Institución Universitaria

Modelo de monitoreo para la detección de escenarios de riesgo asociados a la identidad y control de acceso mediante la integración de una solución IAM con un SIEM para mejorar la respuesta a incidentes de seguridad

Lenitt Eliana López Carmona

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2023

Modelo de monitoreo para la detección de escenarios de riesgo asociados a la identidad y control de acceso mediante la integración de una solución IAM con un SIEM para mejorar la respuesta a incidentes de seguridad

Lenitt Eliana López Carmona

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director (a):

MSc. Gabriel Enrique Taborda Blandón

Línea de Investigación:

Ciencias Computacionales

Grupo de Investigación:

Automática, electrónica y Ciencias Computacionales

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2023

Dedicado al amor más puro que he podido experimentar: mi Abuela, que ahora me acompaña desde el cielo.
Gracias por hacer de mi lo que hoy soy, te amaré por siempre mi bombón de coco.

Agradecimientos

A Dios, por todas las bendiciones que me ha regalado, desde la vida hasta la oportunidad de vivir este reto de la Maestría.

A mi madre, por sus oraciones y voz de aliento para continuar siempre adelante.

A mi hijo, por apoyarme y relevarme cada vez que lo necesité.

A todos mis familiares, amigos y compañeros que estuvieron atentos a este proceso y me motivaron para no desfallecer.

A los docentes del ITM, que aportaron de una u otra forma con el logro de la hazaña que representa este trabajo.

Resumen

En el entorno digital actual, la identidad ha ganado cada vez más importancia, haciéndola más atractiva para los ciberdelincuentes, quienes buscan ganar acceso mediante técnicas evolucionadas. Es así, como las violaciones de datos han incrementado progresivamente cada año, generando más alertas para los equipos de seguridad, los cuales con poco personal y con información insuficiente, deben invertir más tiempo para investigar, comprender y tomar las acciones frente a cada amenaza. Para mejorar esta situación, esta investigación propone un modelo de monitoreo que integra una solución IAM con un SIEM; ambos Opensource, que, asignando un puntaje de riesgo para descartar las alertas sustentadas en las configuraciones y políticas para cada cuenta, deja sólo las amenazas reales no justificadas. Finalmente, se valida la aplicación del modelo con unos ataques controlados para entregar una lista minimizada de las alertas demostrando el mejoramiento en los tiempos de respuesta a incidentes de seguridad.

Palabras clave:

Amenazas, control de acceso, identidad, IAM, monitoreo, SIEM.

Abstract

In today's digital environment, identity has become increasingly important, making it more attractive to cybercriminals, who seek to gain access through evolved techniques. This is how data breaches have increased progressively every year, presenting more alerts to security teams, which with little staff and insufficient information, must invest more time to investigate, understand and take actions against each threat. To improve this situation, this research proposes a monitoring model that integrates an IAM solution with a SIEM; both Opensource, which, assigns a risk score to rule out the alerts based on the configurations and policies for each account, leaves only the real unjustified threats. Finally, the application of the model is validated with controlled attacks to deliver a minimized list of alerts, demonstrating the improvement in response times to security incidents.

Keywords:
Access control, IAM, identity, model, monitoring, SIEM, Threats

Contenido

Pág.

Lista de figuras

Pág.

Lista de tablas

Pág.

Lista de Símbolos y abreviaturas

Abreviaturas

Abreviatura	Término
BSI	Bundesamt für Sicherheit in der Informationstechnik - Oficina Federal Alemana para la Seguridad de la Información
CISA	Cybersecurity and Infrastructure Security Agency
CSOC	Cyber Security Operations Center
IEC	International Electrotechnical Commissions
IAM	Identity and Access Management
ISACA	Information Systems Audit and Control Association
ISCM	Information Security Continuos Monitoring
ISECOM	Institute for Security and Open Methodologies
ISF	Information Security Forum
ISO	International Organization for Standardization
ISSAF	Information System Security Assessment Framework
NIST	National Institute of Standards and Technology
OISSG	Open Information Systems Security Group
OSA	Open Security Architecture
OSSTMM	Open Source Security Testing Methodology
PSIM	Physical Security Information Management
SIEM	Security Information and Event Management
SOC	Security Operations Center

Introducción

Actualmente las organizaciones de todos los tamaños enfrentan el reto del incremento de las identidades digitales de los usuarios como resultado de la inclusión tecnológica como la transformación digital, el uso exponencial de dispositivos móviles y la tecnología IoT. Este crecimiento explosivo en las identidades trae consigo un mayor riesgo de violaciones relacionadas con la identidad que pueden ocurrir en muchos frentes, no solo a través de ataques de phishing, sino también de esquemas de ingeniería social, ataques de fuerza bruta y más. [1]

De otro lado, el aumento del trabajo remoto, catalizado en gran medida por la pandemia COVID-19, ha provocado que las terminales de muchas organizaciones se vuelvan mucho más diversas, ya que los empleados trabajan desde computadoras portátiles, tabletas y teléfonos inteligentes. Sin embargo, el trabajo remoto también es generalmente menos seguro, por tres razones principales:

1. Las organizaciones que no hayan invertido en herramientas sólidas de ciberseguridad en la nube para empleados remotos (incluso en dispositivos personales cuando sea necesario), así como el Múltiple Factor de Autenticación - MFA y tecnologías de seguridad de correo electrónico, estarán en riesgo de ataques de phishing e intentos de descifrado de contraseñas.
2. Las redes Wi-Fi públicas o personales gratuitas se pueden piratear y usar para instalar malware en dispositivos que están conectados a ellas sin una VPN.
3. Es más difícil mantener una mentalidad de “primero la seguridad” en casa que en la oficina.

Debido a esto, los dispositivos personales tienen el doble de probabilidades de infectarse con malware que sus contrapartes corporativas [2].

De acuerdo con el reporte global: “Ciberseguridad en la era del trabajo remoto” (figura 1), el 60% de los encuestados dijeron que han experimentado un ciberataque, el 56% de los que experimentaron el robo de credenciales y el 48% experimentó la ingeniería social, como el phishing [3].

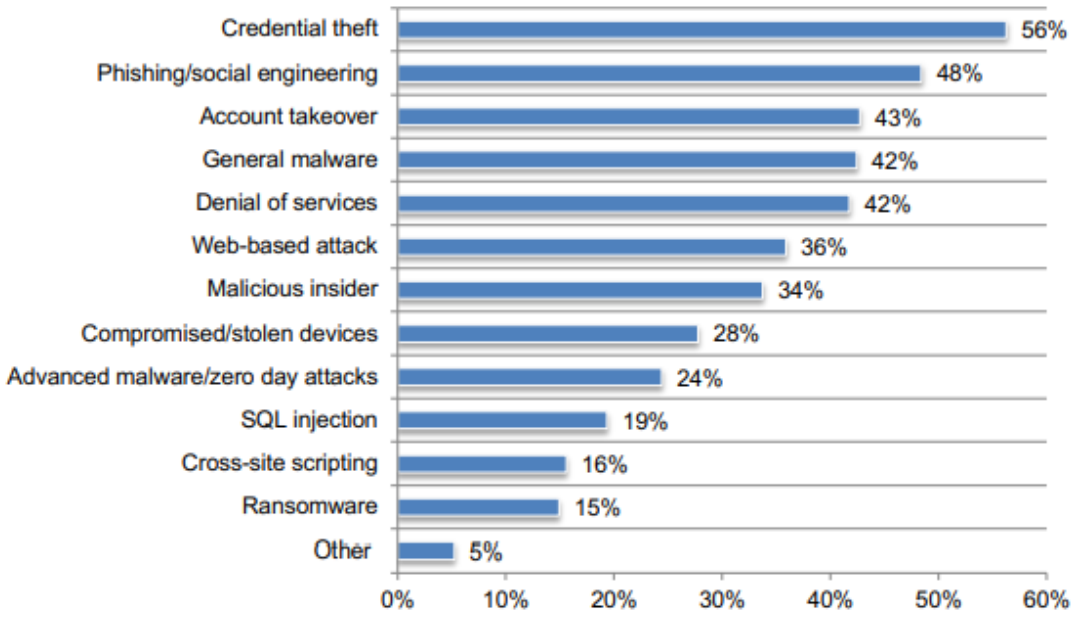

Figura 1: ¿Qué describe mejor el tipo de ataques experimentados por su organización?

