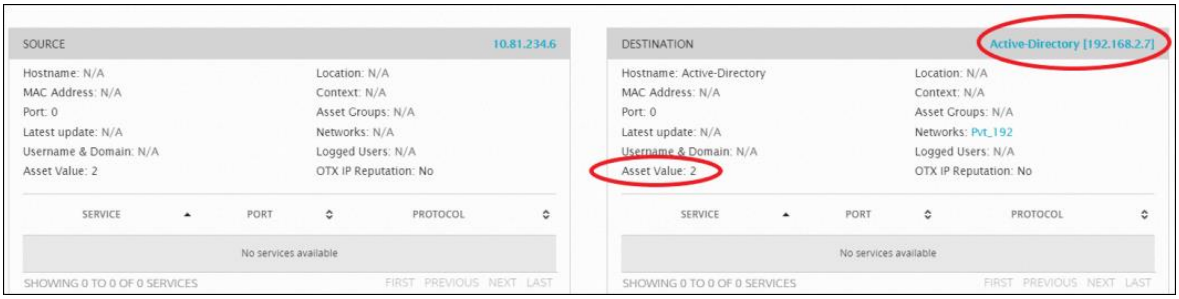


Figura 3.3. Windows - Valor del activo

Para solventar este inconveniente, se ha creado un segmento de red en el listado de activos y se ha marcado que todos los activos van a tener el valor de 5 como se indica en la Figura 3.4

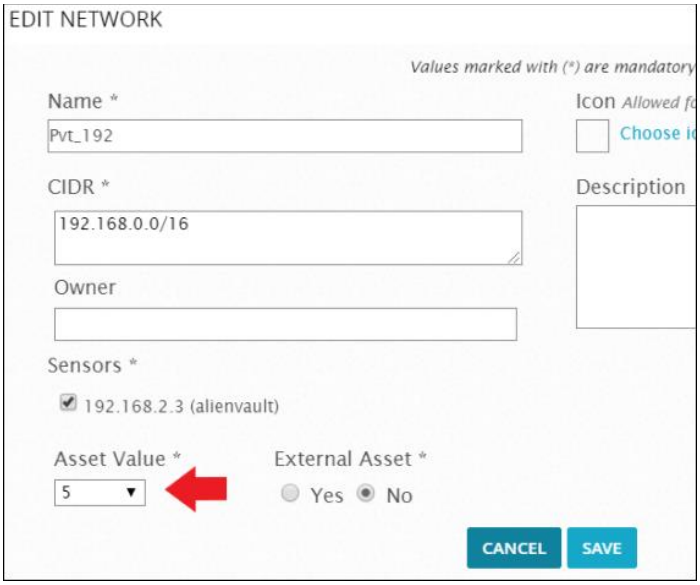


Figura 3.4. Creación de subred y modificación del valor

En la Figura 3.5, se puede observar como la alarma se encuentra con el valor correcto.

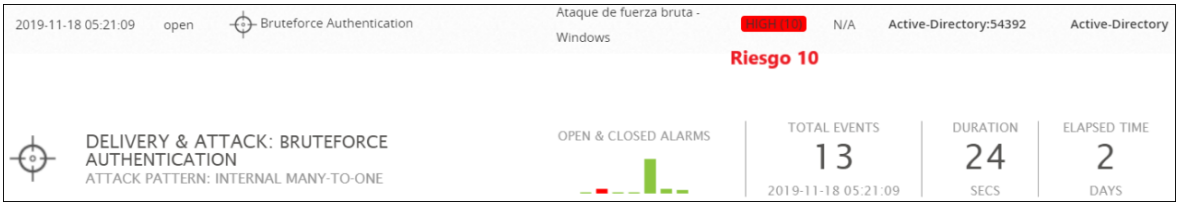


Figura 3.5. Windows - Alarma de acceso exitoso con riesgo 10

En la alarma de ataque de fuerza bruta exitoso se puede ver la detección del evento de acceso exitoso como se indica en la Figura 3.6

Figura 3.6. Windows - Detección de acceso exitoso

3.1.2 EQUIPOS LINUX

En la Figura 3.7 se indica el ataque realizado con la herramienta “hydra” hacia el activo MicroDM (192.168.2.3). Este ataque simula 20 intentos fallidos, representando un ataque no exitoso.

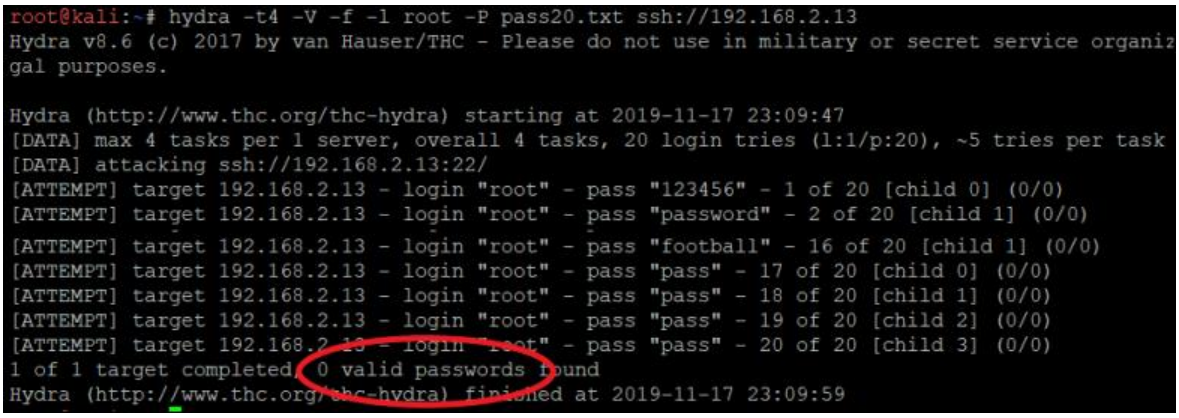


Figura 3.7. Linux - Ataque de fuerza bruta no exitoso

Después de concluir el ataque, se generó en OSSIM la alarma “Ataque de fuerza bruta - Linux” con un riesgo de 3 como se observa en la Figura 3.8, correspondiente a un ataque no exitoso con un número de intentos menor a 20.

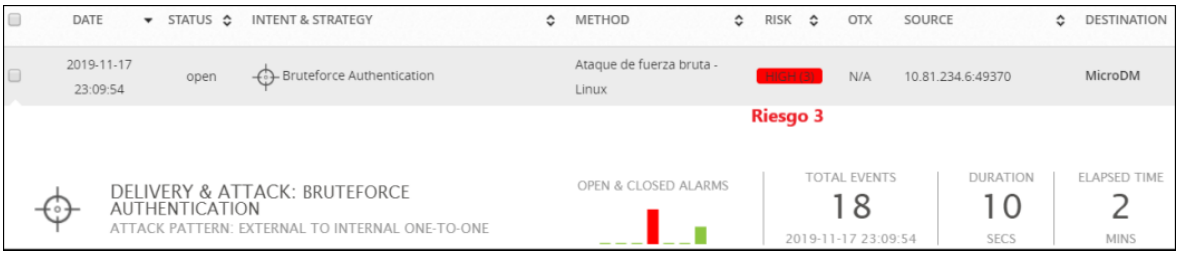


Figura 3.8. Linux - Alarma de ataque de fuerza bruta no exitoso

A continuación, se realizó un nuevo ataque en el cual se añade en el listado de contraseñas a utilizar la credencial correcta para simular un ataque de fuerza bruta exitoso muestra en la Figura 3.9.