La realidad nacional no está tan distante de esta visión de riesgos, pues tal y como lo demuestra la XXI Encuesta Nacional de Seguridad Informática (figura 2), en Colombia se mantiene la tendencia en materia de incidentes de seguridad en concordancia con las tendencias internacionales [4]. Para este año hay datos interesantes, se sostienen los errores humanos como el tipo de incidente más reportado; sin embargo, decrece un 12% frente al año anterior. Las brechas de seguridad provocadas por terceros es el tipo de incidente que mayor crecimiento con un 4%, seguido de acceso no autorizados en la web con un 3% y suplantación de identidad con un 2%.

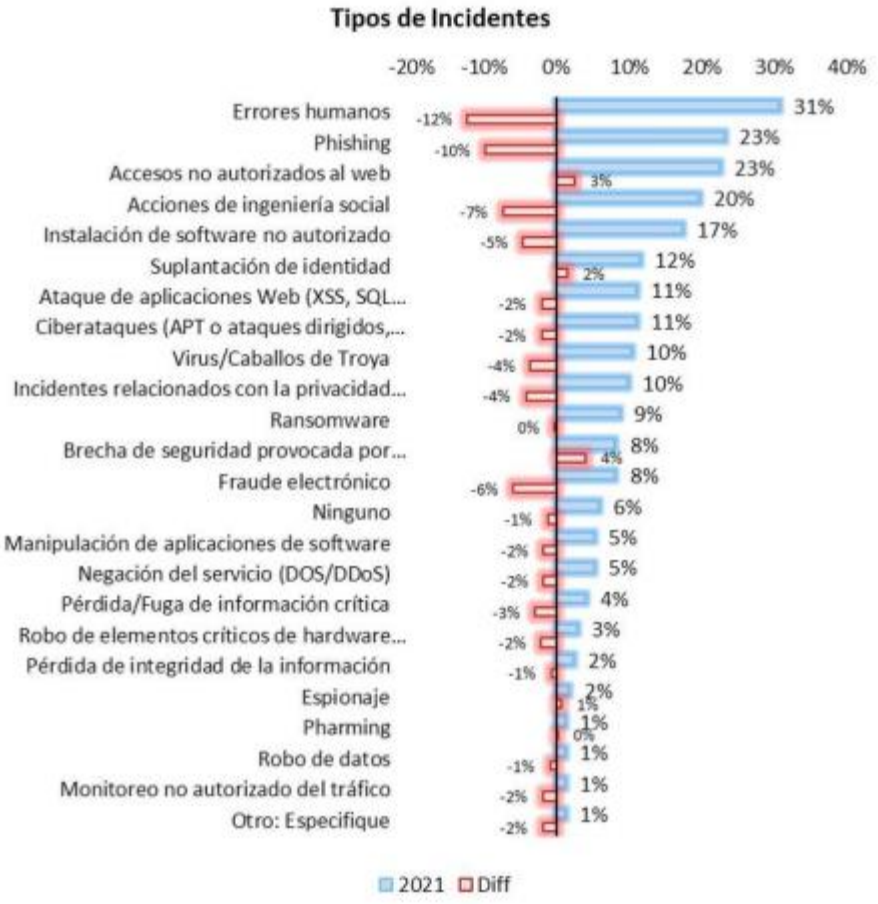

Figura 2: Tipos de incidentes de seguridad

Por otro lado, acorde a la figura 2, se puede evidenciar que los ataques relacionados con la identidad como el phishing, los accesos no autorizados a la web y la suplantación de identidad son los más representativos teniendo los dos últimos un crecimiento del 3% y del 2% respectivamente respecto al año anterior. Lo cual nos lleva a concluir que la protección de la identidad digital de los usuarios debería ser un aspecto vital para todas las organizaciones independiente de su tamaño, de su sector o del tipo de infraestructura que utilicen para la habilitación de los servicios informáticos.

El presente documento es el producto de una investigación aplicada que propone un modelo de monitoreo que integra el contexto de las cuentas de usuario en cuanto a los roles y privilegios gestionadas por un sistema IAM con los registros de identidad de un SIEM, para optimizar el monitoreo, comprender las alertas y agilizar los procesos de respuesta a incidentes. El aumento en los ataques del control de acceso a raíz de los cambios tecnológicos de los últimos años ha generado un gran volumen de registros de transacciones que abruman los equipos de seguridad de TI, razón por la cual este trabajo toma sentido en cuanto permita reducir las operaciones manuales, mejorar las decisiones

respecto a posibles eventos de seguridad e incrementar el asertividad en la aplicación de contramedidas cuando se vea comprometida la identidad. Se pretende entonces recolectar los componentes de ambos sistemas y describir la manera en que se pueden interrelacionar para lograr un funcionamiento articulado que se pueda validar en la implementación de una solución IAM Open Source integrado con un SIEM Open Source para la detección de posibles escenarios de riesgos.

Para la realización de este proyecto, se definió como objetivo General: *"Diseñar un modelo de monitoreo para la detección de escenarios de riesgo asociados a la identidad y el control de acceso mediante la integración de una solución IAM con un SIEM que permita comprender las alertas para agilizar los procesos de respuesta a incidentes".*

El cual se alcanzó mediante la ejecución de los siguientes objetivos específicos:

- "Caracterizar las posibles amenazas que comprometen la identidad y el control de acceso".
- "Integrar las soluciones de IAM y SIEM de distribución Open Source para contextualizar las alertas de identidad".
- "Construir el modelo de monitoreo soportado en los estándares y guías internacionales sobre respuesta a incidentes, gestión de identidades y monitoreo continuo de seguridad de la información".
- "Validar que con la aplicación del modelo de monitoreo se puedan detectar escenarios con alto puntaje de riesgo a través de la verificación realizada en el caso de estudio, prueba de concepto o simulación".

En este sentido, el documento contiene los siguientes elementos: el marco teórico que fundamenta la investigación, el estado del arte con la recolección de literatura relacionada, la metodología como hoja de ruta desarrollada para la investigación, los resultados obtenidos en su aplicación, las conclusiones y el trabajo futuro.

1. Marco Teórico y Estado del Arte

1.1 Marco teórico

Para lograr el objetivo de este proyecto de proponer un modelo de monitoreo en el que los eventos de identidad y control de acceso recolectados por un IAM se integren con una solución SIEM, es necesario definir y ampliar algunos conceptos, que sirven de base para facilitar el entendimiento del contexto en el cual se desarrollará.

1.1.1 Amenaza, vulnerabilidad y riesgo

La información que procesamos diariamente como individuos u organizaciones se encuentra en peligro cuando confluyen dos elementos: amenazas y vulnerabilidades. Para el ámbito de este proyecto, las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene. Por otro lado, una amenaza, es cualquier situación o evento externo al sistema que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan [5].

Ahora bien, cuando una amenaza se aprovecha de una vulnerabilidad en los sistemas de información para causar daño, hablamos del concepto de riesgo; conocido como la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando perjuicios a la organización [6].

El método de clasificación de amenazas del Open Security Architecture - OSA, contempla tres dimensiones ortogonales denominadas motivación, localización y agente que pueden visualizarse en la figura 3:

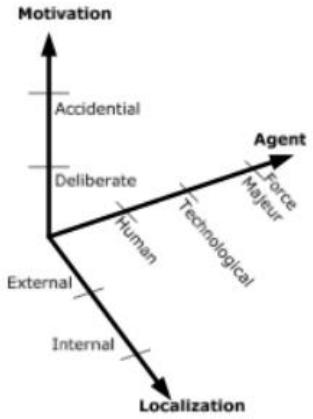

Figura 3: Dimensiones ortogonales para clasificación de amenazas. Fuente **[7]**

El agente de amenaza es el actor que impone la amenaza sobre un activo específico, que puede tratarse de agentes de fuerza mayor que son principalmente ambientales, los agentes tecnológicos que son causados por procesos físicos o químicos en el material como por ejemplo el envejecimiento y, por último, amenazas causadas por humanos como, por ejemplo, los usuarios atacantes.