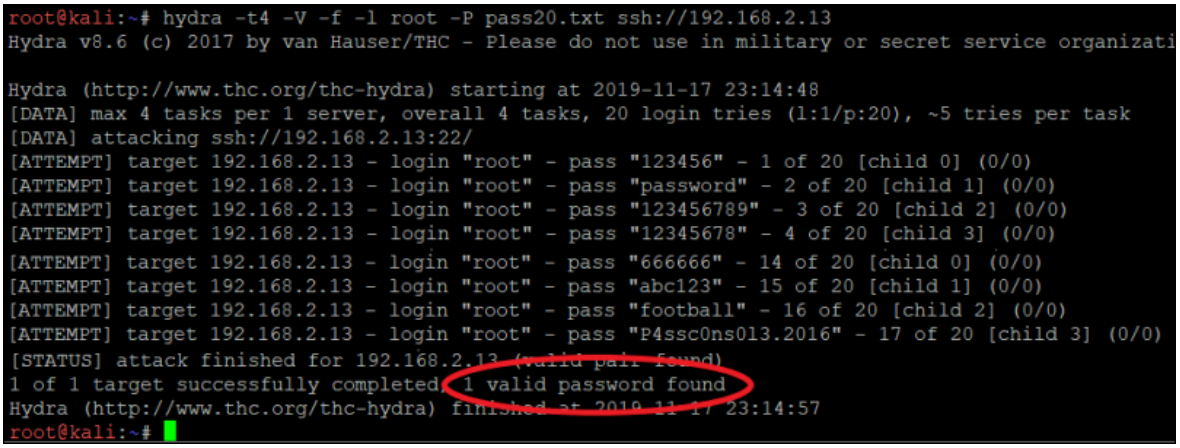


Figura 3.9. Linux - Ataque de fuerza bruta exitoso

En la Figura 3.10 se puede ver la generación de la alarma correspondiente a la directiva de ataque de fuerza bruta a un sistema Linux con un riesgo de 10, debido a que hubo un acceso exitoso durante el ataque como se indica en la Figura 3.11

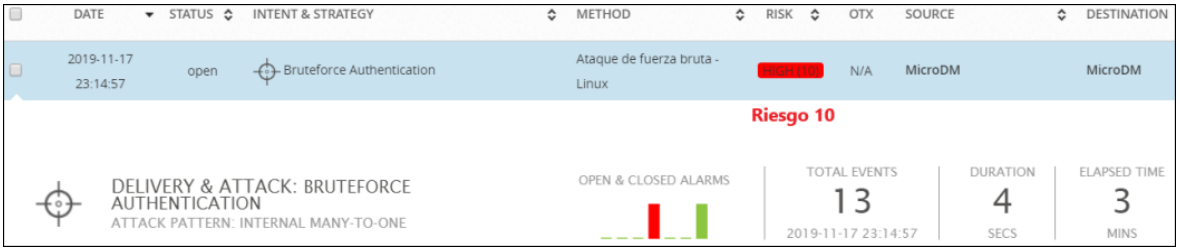


Figura 3.10. Linux - Alarma de ataque de fuerza bruta exitoso

Figura 3.11. Linux - Detección de acceso exitoso

3.1.3 FIREWALL

En la Figura 3.12 se indica el ataque realizado con la herramienta “hydra” hacia el equipo firewall. Este ejercicio simula un ataque no exitoso.

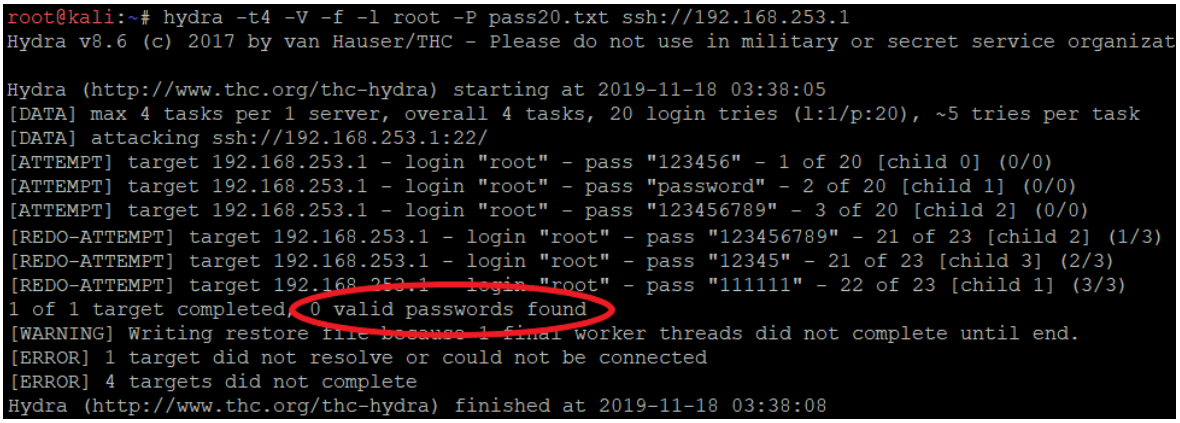


Figura 3.12. Firewall - Ataque de fuerza bruta no exitoso

Después de concluir el ataque, se observa en OSSIM la generación de la alarma “Ataque de fuerza bruta - Firewall” con un riesgo de 3 como se observa en la Figura 3.13, correspondiente a un ataque no exitoso.

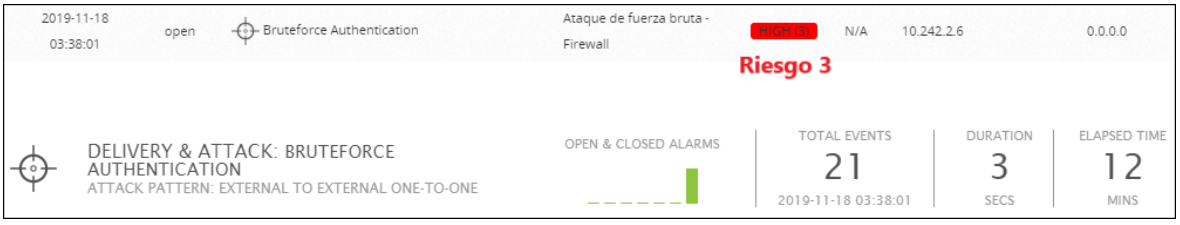


Figura 3.13. Firewall - Alarma de ataque de fuerza bruta no exitoso

A continuación, se realizó un nuevo ataque en el cual se añade en el listado de contraseñas a utilizar, la credencial correcta para simular un ataque de fuerza bruta exitoso muestra en la Figura 3.14

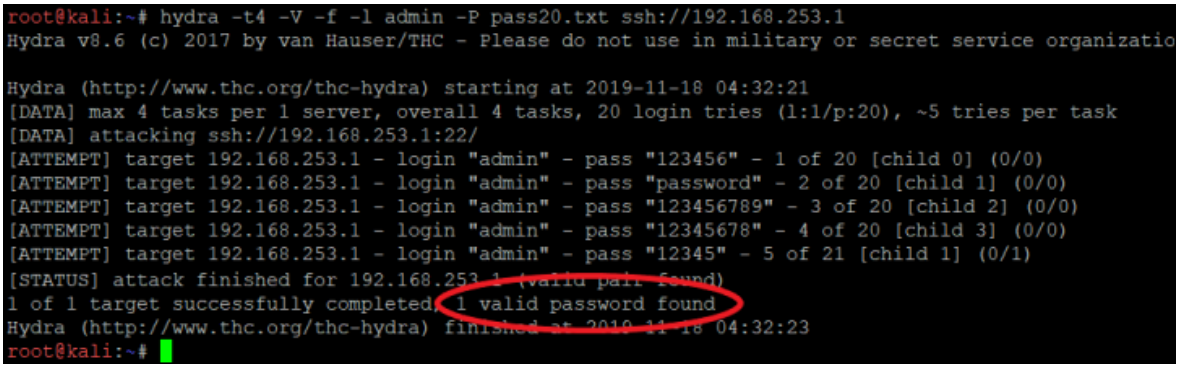


Figura 3.14. Firewall - Ataque de fuerza bruta exitoso

En la Figura 3.15 se puede ver la generación de la alarma correspondiente a la directiva de ataque de fuerza bruta hacia el equipo firewall Sophos XG con un riesgo de 10, debido a que hubo un acceso exitoso durante el ataque como se indica en la Figura 3.16

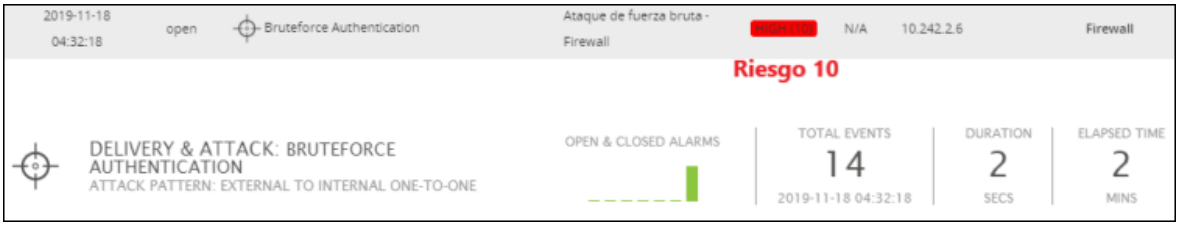


Figura 3.15. Firewall - Alarma de ataque de fuerza bruta exitosos

Figura 3.16. Firewall - Detección de acceso exitoso

3.1.4 EQUIPO VIRTUALIZADOR VMWARE

En la Figura 3.17 se indica el ataque realizado con la herramienta “hydra” hacia el equipo virtualizador VMware ESXi. Este ejercicio simula un ataque no exitoso.

```
root@kali:~# hydra -t4 -V -f -l root -P pass20.txt ssh://192.168.2.2
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service or

Hydra (http://www.thc.org/thc-hydra) starting at 2019-11-18 00:38:21
[DATA] max 4 tasks per 1 server, overall 4 tasks, 20 login tries (l:1/p:20), ~5 tries per
[DATA] attacking ssh://192.168.2.2:22/
[ATTEMPT] target 192.168.2.2 - login "root" - pass "123456" - 1 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.2.2 - login "root" - pass "password" - 2 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.2.2 - login "root" - pass "123456789" - 3 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.2.2 - login "root" - pass "12345678" - 4 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.2.2 - login "root" - pass "Pass" - 17 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.2.2 - login "root" - pass "pass" - 18 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.2.2 - login "root" - pass "pass" - 19 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.2.2 - login "root" - pass "pass" - 20 of 20 [child 0] (0/0)
1 of 1 target completed, 0 valid passwords found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 4 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2019-11-18 00:38:34
root@kali:~#
```

Figura 3.17. Linux - Ataque de fuerza bruta no exitoso

Después de concluir el ataque, se generó en OSSIM la alarma correspondiente a un “Ataque de fuerza bruta - VMware” con un riesgo de 3 como se observa en la Figura 3.18, debido a que hubieron menos de 20 eventos de acceso fallidos y ningún acceso exitoso.

Figura 3.18. Linux - Alarma de ataque de fuerza bruta no exitoso

Se realizó un nuevo ataque, en el cual se añade la contraseña correcta en el listado de contraseña a utilizar, dando como resultado un ataque exitoso como se muestra en la Figura 3.19

```
root@kali:~# hydra -t4 -V -f -l root -P pass20.txt ssh://192.168.2.2
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service o

Hydra (http://www.thc.org/thc-hydra) starting at 2019-11-18 00:49:31
[DATA] max 4 tasks per 1 server, overall 4 tasks, 20 login tries (l:1/p:20), ~5 tries per
[DATA] attacking ssh://192.168.2.2:22/
[ATTEMPT] target 192.168.2.2 - login "root" - pass "123456" - 1 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.2.2 - login "root" - pass "password" - 2 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.2.2 - login "root" - pass "123456789" - 3 of 20 [child 2] (0/0)
[ATTEMPT] target 192.168.2.2 - login "root" - pass "12345678" - 4 of 20 [child 3] (0/0)
[ATTEMPT] target 192.168.2.2 - login "root" - pass "12345" - 5 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.2.2 - login "root" - pass "111111" - 6 of 20 [child 3] (0/0)
[STATUS] attack finished for 192.168.2.2 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-11-18 00:49:40
root@kali:~#
```

Figura 3.19. Linux - Ataque de fuerza bruta exitoso

En la Figura 3.20 se puede ver la generación de la alarma correspondiente a un ataque de fuerza bruta en VMware con un riesgo de 10, debido a que hubo un acceso exitoso durante el ataque como se indica en la Figura 3.21

Figura 3.20. Linux - Alarma de ataque de fuerza bruta exitoso

Figura 3.21. Linux - Detección de acceso exitoso

3.2 PRUEBAS DE MODIFICACIÓN – CREACIÓN DE USUARIO

En este caso se realiza la creación de un usuario en cada equipo para la generación de la respectiva alarma de notificación en OSSIM.

3.2.1 EQUIPOS WINDOWS

Para este activo se elaboraron 2 directivas, las cuales indicarán si la creación del nuevo usuario lo hizo un usuario que se encuentra listada como administrador o una persona ajena a este grupo. Este listado se lo añadió en la directiva correspondiente utilizando el campo USERNAME como filtro.

3.2.1.1 Creación de usuario desde cuenta listada como administrador

Se realiza la creación del usuario “prueba” en el equipo Windows como se indica en la Figura 3.22. Adicionalmente, se añade a este nuevo usuario al grupo administradores como se puede ver en la Figura 3.23, lo que permitirá comprobar la directiva que detectará la creación de nuevos usuarios a través de una cuenta que no esté listada como administrador en la directiva respectiva.