La dimensión de motivación responde a la pregunta 'por qué' se crea una amenaza, que, combinada con la dimensión del agente, nos indica por ejemplo que una amenaza causada por un agente humano es causada ya sea por una intención deliberada o accidentalmente por descuido. Para la clase tecnológica, solo las amenazas accidentales son concebibles/posibles, ya que la motivación deliberada solo es posible para un humano. Lo mismo se aplica a la fuerza mayor [8].

1.1.2 Ataque informático

Este concepto referenciado también con ciberataque o ataque cibernético hace referencia al conjunto de acciones realizadas por actores de amenazas, que intentan obtener acceso no autorizado, robar datos o causar daños a computadoras, redes informáticas u otros sistemas informáticos. Un ataque cibernético se puede lanzar desde cualquier lugar. El ataque puede ser realizado por un individuo o un grupo utilizando una o más tácticas, técnicas y procedimientos (TTP) [9].

Ahora bien, hablar de TTP es entender como el atacante cumple su misión; desde el reconocimiento hasta una posible exfiltración de datos, pero conociendo en detalle los tipos de actividades que realizan los ciberdelincuentes (táctica), las habilidades o métodos generales (técnica) para cada táctica y por último la serie específica de pasos que los ciberdelincuentes pueden utilizar para llevar a cabo un ataque (procedimientos). El análisis TTP puede ayudar a los equipos de seguridad a detectar y mitigar ataques al comprender la forma en que operan los actores de amenazas [10].

1.1.3 Control de Acceso

De acuerdo con la organización IDpro el control de acceso es controlar quién puede tener acceso a datos, sistemas, servicios, recursos, ubicaciones. El ‘Quién’ puede ser un usuario, un dispositivo o una cosa, un servicio [11].

En forma equivalente en el estándar ISO/IEC 24760-1:2019 también se incluye una definición para control de acceso como un concepto abstracto de controlar el acceso de los usuarios a las aplicaciones. Es un término muy amplio y general, sin embargo, suele referirse a un mecanismo para definir y evaluar políticas de autorización [12].

1.1.4 Identidad

El marco para la administración de la identidad creado por la International Organization for Standardization (ISO) bajo el documento: ISO/IEC 24760-1:2019 establece la identidad como el hecho de ser quién o qué, una persona o cosa. Habla de ella como el conjunto de características, cualidades, creencias, comportamientos y otros aspectos de una entidad. La identidad se puede aplicar a personas, cosas, incluso conceptos intangibles, conocidos como entidades. Una entidad puede tener varias identidades (a menudo conocidas como personas). En el contexto de las tecnologías de la información, las partes de la identidad generalmente se pueden representar en una forma de registro digital, conocida como identidad digital.

La identidad no debe confundirse con el identificador. La identidad es un conjunto de características, mientras que el identificador es un valor que se utiliza para referirse a la identidad [12].

De allí, que para el ámbito de este proyecto es importante conocer la diferencia entre gestión de identidad y gestión de acceso, entendiendo que la primera gestiona los atributos relacionados con el usuario y la segunda evalúa los atributos en función de las políticas para tomar decisiones de Sí/No.

1.1.5 Identidad digital

La transformación digital que experimentamos desde hace varias décadas y que algunos relacionan con el inicio de la World Wide Web en los 90’s, ha impulsado la apropiación de la tecnología y la interconexión de las empresas, las personas y las cosas. Cada día es más frecuente usar el internet para nuestras actividades cotidianas como agendar una cita médica, realizar transacciones bancarias, comprar bienes y servicios, por lo cual su creciente importancia ha incrementado el interés de los delincuentes del ciberespacio para robar lo que se conoce como identidad digital y poder suplantar un usuario, un subsistema o un dispositivo con fines lucrativos o reputacionales. Según la IDpro; organización profesional para profesionales de IAM, la identidad digital se define como la combinación de un identificador único junto con atributos relevantes que identifican de forma única a una entidad [13]. Según el tipo de identidad (humana; como fuerza de trabajo o cliente, y los tipos no humanos como sistema o dispositivo), las fases del ciclo de vida de la identidad serán diferentes.

1.1.6 Identity and Access Management (IAM)

El Identity Management Institute (IMI), primera organización líder mundial en certificación dedicada a la gestión de identidades, la gestión de riesgos y el cumplimiento, define el concepto de identidad y control de acceso (IAM) como el conjunto integral de tecnologías, políticas de toda la empresa y procesos para otorgar, controlar y contabilizar las identidades a lo largo de su ciclo de vida para asegurar el acceso y las transacciones, así como el no repudio. Esto incluye la incorporación e identificación de cada identidad, su autenticación con una credencial de confianza, la autorización de acceso a los recursos,

la asignación de responsabilidades, el seguimiento de actividades, la desvinculación y la gestión de otros atributos asociados con un usuario individual [14].

De los anteriores elementos tomaremos para este proyecto, como los principales componentes de IAM en el mismo orden que ocurren sus fases: la identificación, la autenticación, la autorización, el perfilamiento, la trazabilidad y el desaprovisionamiento como los componentes esenciales de IAM para analizar su compromiso en cada una las amenazas sugeridas por algunas guías y buenas prácticas de seguridad de la información.

1.1.7 Identificación

Consiste en el acto de establecer la existencia de la identidad con la que se va a interactuar. Antes de la autenticación se debe validar cual identidad se pretende utilizar.

1.1.8 Autenticación

Es el proceso de comprobación de la legitimidad de uso de una identidad o la propiedad de una cuenta cuando la misma se usa para acceder a un recurso.

1.1.9 Autorización

Es el derecho de acceso a un recurso que se otorga luego de la autenticación de la identidad de un usuario, sistema o dispositivo.

1.1.10 Perfilamiento

Lo definiremos como los niveles de acceso o la asignación de privilegios relacionados a cada uno de los recursos.

1.1.11 Trazabilidad

Para lo concerniente, se tratará del seguimiento de las actividades realizadas por una entidad.

1.1.12 Desaprovisionamiento

Se incluye en este concepto el retiro de los permisos o la eliminación de la entidad como parte final de su ciclo de vida.

1.1.13 Indicadores de ataques

Cuando hablamos de indicadores de ataque (IOA) utilizamos un enfoque proactivo para la detección de amenazas, ya que se tratan de evidencias o señales que se centran en identificar la actividad del atacante mientras está ocurriendo el ataque. Responden a la pregunta: ¿qué pasa y por qué?, mientras los indicadores de compromiso (IOC) responden a ¿qué pasó? En la misma línea, un IOC es una evidencia digital de que ha sucedido un incidente cibernético, mientras que un IOA es cualquier evidencia digital o física de que es probable que ocurra. La figura 4 muestra una comparación entre los indicadores de ataques (IOA) y los indicadores de compromiso (IOC), donde con algunos ejemplos se puede diferenciar su carácter proactivo y reactivo respectivamente:

Figura 4: Ejemplos de IOA y IOC. Fuente **[15]**

1.1.14 Monitoreo

De acuerdo con el enfoque de este proyecto utilizaremos el concepto de monitoreo aplicado a la ciberseguridad como la observación continua de un ecosistema TI para detectar amenazas cibernéticas y posibles violaciones de datos.

1.1.15 Gestión de acceso privilegiado (PAM)

De acuerdo con la empresa de seguridad de la información CyberArk, el acceso privilegiado es un término para designar un acceso especial o habilidades que van más allá de las de un usuario estándar. El acceso privilegiado permite a las organizaciones asegurar su infraestructura y sus aplicaciones, administrar su negocio de manera eficiente y mantener la confidencialidad de los datos sensibles y la infraestructura crítica. La gestión

de acceso privilegiado se refiere a una estrategia integral de ciberseguridad, que comprende personas, procesos y tecnología, para controlar, monitorear, proteger y auditar todas las identidades y actividades privilegiadas humanas y no humanas en un entorno de TI empresarial [16]. Lo anterior nos lleva a concluir que pueden existir muchas cuentas privilegiadas de tipo humano y no humano, las cuales para el ámbito de este proyecto acotaremos dentro de las humanas, las cuentas de los administradores de sistemas de TI y las cuentas de los usuarios comerciales privilegiado que están por fuera de TI, pero tiene acceso a sistemas confidenciales como finanzas, recursos humanos, entre otros.