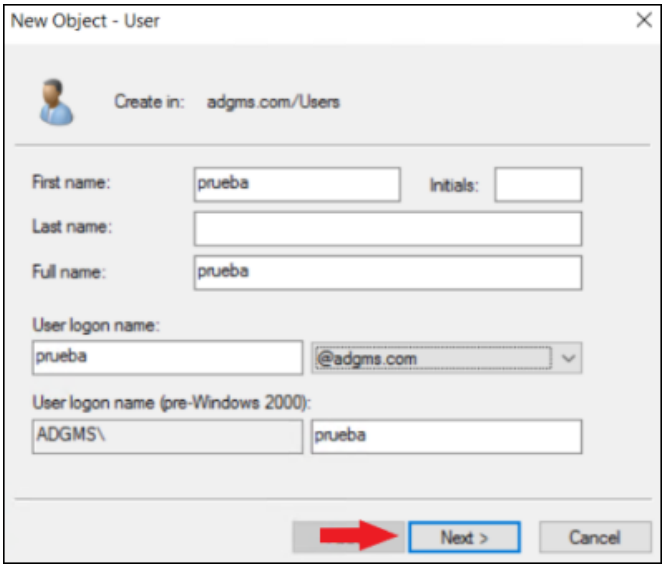


Figura 3.22. Creación del usuario prueba

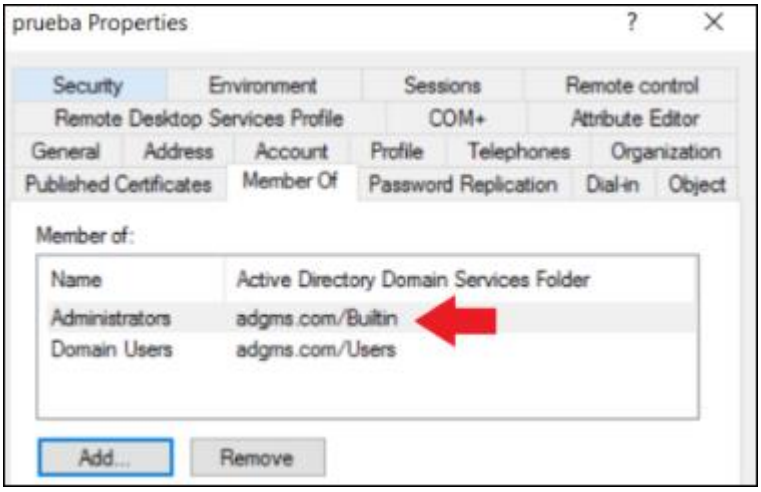


Figura 3.23. Agregación del usuario prueba al grupo de administradores

Una vez que se terminó de crear el usuario “prueba”, se observa en OSSIM la generación de la alarma correspondiente al cambio de configuración en Windows con una cuenta Administrador con riesgo 2 como se ve en la

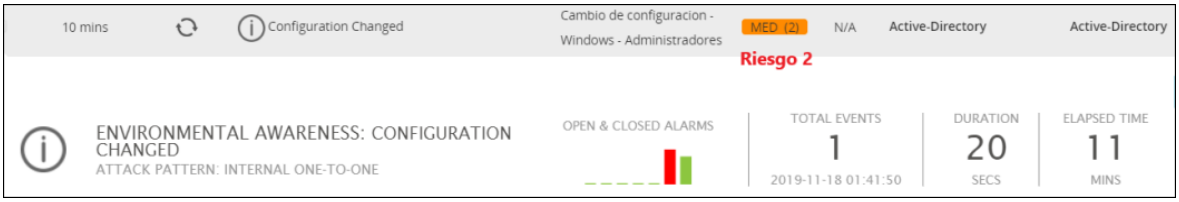


Figura 3.24. Alarma cambio de configuración desde Administrador

En la Figura 3.25 se puede ver el evento correspondiente a la creación del usuario “prueba” desde la cuenta “Administrator”, la cual se encuentra listada en la directiva como cuenta de Administradores.

Figura 3.25. Detección de evento de adición de usuario prueba con cuenta de administrador

3.2.1.2 Creación de usuario desde cuenta no listada como administrador

Utilizando la cuenta “prueba” creada en 3.2.1.1 se realiza la creación del usuario “generico”, ya que el usuario utilizado no está en el listado de OSSIM, se genera la alarma de la Figura 3.26, la cual tiene un riesgo de 8 porque en el evento de creación de usuario se detecta que el usuario que realizó la creación del nuevo usuario no corresponde a uno que se encuentre en el listado de OSSIM, en este caso se utilizó el usuario “prueba” como se muestra en la Figura 3.27

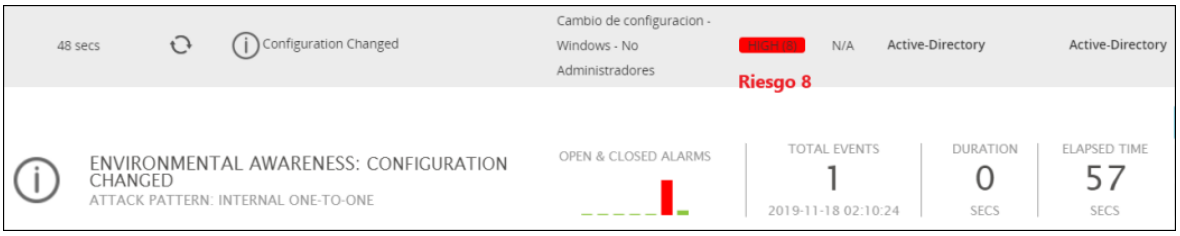


Figura 3.26. Alarma creación de usuario utilizando cuenta que no está listada como administrador

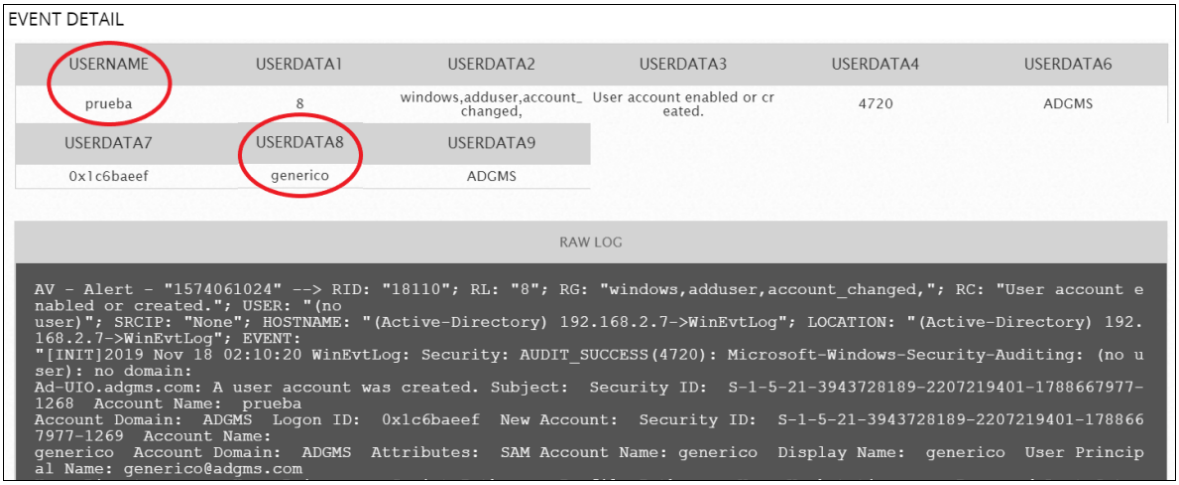


Figura 3.27. Detección de creación de usuario a través la cuenta prueba

3.2.2 EQUIPOS LINUX

En la Figura 3.28 se puede ver la alarma generada en OSSIM con el riesgo de 8 cuando se realizó la creación del usuario “prueba”. La detección del evento se muestra en la Figura 3.29