1.1.16 Respuesta a incidentes

Para entender en qué consiste este concepto es necesario delimitar previamente los conceptos de evento e incidente de seguridad informática. De acuerdo con la guía para el manejo de incidentes de seguridad informática; NIST 800-61 revisión 2, un evento es cualquier ocurrencia observable en un sistema o en una red, los cuales pueden considerarse como adversos sí tienen una consecuencia negativa. Por su parte un incidente de seguridad informática corresponde a una violación o amenaza inminente de violación a las políticas de seguridad de la información, al uso aceptado de las políticas o las prácticas estándares de seguridad [17]. Conjugando lo anterior todos los eventos no corresponden a incidentes de seguridad informática, pero cuando estos se presentan se debe contar con la capacidad para atender, reaccionar y mitigar el posible impacto que estos generan sobre los activos de información o su operación, buscando que el tiempo medio para reconocer (MTTA) y para corregir (MTTR) sean el mínimo posible.

1.1.17 Security Information and Event Management (SIEM)

Un SIEM como el concepto, fue acuñado en el 2005 por Amrit Williams Mark Nicolett para la convergencia de la gestión de eventos de seguridad (SEM) y software de gestión de información de seguridad (SIM) y que ha sido diseñado para ayudar en el diseño de políticas de seguridad y la gestión de eventos desde múltiples fuentes. De acuerdo con [18], un SIEM simple se compone de bloques separados (por ejemplo, dispositivo fuente, recolección de logs, normalización del “parsing”, motor de reglas, almacenamiento de logs, monitoreo de eventos), los cuales pueden trabajar independientemente uno del otro, pero que, pero sin que todos trabajen juntos, el SIEM no funcionaría adecuadamente. En la figura 5 se pueden visualizar estos componentes [18]:

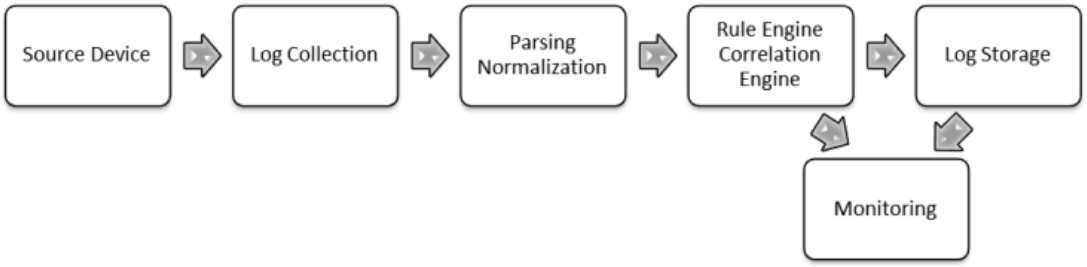

Figura 5: Componentes básicos de SIEM. Fuente **[18]**

1.1.18 Syslog

De acuerdo con la empresa Solarwinds líder en soluciones de administración y monitoreo IT, el protocolo de registro del sistema syslog, es un protocolo estándar que permite que los dispositivos de red interactúen con un servidor de registro e intercambien datos de eventos. Los mensajes que se transmiten a través de syslog contienen información como marcas de tiempo, identificación del dispositivo y dirección IP, clasificación de gravedad del evento e información específica del evento [19]. Para el propósito de este proyecto se utilizó este conocido protocolo para el envío de los eventos generados por la solución IAM, con el fin de que la solución SIEM opere como un servidor syslog listener; que recopile, filtre y administre los datos de eventos.

1.2 Estado del arte

Para ubicar los trabajos relacionados con esta investigación en las fuentes de información fue necesario dividir el tema principal en dos subtemas; primero los modelos de monitoreo para eventos de ciberseguridad y segundo la integración de las soluciones IAM y SIEM. Sin embargo, no se encontraron documentos sobre la integración propuesta, por cual se realizó una búsqueda de posibles integraciones de IAM y de SIEM con otras soluciones en forma separada.

Los datos recopilados se basaron en literatura académica, libros de referencia y de las publicaciones de empresas tecnología como Sailpoint, Gartner, Securonix, LogRhythm, Kpmg entre otros. Por último, se acotó la fecha de las fuentes al período comprendido entre los años 2018 y 2022, con el fin de tener la información lo más reciente posible.

En orden cronológico y de acuerdo con la división planteada, en lo que respecta a los modelos de monitoreo, la ontología del proceso de análisis de un CSOC propuesta en [20] plantea un flujo de trabajo en las etapas de detección, respuesta y recuperación que sirve como árbol de decisión en el análisis y atención de un posible incidente de ciberseguridad.

En la misma línea, el modelo de simulación de ciberataque aleatorio propuesto en [21] incluye seis módulos direccionados a categorías de potenciales ciberataques entre los que se encuentran el control de acceso y la ingeniería social. Para ambas, se ofrecen ejemplos de listas de chequeo de buenas prácticas y la frecuencia con que se sugiere se revise el módulo al mismo tiempo es un modelo proactivo y herramienta mejorada para determinar la preparación individual y corporativa para detectar, prevenir, responder y mitigar los ciberataques en la era digital post COVID-19.

Con relación a los antecedentes de integraciones, en [22] los autores proponen la integración del sistema de software de gestión de la información de seguridad física PCMS con el conocido SIEM Qradar de IBM con el fin de monitorear las vulnerabilidades físicas y lógicas de sistemas de seguridad físicos como sensores, cámaras, paneles de control, entre otros, que al estar interconectados se encuentran expuestos a ciberataques. Su resultado indica que es posible detectar ambos tipos de anomalías (ciber y físicas) con ambos sistemas, así como identificar amenazas críticas de seguridad ciberfísica que pueden poner en peligro una infraestructura o el propio sistema de protección. El anterior proyecto, ejemplifica cómo es posible tomar las alertas de un sistema que monitorea la seguridad de los sistemas físicos y reenviarlos en forma segura como un syslog o datos de aplicaciones usando el protocolo TLS de manera que puedan llegar al tablero de PCMS y el operador del SOC pueda interactuar con la contraparte cibernética o física, para enfrentar y resolver el ataque en curso.

Por su parte, el autor de la tesis referenciada en [23] propone una metodología para la integración de la solución IAM AC Identita de Autocont con la aplicación empresarial SVI-Sistema de Atención Temprana para la protección social y jurídica de los niños en la

República Checa. De acuerdo con la revisión bibliográfica realizada en esta investigación, no se encontraron fuentes que abordaran la integración, por lo tanto, su aporte más representativo es el diseño de la metodología, pues facilita la incorporación de una solución de gestión de acceso e identidad en forma centralizada para simplificar la administración de cuentas de usuario en las diferentes aplicaciones empresariales.

Los trabajos mencionados se agrupan en tabla 1.2.1, donde se resume cual es la temática y lo que pretende lograr, cuáles son los faltantes frente al proyecto propuesto y como se pretende complementar con su elaboración:

TEMA	TRABAJO RELACIONADO	PROPÓSITO	LIMITANTES	PROPUESTA DE GENERACIÓN DE VALOR
MODELO DE MONITOREO A RIESGOS DE IDENTIDAD Y CONTROL DE ACCESO MEDIANTE INTEGRACIÓN DE IAM Y SIEM	2018-CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process **(Artículo de conferencia)**	Plantea una ontología del proceso de análisis de un CSOC que cubre las etapas de: detección, respuesta y recuperación de un posible incidente de ciberseguridad, que puede guiar la toma de decisiones de los analistas y en el conocimiento de los activos, las amenazas y las vulnerabilidades.	Incluye la tarea del monitoreo en la etapa de detección, pero no propone un modelo específico para llevar a cabo las actividades de vigilancia sobre las alertas.	El trabajo propuesto realizará un zoom sobre la tarea de monitoreo para proponer un modelo que correlacionando eventos asociados a la identidad y control de acceso suministrados por el IAM tipifique amenazas reales,
	2020-Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era **(Artículo de revista científica)**	Aporta buenas prácticas en las listas de chequeo para los módulos de ingeniería social y control de acceso relacionadas con el proyecto propuesto para ser tenidas en cuenta en la creación del modelo de monitoreo.	No propone un modelo de monitoreo para las categorías de potenciales ciber ataques que modulariza en su propuesta.	
	2019- F. Frattini, U. Giordano and V. Conti, "Facing Cyber-Physical Security Threats by PSIM-SIEM Integration". **(Artículo de conferencia)**	Presenta la integración del SIEM de IBM Qradar con el software de gestión de seguridad física PCMS para monitorear anomalías ciber-físicas. Argumenta la premisa presentada en cuanto indica que hay ataques con síntomas difíciles de entender sin antedecendes detallados de un sistema al otro.	Sólo incluye el ataque de inicio de sesión de administración fallidos a los paneles de control (CP)como un escenario de ataque para ejemplificar la integración, sin contemplar otros escenarios asociados a la identidad y control de acceso.	
	2020-Integrace IAM v podnikovém IS- Integración de IAM y Sistemas de Información Corporativa.**(Tesis)**	Propone una metología para la integración de la solución IAM AC Identita con la aplicación empresarial SVI-Sistema de Atención Temprana para la protección social y jurídica de los niños en la República Checa. Se toma como referencia las opciones de integración propuestas para ser tenidas en cuenta como criterios en la selección de la solución SIEM que se integrará con la solución IAM	Es una integración de un software específico empresarial que se alimenta de la solución IAM pero que no incluye la salida de registros de identidad y control de acceso.	El trabajo propuesto incluye la recolección de los registros de identidad y control de acceso como insumo para el SIEM

Tabla 1.2.1: Resumen comparativo del estado del arte. Elaboración propia

Por otro lado, en lo que respecta a las publicaciones de entidades de tecnología, Sailpoint como líder en soluciones de gobernanza de identidades, enfoca la integración de sus soluciones con el SIEM Splunk argumentando que esta combinación permite a las empresas automatizar las tareas de gobierno de identidad con las modificaciones del acceso a la identidad y proporcionar al SIEM un contexto de identidad para tomar decisiones más acertadas [24]. Del mismo modo, la compañía especialista en SIEM, LogRhythm presenta en uno de sus webcasts cómo la integración con el IAM Okta permite a los analistas de seguridad tomar decisiones más informadas y realizar investigaciones cuando tiene el panorama completo de los eventos de identidad [25].

Como se evidencia en esta recopilación de trabajos relacionados, la integración de estas dos soluciones trae consigue múltiples beneficios en cuanto a la eficiencia en la atención de incidentes y la ganancia bidireccional que puede obtenerse en la limitación de registros del SIEM y la aplicación de correcciones sobre la solución IAM. Sin embargo, en la literatura consultada no se encuentra un modelo de monitoreo que plantee como se puede realizar la integración y cuáles son las consideraciones que deben tenerse en cuenta, por lo cual la realización de este proyecto es totalmente pertinente y puede impactar positivamente la operación de los equipos de seguridad de TI o de un SOC que administre los eventos y registros de seguridad de la información de cualquier organización.

2. Metodología

Para el desarrollo de la investigación aplicada se utilizó el método deductivo, que mediante un razonamiento lógico pretende obtener unas conclusiones a partir de una premisa o hipótesis; iniciando de lo general para llegar a lo particular.

La metodología empleada se puede observar en la figura 6 que presenta las (4) fases planeadas con sus respectivas actividades, las cuales se explicarán en detalle a continuación:

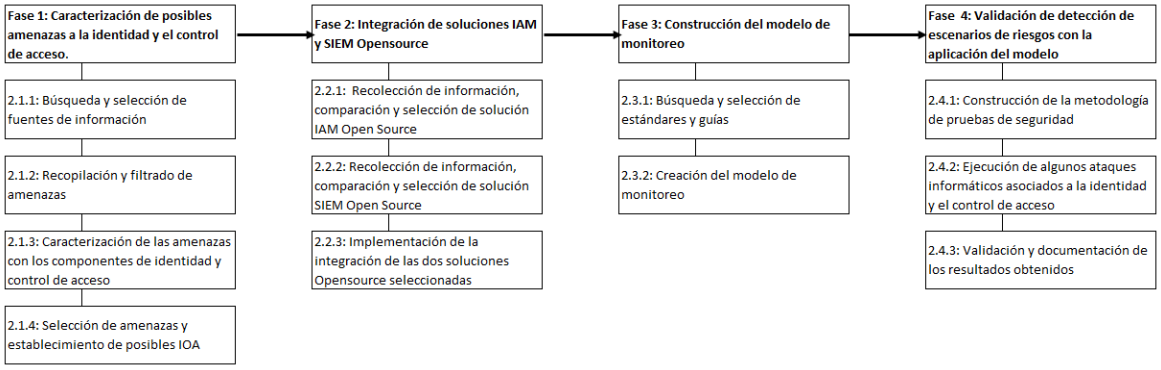

Figura 6:Metodología del proyecto de investigación. Fuente propia.

2.1 Fase 1: Caracterización de posibles amenazas a la identidad y el control de acceso

Para definir las características o circunstancias que identifican a cada una de las amenazas que pueden comprometen a la identidad y el control de acceso, se desarrollaron las siguientes actividades:

2.1.1 Búsqueda y selección de fuentes de información

En esta etapa se utilizaron los buscadores y las bases de datos científicas y académicas como: Google Académico, IEEE, y Springer Link para ubicar los trabajos de grado, artículos y libros relacionados con las amenazas a la identidad y al control de acceso con fecha de publicación entre los años 2018 y 2022, a fin de tener la información más reciente. Para ello se utilizaron varias ecuaciones de búsqueda, seleccionando las siguientes como las que tuvieron mejores resultados: “Access Control Threats”, “Treaths of Authentication”, “Threats related to Access Control, or Accounts, or Credential, or Identity”. Igualmente se amplió el rango incluyendo los estándares y publicaciones de institutos o proyectos relacionados con ciberseguridad y seguridad en las aplicaciones como Mitre, Nist y Owasp.

El resumen de las fuentes de información seleccionadas se reportará en la etapa de resultados en la tabla 2.1.1:

N° FUENTE	AUTOR	NOMBRE DEL DOCUMENTO/ PUBLICACIÓN/ TRABAJO	AÑO

Tabla 2.1.1: Matriz de fuentes de información seleccionadas

La finalidad de esta actividad es ubicar varias fuentes que contengan información actualizada y suficiente para recopilar la base de amenazas, que monitoreadas proactivamente permiten tomar decisiones informadas y rápidas en los equipos de seguridad de TI.

2.1.2 Recopilación y filtrado de amenazas

De las anteriores fuentes se extrajo un listado de amenazas asociadas a la identidad y el control de acceso, eliminando los duplicados para obtener el consolidado de (32) amenazas presentado en la tabla 2.1.2 con su definición técnica.

N°	AMENAZA	DEFINICIÓN

Tabla 2.1.2: Listado de amenazas consolidado

2.1.3 Caracterización de las amenazas con los componentes de identidad y control de acceso

En esta etapa se analizó para cada amenaza de la lista anterior, si comprometen o no cada uno de los componentes de la identidad y control de acceso descritos en el marco teórico, los cuales se presentan como columnas de la tabla 2.1.3.

Para darle una cuantificación de cómo una amenaza afecta un componente, se tomó la siguiente escala de calificación:

- 0 - si cuando se materialice la amenaza no se compromete el componente.
- 1- si el componente se compromete ya sea en forma parcial o total.