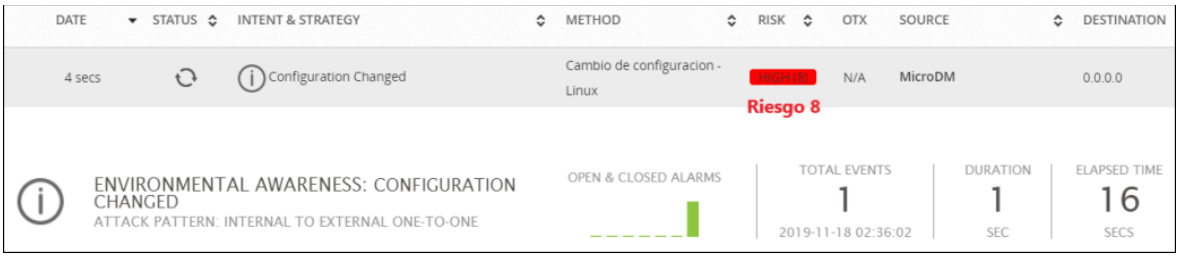


Figura 3.28. Linux - Creación del usuario prueba

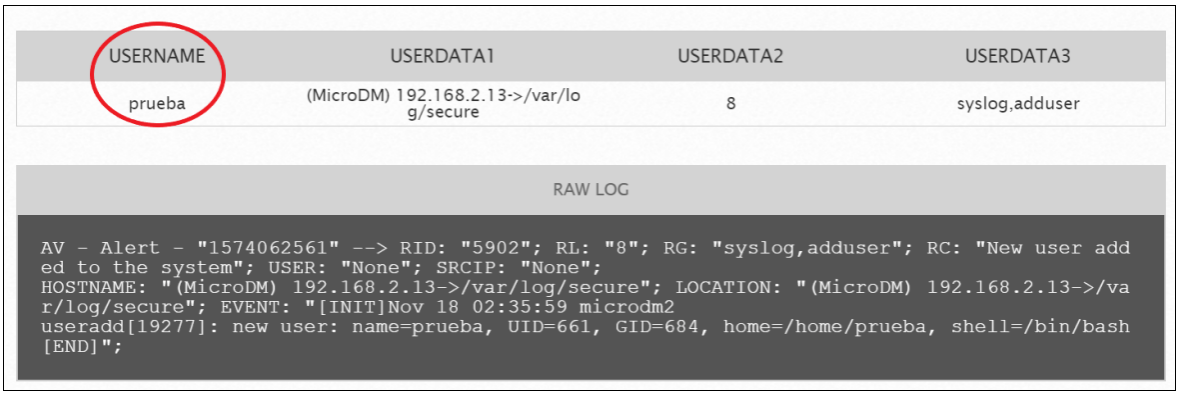


Figura 3.29. Detección del evento de creación del usuario prueba

3.2.3 FIREWALL

En el equipo firewall Sophos XG se realiza la creación del usuario “prueba” como se indica en la Figura 3.30. Una vez realizada la creación, se observa la generación de la alarma de riesgo 8 como se indica en la Figura 3.31

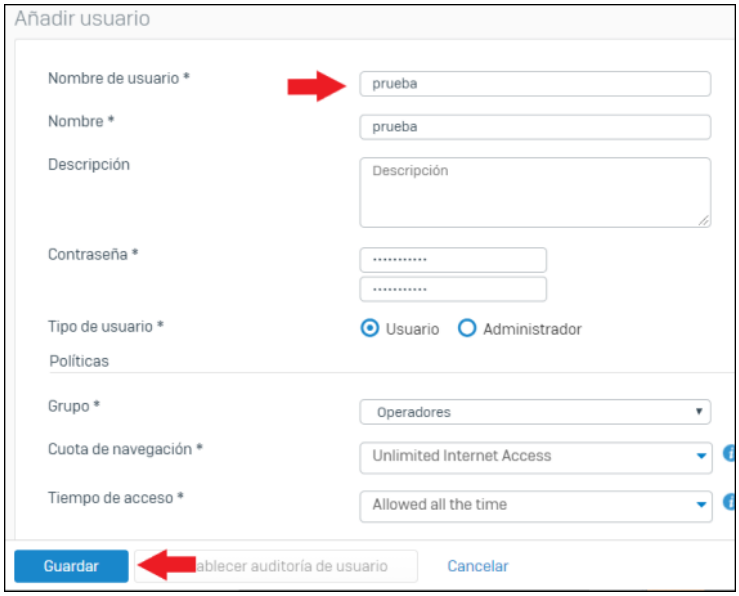


Figura 3.30. Firewall - Creación del usuario prueba

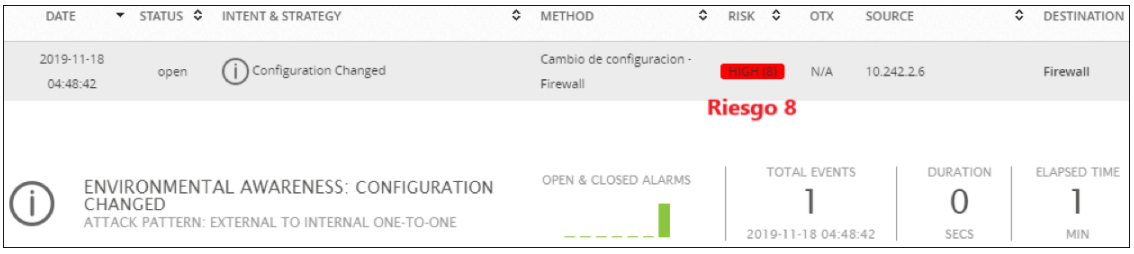


Figura 3.31. Firewall - Alarma creación del usuario

Como se indica en la Figura 3.32, la detección del evento de creación de usuario es correcta.

Figura 3.32. Firewall - Detección del evento de creación del usuario prueba

3.2.4 EQUIPO VIRTUALIZADOR VMWARE

En el equipo VMWare ESXi 5.1 se realiza la creación del usuario “prueba” como se indica en la Figura 3.33. Una vez realizada la creación, se observa la generación de la alarma de riesgo 8 como se indica en la Figura 3.34

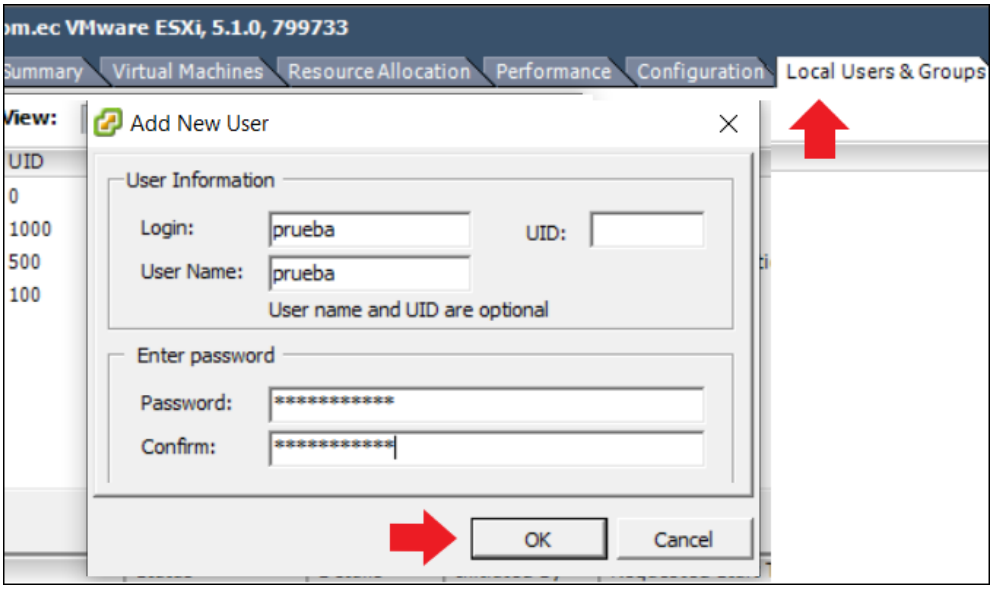


Figura 3.33. VMware - Creación de usuario prueba

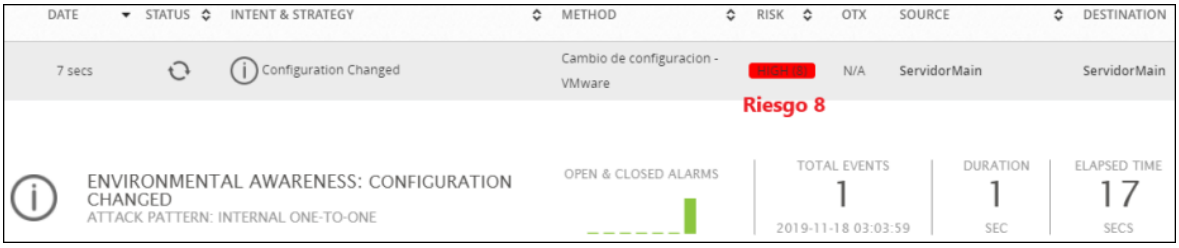


Figura 3.34. VMware - Alarma de creación de usuario prueba

Como se indica en la Figura 3.35, la detección del evento de creación de usuario es correcta utilizando el campo USERDATA1 como filtro para este tipo de evento.