En la última columna de la tabla se sumaron las calificaciones de cada amenaza en cada uno de los componentes. Dicha cualificación se reflejará en una matriz como la que muestra la tabla 2.1.3:

N°	AMENAZA	IDENTIFICIÓN	AUTENTICACIÓN	AUTORIZACIÓN	PERFILAMIENTO	TRAZABILIDAD	DESAPROVISIONAMIENTO	TOTAL

Tabla 2.1.3: Caracterización de amenazas

El propósito de la tabla anterior es obtener las (5) amenazas con los (5) valores totales más altos pues implican un mayor compromiso de los componentes de identidad y el control de acceso y establecer las amenazas sobre las cuales se determinarán los posibles indicadores de ataque en la fase siguiente.

2.1.4 Selección de amenazas y establecimiento de posibles IOA

El resultado final de esta etapa es tomar las amenazas con los totales más altos en cuanto a componentes de identidad y control de acceso comprometidos para ubicar algunos indicadores de ataque (IOA) relacionados que podría dar cuenta en un proceso proactivo de monitoreo, de un posible ataque. La estructura de esta tabla relacional de amenazas y los Indicadores de Ataque (IOA) delimitados para este proyecto es la presentada en la tabla 2.1.4:

AMENAZA	POSIBLES INDICADORES DE ATAQUE	IOA DEFINIDO

Tabla 2.1.4: Relación de amenazas con IOA

Con esta última etapa, se tiene la caracterización de las amenazas que afectan la identidad y el control de acceso, insumo fundamental para la perfilación y configuración del proceso de monitoreo.

2.2 Fase 2: Integración de soluciones IAM y SIEM Open Source

Le corresponde a esta etapa la misión de evaluar las distintas soluciones de código abierto (Open Source) tanto de IAM como de SIEM para que, basados en algunas funcionalidades, se puedan establecer las dos mejores soluciones para integrarse, de manera que los

registros de acceso e identidad reportados en el IAM se descarguen en el SIEM y mediante una contextualización de las amenazas, se pueda establecer un puntaje de riesgo para cada uno de los escenarios, con ello tener un proceso de monitoreo más proactivo. Para el logro de esa meta, se realizaron las siguientes actividades:

2.2.1 Recolección de información, comparación y selección de solución IAM Open Source

Partiendo del hecho que se pretende establecer un modelo de monitoreo a bajo costo que pueda ser implementado en empresas de todos los tamaños, se decidió optar por las soluciones de distribución Open Source, que además de permitir el acceso y la modificación al código fuente, no representen una alta inversión por sus derechos de uso. Adicionalmente, entendiendo que uno de los propósitos del proyecto es mejorar los tiempos de respuesta sólo se tuvieron en cuenta las soluciones IAM que permitieran hacer un manejo de log a través del servicio syslog; automatizando así la exportación de los registros hacia el SIEM.

Teniendo estos dos criterios como filtro, se realizó una investigación de páginas web de empresas de consultoría dedicadas a evaluar soluciones de software como Gartner, Capterra, Solutions Review, Medevel y Saasworthy, donde basándose en sus análisis y comparaciones de los diferentes productos de código abierto se pudieron establecer las funcionalidades más importantes los cuales serán evaluados para las cuatro (4) soluciones Open Source más viables en la tabla 2.2.1. La metodología de calificación de estos requisitos se estableció con base en un puntaje de cuatro valores, valorando que tanto cumple la característica buscada en la solución IAM a analizar:

- 0-No Soportado
- 1-Mínimamente Soportado
- 2-Bien Soportado y
- 3-Ampliamente Soportado

N°	CARACTERISTICA	DESCRIPCIÓN	SOLUCIÓN 1	SOLUCIÓN 2	SOLUCIÓN 3	SOLUCIÓN 4

Tabla 2.2.1: Selección de IAM Open Source

La sumatoria de puntaje anterior permite seleccionar la solución IAM con más facilidades de operación para el usuario y con el soporte de estándares de autorización de acceso y autenticación de usuarios, esto es, aquella solución cuyo puntaje sea superior.

2.2.2 Recolección de información, comparación y selección de solución SIEM Open Source

De manera similar, para la selección de la solución de Gestión de Eventos e Información de Seguridad se verificó la documentación de las soluciones SIEM: AlientVault OSSIM, Apache Metron, Mozdef y Wazuh para verificar que soportarán la recepción de logs a través del servicio syslog. Igualmente se evaluaron sus fichas para conocer si las funcionalidades incluidas en las versiones Open Source o de uso gratuito incluyeran las características de correlación de eventos de las soluciones SIEM para el cumplimiento del objetivo de integración de este proyecto. Los resultados de esta fase serán presentados en el apartado de resultados, sección 3.2.2.

2.2.3 Implementación de la integración de las dos soluciones Opensource seleccionadas

Como secuencia de las actividades anteriores, en esta etapa se tomaron las soluciones Opensource resultantes y basados en la documentación de la casa matriz y en la investigación de blogs técnicos para la resolución de problemas, se realizó la creación de las máquinas virtuales, las configuraciones de los parámetros y las pruebas de funcionamiento para demostrar que los registros de eventos de identidad obtenidos de la solución IAM fueran enviadas a través del protocolo syslog hacia la solución SIEM. Adicionalmente, fue necesario la creación de reglas y decodificadores en la solución SIEM para que los registros obtenidos pudieran ser procesados y analizados de modo que se presentaran como alertas en el tablero de control, convirtiéndose así en el insumo para su categorización en las siguientes fases del proyecto.

2.3 Fase 3: Construcción del modelo de monitoreo

La contextualización que nos brinda el entorno de amenazas planteado en la fase 1, nos lleva a entender que la dinámica de los riesgos cibernéticos es cada vez más cambiante y que la creación, implementación y seguimiento de un modelo de monitoreo continuo de seguridad se convierte en una necesidad dentro la gestión de riesgos empresariales.

Basado en lo anterior, esta fase se enfocó en consultar fuentes de información relacionadas con la respuesta a incidentes, gestión de identidades y el monitoreo continuo a la seguridad de la información, que pudieran servir de apoyo para proponer una estrategia que oriente sobre los pasos que deberían ejecutarse cuando se reciba una alerta en el caso específico de los riesgos asociados a la identidad y el control de acceso. Durante esta fase se adelantaron (2) actividades principales que se relacionan a continuación:

2.3.1 Búsqueda y selección de estándares y guías

Durante esta actividad se estudiaron las normas, publicaciones y guías de entidades reconocidas como la ISO, el NIST y otras fuentes como artículos y blogs especializados en el tema, con un rango de fecha ampliado entendiendo que algunos estándares son de única publicación y no han tenido actualizaciones recientes.

El resumen de las fuentes de información seleccionadas se reportará en la etapa de resultados en la tabla 2.3.1:

N° FUENTE	AUTOR	NOMBRE DEL DOCUMENTO/ PUBLICACIÓN/ TRABAJO	AÑO

Tabla 2.3.1: Matriz de estándares y guías seleccionadas

En definitiva, el cometido de esta etapa es recoger conceptos de varios estándares que sirvan de guía para establecer las consideraciones o prácticas recomendadas en el monitoreo para la detección de riesgos asociados a la identidad y el control de acceso.

2.3.2 Creación del modelo de monitoreo

El monitoreo continuo de la seguridad trae beneficios para todas las empresas como la visibilidad de los activos, el conocimiento de las crecientes amenazas y el suministro de información para la toma de decisiones de gestión de riesgos de la organización. De allí, que para tener un programa de monitoreo exitoso es necesario crear una serie de pasos que constituyan un marco procedimental para que el equipo de monitoreo teniendo como insumo la lista de los IOA de las amenazas priorizadas de la fase 1, sepa como priorizar el riesgo de la alerta y orientar sobre la ejecución de las fases de atención de incidentes propuesta de las fuentes de información seleccionadas en el paso anterior. El modelo propuesto se presentará en la etapa de resultados correspondiente.