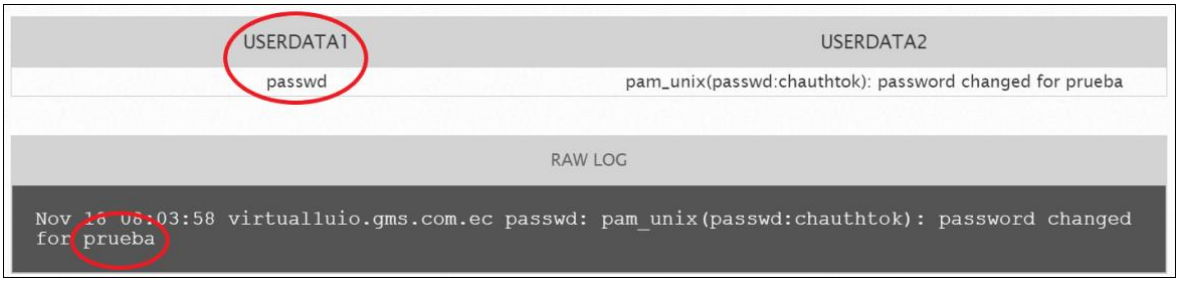


Figura 3.35. VMware - Detección del evento creación de usuario prueba}

3.3 PRUEBAS DE MODIFICACIÓN – INTEGRIDAD DE ARCHIVOS

Se realiza la modificación en el archivo C:\Windows\System32\drivers\etc\hosts como se indica en la Figura 3.36, y con ello se obtiene la detección del evento de cambio de integridad de archivos “AlienVault HIDS: Integrity checksum changed” como se observa en la Figura 3.37

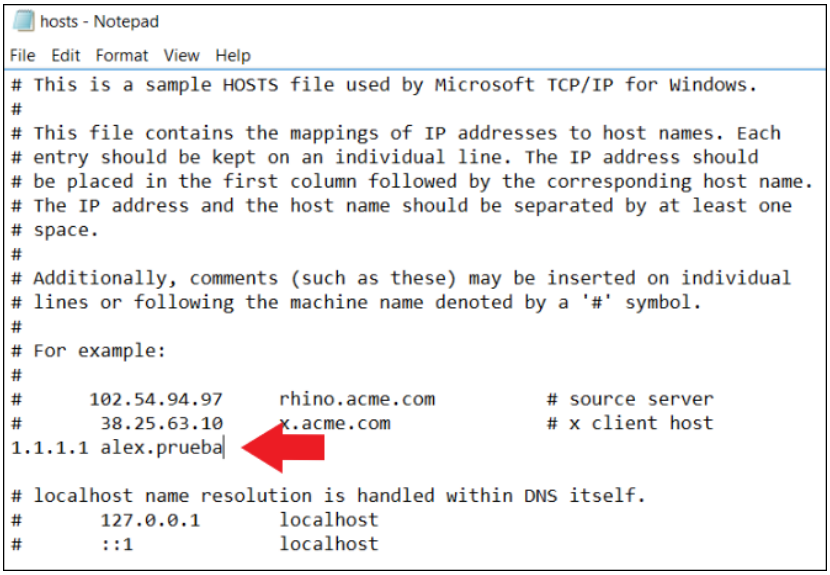


Figura 3.36. Modificación de archivo C:\Windows\System32 \drivers\etc\hosts

Figura 3.37. Detección de cambio de integridad en archivos

3.4 PRUEBAS DE DETECCIÓN DE CONEXIONES HACIA IP MALICIOSAS

Con esta prueba se requiere comprobar que se monitorean las conexiones salientes que maneja el firewall Sophos XG. Para esto se va a utilizar el dominio “suncocity.com”, el cual es catalogado como malicioso en Virustotal por 4 motores de antivirus como se indica en la Figura 3.38

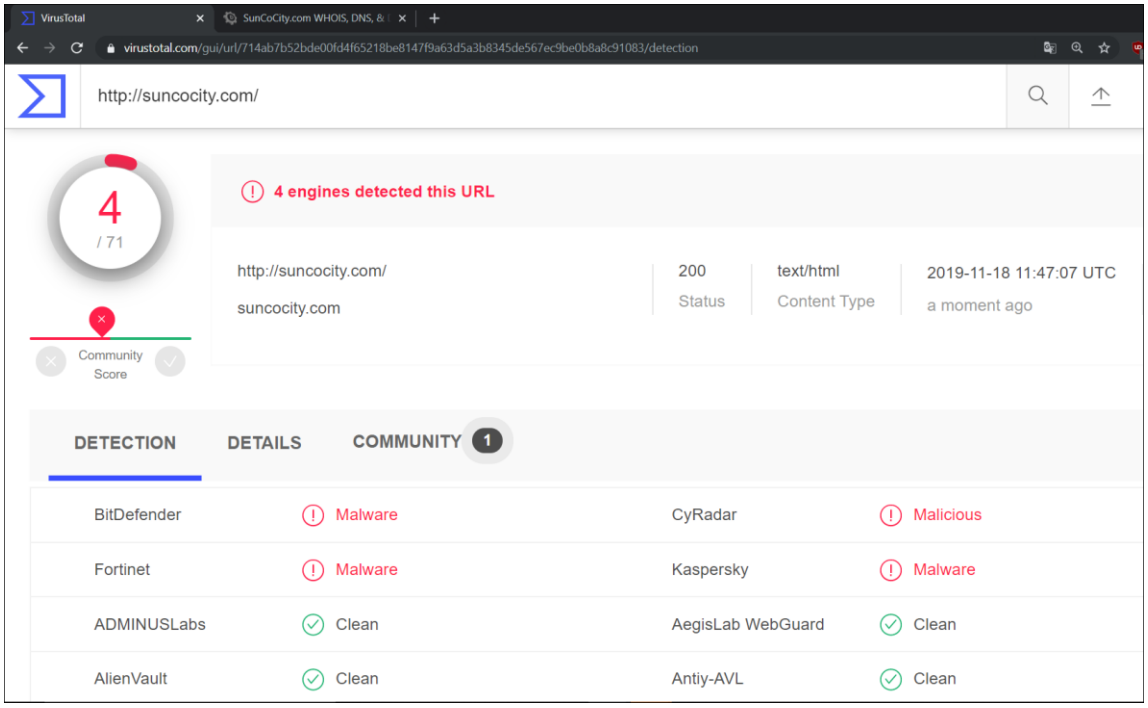


Figura 3.38. Reputación del dominio "suncocity.com"

La dirección IP pública que tiene asignado el dominio “sincocity.com” es la 198.27.88.131 como se indica en la Figura 3.39, esta será la dirección IP que manejará el firewall como dirección IP destino y la cual se debe de alertar cualquier conexión permitida.

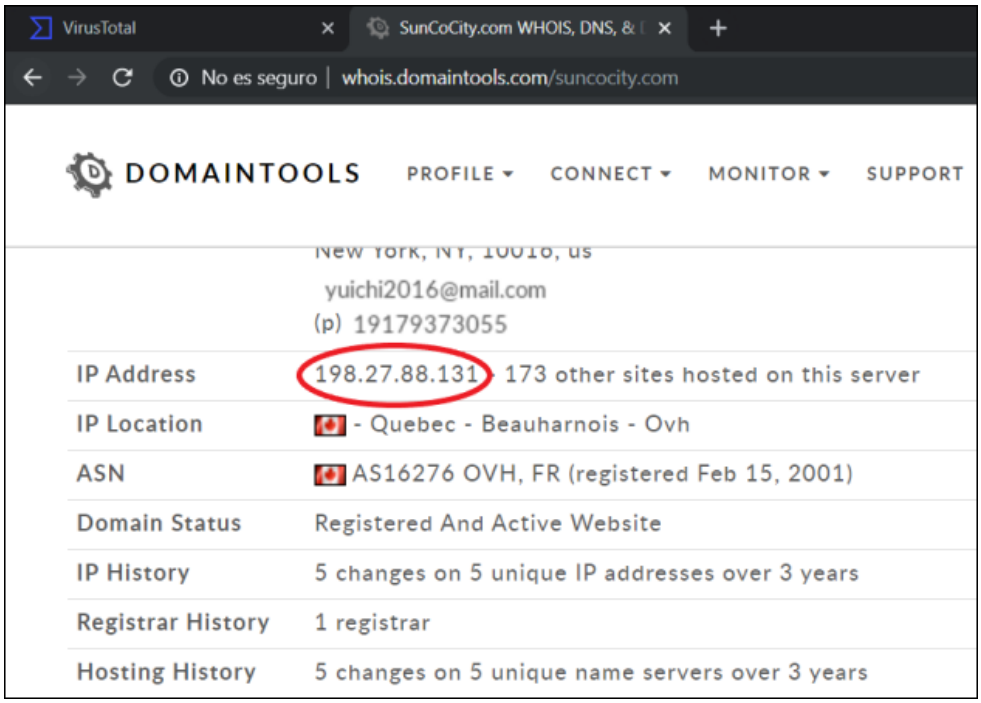


Figura 3.39. Dirección IP asignada al dominio "suncocity.com"

Desde una dirección IP interna 10.81.234.6, se realiza la conexión hacia el dominio “sucocity.com” y se establece la comunicación desde el navegador web como se indica en la Figura 3.40. Esta conexión via web es indicativo de que no hay ninguna regla que deniegue la conexión saliente hacia el dominio detectado como malicioso.

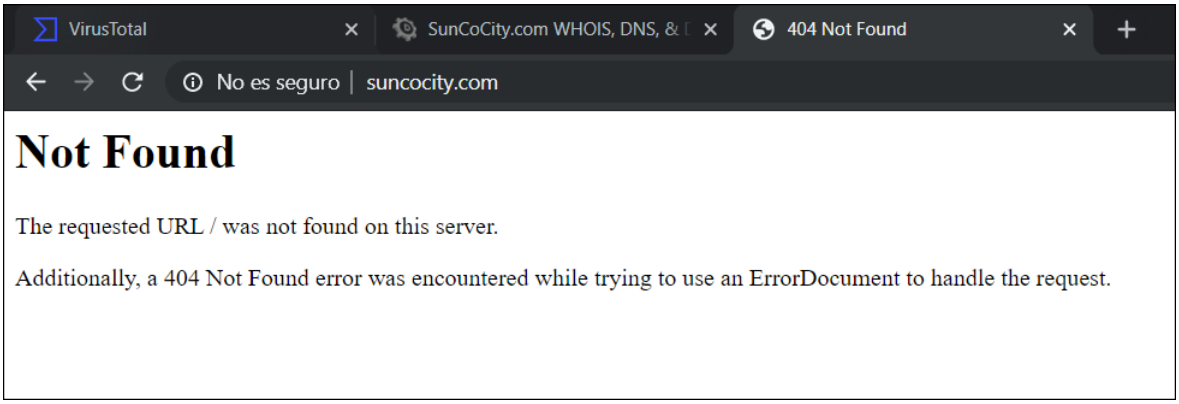


Figura 3.40. Acceso al dominio "suncocity.com" desde la red interna

Se verifica la generación de la alarma de conexión permitida hacia una dirección IP como se indica en la Figura 3.41

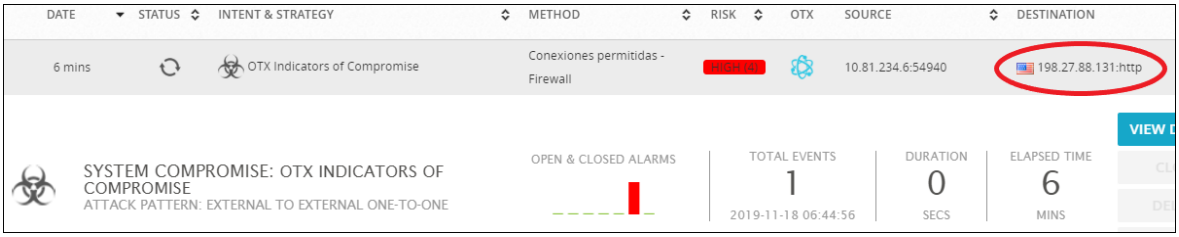
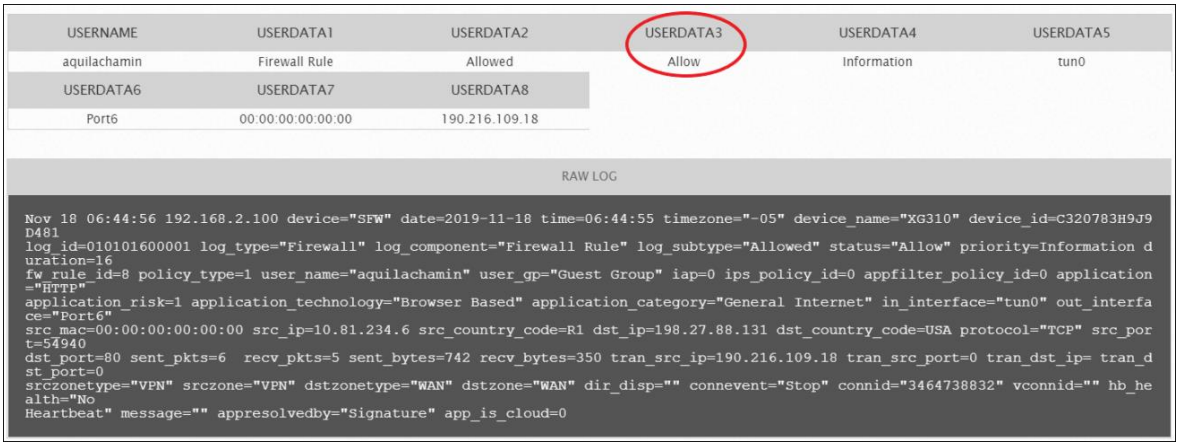


Figura 3.41. Alarma generada debido al acceso a la I detectada como maliciosa

En la Figura 3.42 se puede ver la detección del evento de conexión permitida y en la Figura 3.43 se indica el respectivo log que verifica que la conexión se estableció.