2.4 Fase 4: Validación de la detección de escenarios de riesgos con la aplicación del modelo

En esta última fase se estudiaron las metodologías de pruebas de seguridad existentes con el fin de seleccionar los referentes para construir el procedimiento propio para realizar algunos ataques informáticos basados en los indicadores de ataques identificados en la etapa 1 de caracterización de amenazas. Para ello, se definieron las siguientes actividades:

2.4.1 Construcción de la metodología de pruebas de seguridad

Las pruebas de seguridad son una forma de prueba de software no funcional que verifica el software en busca de amenazas, riesgos y vulnerabilidades [26]. Teniendo claro los objetivos, se debe determinar el tipo de prueba de seguridad entre: el escaneo de vulnerabilidades, las pruebas de penetración, las evaluaciones del riesgo, las auditorias de seguridad, las revisiones de código seguro o la evaluación de postura de seguridad. Para este caso, que se pretende lanzar algunos ataques informáticos que generen alertas sobre amenazas a la identidad y control de acceso en el SIEM y con ello, poder validar el modelo de monitoreo; dichos ataques se enmarcan dentro de la clasificación de pruebas de penetración.

De acuerdo con lo anterior, se revisó en primera instancia la Guía técnica para Pruebas y Evaluación de la Seguridad de la Información del instituto NIST identificada como la SP800-115 del año 2008, de la cual se tomó su estructura de fases para la construcción de la metodología que orientará la ejecución de pruebas. En forma equivalente, se evaluó el marco de Evaluación de la Seguridad del Sistema de Información (ISSAF) del Grupo Abierto de Seguridad de los Sistemas de Información (OISSS) versión 0.2.1 del año 2006, donde igualmente se consideraron como base las fases de la metodología de pruebas de penetración. Esta misma metodología clasifica la evaluación de la seguridad del sistema de información en varios dominios y detalla los criterios específicos de evaluación o prueba para cada uno de estos dominios [27], por lo que del capítulo de controles técnicos y evaluaciones de seguridad se tomó el componente de pruebas de seguridad de contraseña que propone varios escenarios para obtener credenciales de autenticación con bajos y altos privilegios ubicando al ejecutor de pruebas en distintos roles.

Finalmente, se estudió el Manual de Metodología de pruebas de seguridad de código abierto (OSSTMM) del Instituto para la Seguridad y Metodologías Abiertas (ISECOM) en su versión 3.0 del año 2010, que se autodefine como una metodología para probar la seguridad operativa de los lugares físicos, las interacciones humanas y todas las formas de comunicación, como las inalámbricas, por cable, analógicas y digitales [28]. Como en los anteriores casos, se tomaron las etapas de ejecución de esta metodología con el fin de comparar las tres propuestas y a partir de ellas proponer una metodología propia que se expone en la sección 3.4.1 de resultados.

2.4.2 Ejecución de algunos ataques informáticos asociados a la identidad y el control de acceso

Para llevar a cabo esta tarea primero se definieron las herramientas requeridas, se realizaron las implementaciones de software para complementar la integración de las soluciones Opensource seleccionadas en el proyecto para obtener las evidencias de los ataques como alertas reportadas en el tablero de control del Siem.

2.4.3 Validación y documentación de los resultados obtenidos

Durante esta etapa final, se registraron las decisiones tomadas con cada una de las alertas recibidas en el Siem, durante la aplicación de las etapas del modelo de monitoreo propuesto. Esto con el fin de conocer el tratamiento que se le daría a cada una de las alertas en un entorno real de vigilancia de amenazas y determinar si es posible o no agilizar los procesos de respuesta a incidentes.

3. Resultados

De acuerdo con la metodología expuesta en el capítulo anterior, se presentan los resultados obtenidos en cada una de las fases:

3.1 Fase 1: Caracterización de posibles amenazas a la identidad y el control de acceso

3.1.1 Búsqueda y selección de fuentes de información

En el proceso de exploración de los catálogos de amenazas se descubrió un trabajo previo realizado por la OSA; proyecto abierto para desarrollar un modelo de arquitectura de seguridad, que planteó una tabla en el 2008 de catálogos patrocinados por el gobierno o de marcos de gestión de riesgos comerciales [7]. Se buscaron las versiones actualizadas de los catálogos, encontrando que Los catálogos del BITS y CRAMM no se encontraban disponibles a la fecha, el BSI en su compendio de protección básica de TI presenta un apéndice donde relaciona en forma muy general las amenazas elementales para la identidad y el control de acceso y el MELANI, como Centro de Reportes y Análisis para Aseguramiento de la Información de Suiza en los últimos años se encuentra dedicado a expedir reportes semestrales de los ciber incidentes y ciber riesgos más importantes. Por su parte Microsoft en su herramienta de modelado de amenazas permite crear una lista de amenazas para mitigar los posibles problemas de seguridad en el Ciclo de vida de desarrollo de seguridad de aplicaciones (SDL). Por último, se revisó el Anexo C: Tipos de Amenazas del manual de buenas prácticas del Foro de Seguridad de la información, pero al sólo poder contar con la versión 2011 del mismo, se descartó por resultar muy desactualizado.

No obstante, la búsqueda de información de organizaciones de código abierto, de libros especializados en el tema y de varias tesis de maestría permitió seleccionar (4) fuentes de información, las cuales se presentan en la tabla 3.1.1 organizadas cronológicamente. La primera fuente; proveniente de la organización que se ha convertido en referente para el

desarrollo de aplicaciones web con su OWASP Top 10, nos entrega un manual con los escenarios automatizados por software que producen efectos no deseados en las aplicaciones web, del cual tomamos el subconjunto de eventos de amenazas relacionados con las credenciales de las cuentas. Considerar esta fuente es importante, teniendo en cuenta que los ataques a sitios web han cambiado de un ciber atacante dedicado a varios bots automatizados, motivando a la fundación OWASP a publicar este manual que se ha convertido en un estándar industrial de facto en la clasificación de los bots y una mejor comprensión de todos los aspectos de la automatización web maliciosa [29].

En segundo lugar, en la tesis de maestría el autor realiza una caracterización de las principales técnicas de ataque utilizadas para el robo de credenciales, de las cuales se recogen algunas en este trabajo, soportado en que las amenazas se materializan a través de ataques que utilizan estos métodos para lograr el objetivo táctico de su acción.

A continuación, la tercera fuente dedica un capítulo a las amenazas a la autenticación como los acercamientos que un atacante realiza para penetrar a un sistema y comprometer los mecanismos usados para evidenciar que una persona, un proceso o un sistema son quienes dicen ser. En esta fuente, a pesar de que se realiza una buena colección, se debieron comprender las amenazas propuestas, toda vez que algunas se trataban más de vulnerabilidades y técnicas de ataques que la misma amenaza en sí. Sin embargo, propone varias contramedidas específicas para cada amenaza.

Finalmente, la última fuente es considerada en función del énfasis que hace sobre la relación directa de la autenticación en el control de acceso, reconociéndolo como un paso vital para garantizar los derechos del usuario a los recursos. En adición a la anterior, este libro recalca que las amenazas al control de acceso no pueden ser eliminadas al 100% porque constantemente los atacantes están ideado nuevas. Por último, aunque esta fuente sólo presenta las (3) principales amenazas al control de acceso, las conceptualiza mediante casos de la vida real que orientan en el establecimiento de indicadores de ataque en las siguientes fases.

La tabla 3.1.1 recoge las (4) fuentes descritas anteriormente:

N°	AUTOR	NOMBRE DEL DOCUMENTO/ PUBLICACIÓN/ TRABAJO	AÑO
1	Owasp	OWASP Automated Threats Handbook Web Applications version: 1.2	2018
2	Tesis de Maestría	Modelo de administración de identidad digital (IdM) sobre blockchain para la mitigación del riesgo por suplantación en sistemas e-banking.	2020
3	Sirapat Boonkrong	Authentication and Access Control: Practical Cryptography Methods and Tools (Libro)	2021
4	Mike Chapple	Access Control and Identity Management Third Edition (Book of Information Systems Security and Assurance Series)	2021

Tabla 3.1.1: Matriz de fuentes de información seleccionadas

Teniendo en cuenta que las fuentes seleccionadas corresponden a los últimos 5 años, se puede esperar que la información obtenida a partir de ellas corresponde a las últimas tendencias en cuanto a los nuevos riesgos informáticos que son producto de la evolución de las tecnologías de la información y las comunicaciones.