Figura 3.42. Firewall - Evento de acceso permitido



USERNAME	USERDATA1	USERDATA2	USERDATA3	USERDATA4	USERDATA5
aquilachamin	Firewall Rule	Allowed	Allow	Information	tun0
USERDATA6	USERDATA7	USERDATA8			
Port6	00:00:00:00:00:00	190.216.109.18			

RAW LOG

```
Nov 18 06:44:56 192.168.2.100 device="SFW" date=2019-11-18 time=06:44:55 timezone="-05" device_name="XG310" device_id=C320783H9J9
D481
log_id=010101600001 log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed" status="Allow" priority=Information d
uration=16
fw_rule_id=8 policy_type=1 user_name="aquilachamin" user_gp="Guest Group" iap=0 ips_policy_id=0 appfilter_policy_id=0 application
="HTTP"
application_risk=1 application_technology="Browser Based" application_category="General Internet" in_interface="tun0" out_interfa
ce="Port6"
src_mac=00:00:00:00:00:00 src_ip=10.81.234.6 src_country_code=R1 dst_ip=198.27.88.131 dst_country_code=USA protocol="TCP" src_por
t=54940
dst_port=80 sent_pkts=6  recv_pkts=5 sent_bytes=742 recv_bytes=350 tran_src_ip=190.216.109.18 tran_src_port=0 tran_dst_ip= tran_d
st_port=0
srczonetype="VPN" srczone="VPN" dstzonetype="WAN" dstzone="WAN" dir_disp="" connevent="Stop" connid="3464738832" vconnid="" hb_he
alth="No
Heartbeat" message="" appresolvedby="Signature" app_is_cloud=0
```

Figura 3.43. Firewall - Log de conexión permitida

4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- GMS, al igual que otras empresas de hoy en día cuentan con tecnologías de seguridad variadas como firewalls, antivirus, antispam, etc. El tener una herramienta que ofrece la visualización de los eventos que ocurren en cada una facilitó la gestión del administrador de red y permitió tomar acciones inmediatas sobre la detección de amenazas que se generen en la red como el bloqueo a direcciones IP que el firewall está permitiendo pasar y acciones preventivas como la ejecución de una revisión a las políticas aplicadas en el firewall

- Mediante la implementación de la plataforma OSSIM fue posible realizar la monitorización de las actividades que ocurren dentro de la red en tiempo real sobre los activos seleccionados al monitoreo, y con eso visualizar comportamientos anómalos como equipos de trabajo comprometidos (conexiones a sitios maliciosos) o actividad sospechosa de los usuarios finales.

- El monitoreo del firewall, así como la implementación de la directiva de detección de conexiones maliciosas brinda información importante sobre el estado de salud de los activos involucrados, ya que se observaría una falta de protección de la plataforma de antivirus lo cual podría derivarse de la falta de una tarea de actualizaciones o políticas mal aplicadas. Por lo tanto, se considera muy importante que el firewall sea uno de los activos imprescindible durante el monitoreo.

- Las directivas de correlación implementadas van alienadas a la detección de amenazas específicas en la red como equipos comprometidos, intentos de acceso a servidores críticos. Existen estándares de cumplimiento que dan las pautas necesarias para que el monitoreo sea más completo y abarque un número mayor de áreas como lo son la norma ISO 27000, PCI, HIPPA.

- La integración de los activos a monitorear no presentó inconvenientes durante la instalación de los respectivos agentes OSSEC utilizados para la recolección de logs o cuando se realizó la configuración de envío de logs desde los equipos firewall y virtualizador VMware. Con estos antecedentes, se podría comenzar con la integración del resto de activos pertenecientes a la red, con el propósito de tener una visibilidad completa de las actividades que se están desarrollando dentro de la red.

4.2 RECOMENDACIONES

- En el trabajo presentado se limitó el monitoreo a 5 activos, para garantizar la visibilidad completa de las actividades que se realizan dentro de la red se recomienda ampliar el monitoreo a todos los activos internos de la organización tomando en consideración el redimensionamiento que debe realizarse a la plataforma OSSIM.

- Cuando se realice la integración de activos al monitoreo, es importante verificar la recepción de eventos específicos que ayuden en la detección de anomalías como se la hizo en este proyecto, ya que si no se recibe la información apropiada la detección de amenazas no sería posible.

- La plataforma OSSIM presenta la limitación de no almacenar los logs que recibe directamente, por lo que se recomienda tener en consideración el uso del reenvío de logs cuando estos lleguen a la plataforma, ya sea por una regla de Rsyslog o algún otro mecanismo soportado, si una directriz a cumplir es la del almacenamiento de los logs por un tiempo determinado.

- Durante el despliegue de la plataforma OSSIM no se presentaron inconvenientes con respecto al funcionamiento de la plataforma. Los recursos de hardware proporcionados cumplieron con los requisitos indicados en la guía de despliegue, pero se debería considerar realizar un redimensionamiento de los recursos si aumenta el número de activos a monitorear.

5. REFERENCIAS BIBLIOGRÁFICAS

[1] Kaspersky Lab, "Securelist - Kaspersky Lab's cyberthreat research and reports," 14 Diciembre 2016. [Online]. Available: https://securelist.com/kaspersky-security-bulletin-2016-executive-summary/76858/. [Accessed 14 Septiembre 2018].

[2] Deloitte, "Deloitte - La Evolución de la Gestión de Cyber Riesgos y Seguridad de la Información," Julio 2016. [Online]. Available: https://www2.deloitte.com/ec/es/pages/technology-media-and-telecommunications/articles/Cyber-Riesgos-y-Seguirdad-de-la-Informacion.html. [Accessed 11 Octubre 2018].

[3] Consejo Superior de Administración, "Portal de Administración Electrónica del Gobierno de España," 2012. [Online]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. [Accessed 30 Mayo 2018].

[4] AlienVault, "AlienVault: Deployment Guide," 2 Abril 2018. [Online]. Available: https://www.alienvault.com/documentation/resources/pdf/usm-appliance-deployment-guide.pdf. [Accessed 5 Abril 2018].

[5] R. Gerhards, "The Syslog Protocol - RFC 5424," 2009. [Online]. Available: https://tools.ietf.org/html/rfc5424. [Accessed 25 Abril 2018].

[6] Trend Micro Inc., "OSSEC," 2017. [Online]. Available: https://www.ossec.net/. [Accessed 10 Mayo 2018].

[7] AlienVault, "About AlienVault NIDS," 2018. [Online]. Available: https://www.alienvault.com/documentation/usm-appliance/ids-configuration/about-alienvault-nids.htm. [Accessed 25 Abril 2018].

[8] AlienVault, "Leveraging OTX Threat Data with AlienVault USM," 2018. [Online]. Available: https://www.alienvault.com/open-threat-exchange/leveraging-otx-threat-data-in-alienvault-usm. [Accessed 25 Abril 2018].

[9] D. Miller, S. Harris, A. Harper, S. VanDyke and C. Blask, Security Information and Event Management (SIEM) Implementation, New York: McGraw-Hill, 2011.

[10] NAGIOS, «NAGIOS,» 2018. [En línea]. Available: https://www.nagios.org/. [Último acceso: 10 12 2020].

[11] D. Swift, «Successful SIEM and Log Management Strategies for Audit and Compliance,» 04 11 2010. [En línea]. Available: https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528. [Último acceso: 01 08 2019].

[12] PaloAlto Networks, "Brute Force siganture and related trigger conditions," 07 02 2019. [Online]. Available:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClmpCAC. [Accessed 01 08 2019].

[13] PCI Security Standards Council, «Payment Card Industry (PCI) Data Security Standard,» 01 04 2016. [En línea]. Available: https://pcicompliance.stanford.edu/sites/g/files/sbiybj7706/f/pci_dss_v3-2.pdf. [Último acceso: 01 08 2019].

[14] AlienVault, "AlienVault OSSIM: The World's Most Widely Used Open Source SIEM," 2018. [Online]. Available: https://www.alienvault.com/products/ossim. [Accessed 4 Abril 2018].

[15] AlienVault, «Deploy AlienVault HIDS Agents,» 2018. [En línea]. Available: https://www.alienvault.com/documentation/usm-appliance/ids-configuration/deploying-alienvault-hids.htm. [Último acceso: 10 Junio 2018].

[16] AlienVault, «Correlation Directives,» 2018. [En línea]. Available: 07.

ANEXOS

ANEXO A. Valorización de los activos aceptada por las partes involucradas de GMS.

ANEXO B. Valorización de las amenazas aceptada por las partes involucradas de GMS.

ORDEN DE EMPASTADO