3.1.2 Recopilación y filtrado de amenazas

En esta etapa se recogieron las amenazas de cada fuente, se eliminaron las duplicadas o similares como el caso de Password Cracking y Password Guessing que fueron representadas por Credential Cracking y Credential Stuffing respectivamente, por tratarse del mismo concepto y entendiendo que en estas últimas se pretende encontrar tanto el nombre de usuario como la contraseña.

La lista de amenazas consolidadas se presenta en la tabla 3.1.2:

N°	AMENAZA	DEFINICIÓN
1	Account Creation	Crear múltiples cuentas para su posterior uso indebido.
2	Brute force	Técnica de ataque en la que se intenta adivinar una clave probando todas sus combinaciones posibles hasta obtener la correcta.
3	Credential Cracking	Identificar las credenciales de acceso válidas probando diferentes valores para los nombres de usuario y/o contraseñas.
4	Credential Stuffing	Intentos masivos de inicio de sesión utilizados para verificar la validez de los pares de nombre de usuario/contraseña robados.
5	Directory Traversal	Esta técnica explota la configuración de permisos en un sitio web, permitiéndole al atacante acceder a directorios superiores (padre) sin ningún control y acceder a información no autorizada.
6	DNS hijacking	En esta técnica un atacante controla y modifica un servidor DNS para que sus víctimas sean redireccionadas a sitios maliciosos (tipo phishing) y así poder obtener sus credenciales.
7	Eavesdropping	Acto de escuchar las comunicaciones privadas de otros sin su permiso.
8	Execution Code	Técnica con la que se aprovecha un programa mal escrito en su código fuente o vulnerable por su versión y se inyecta código en dicha aplicación, para que el sistema realice acciones no autorizadas.

N°	AMENAZA	DEFINICIÓN
9	Exposed passwords	Corresponde a la utilización de credenciales adquiridas ilegalmente gracias a la exposición masiva de datos de una brecha de seguridad ocurrida en otro sistema.
10	Heightened Access	La habilidad de un atacante de loguearse en un sistema bajo un nivel de acceso y explotar una vulnerabilidad para ganar un nivel superior de acceso.
11	Http Response Splitting	Técnica en la que se inyecta en los retornos de línea del protocolo HTTP para inyectar o alterar contenido del sitio web exponiendo información o induciendo al usuario a ver y ejecutar código malicioso.
12	Leaked databases	Esta técnica consiste en la utilización de credenciales y otra información asociada a la identidad digital aprovechando la revelación de grandes bases de datos que fueron previamente hackeadas.
13	LSASS - Directory attack	Técnica de ataque enfocada en obtener las contraseñas cifradas de la base de datos de un servicio de directorio activo del tipo LDAP.
14	Malware Keyloggers	Malware especializado en robar credenciales interceptando los comandos del teclado cuando el usuario está digitando su usuario y contraseña.
15	Malware Stealers	Malware especializado en el robo de información bancaria y de cualquier tipo de credenciales y datos de identificación que tenga el usuario en su dispositivo enviándolo a un servidor central.
16	Man-in-theMiddle	Este ataque intercepta la comunicación entre dos sistemas conectándose en el medio de cada uno y haciéndose pasar por cada extremo, de forma que logra interceptar los mensajes que van cifrados.
17	Pass-the-hash attack (PtH)	En esta técnica de ataque se capturan los hashes completos usados por los protocolos de autenticación (en especial Kerberos, NTLM o LanMan) y luego se reutilizan para suplantar al usuario.
18	Phishing	Este ataque se basa en la utilización de un sitio web falso que solicita y captura las credenciales del usuario y luego las pasa al atacante.
19	Physical Keylogger	Dispositivo físico conectado entre el teclado y el computador para robar credenciales interceptando los comandos del teclado cuando el usuario está digitando su usuario y contraseña.
20	Replay Attacks	El atacante copia la contraseña o credencial de una entidad y la utiliza para llevar a cabo la autenticación con la otra entidad suplantando el usuario.
21	Shoulder surfing	Esta técnica se enfoca en obtener usuarios y contraseñas simplemente mirando cuando el usuario las introduce. Literalmente: Espiar sobre el hombro.

N°	AMENAZA	DEFINICIÓN
22	Smishing	Esta técnica se basa en enviar a la víctima un mensaje de texto (SMS) para inducirla a ingresar a un sitio falso (phishing) y capturar sus credenciales.
23	Social Engineering	El atacante engaña al usuario para que revele su información confidencial para hacerse pasar por el usuario.
24	Sql Injection	Esta técnica consiste en inyectar sentencias de lenguaje SQL a sitios web que aceptan información a través de un formulario, pudiendo acceder a información sensible o incluso tener cierto nivel de acceso a la configuración del sistema.
25	Vishing	Esta técnica se basa en realizar una llamada telefónica fraudulenta induciendo a la víctima a decir sus credenciales.
26	XSS	El cross-site scripting (XSS) se aprovecha de sitios web con código mal escrito o vulnerable que no ha sido corregido, forzando la ejecución de comandos en sitios cruzados. Esto se logra alterando los mensajes de comunicación que se le envían al servidor.

Tabla 3.1.2: Listado de amenazas consolidado

Se puede observar que en total son 26 amenazas que pueden afectar la identidad y el control de acceso, con lo cual, es una muestra muy representativa y diversa de los múltiples ataques que pueden recibir estos dos elementos importantes para la identificación y permisos de un usuario.

3.1.3 Caracterización de las amenazas con los componentes de identidad y control de acceso

Acorde a la metodología fijada y considerando las amenazas definidas, se procedió a calificar los niveles de impacto sobre los componentes de la autenticación y el control de acceso, obteniendo los resultados descritos en la tabla 3.1.3. Es importante precisar que el nivel de impacto fue fijado de acuerdo al tipo ataque (descripción del mismo) con respecto a los 6 factores considerados:

N°	AMENAZA	IDENTIFICACIÓN	AUTENTICACIÓN	AUTORIZACIÓN	PERFILAMIENTO	TRAZABILIDAD	DESAPROVISIONAMIENTO	TOTAL
1	**Account Creation**	**1**	**1**	**1**	**1**	**1**	**0**	**5**
2	Brute force	1	1	1	0	0	0	3
3	Credential Cracking	1	1	1	1	0	0	4
4	Credential Stuffing	1	1	1	1	0	0	4

5	Directory Traversal	0	0	1	1	1	0	3
6	DNS hijacking	1	1	1	1	0	0	4
7	Eavesdropping	1	1	1	0	0	0	3
8	Execution Code	0	0	1	1	1	0	3
9	Exposed passwords	1	1	1	1	0	0	4
10	Heightened Access	1	1	1	1	1	0	**5**
11	Http Response Splitting	1	1	1	1	0	0	4
12	Leaked databases	1	1	1	1	0	0	4
13	LSASS - Directory attack	1	1	1	0	0	0	3
14	Malware Keyloggers	1	1	1	0	0	0	3
15	Malware Stealers	1	1	1	0	0	0	3
16	Man-in-the Middle	1	1	1	0	0	0	3
17	Pass-the-hash attack (PtH)	1	1	1	0	1	0	4
18	Phishing	1	1	1	1	1	0	**5**
19	Physical Keylogger	1	1	1	0	0	0	3
20	Replay Attacks	1	1	1	0	0	0	3
21	Shoulder surfing	1	1	1	0	0	0	3
22	Smishing	1	1	1	0	0	0	3
23	Social Engineering	1	1	1	0	0	0	3
24	Sql Injection	1	1	1	1	0	0	4
25	Vishing	1	1	1	0	0	0	3
26	XSS	0	1	1	1	0	0	3

Tabla 3.1.3: Caracterización de amenazas

De la tabla anterior podemos concluir que las amenazas más impactantes tienen que ver con la creación u obtención de las credenciales de los usuarios, toda vez que al suplantar una identidad pueden escalar fácilmente en componentes como incrementar sus niveles de permisos, obtener accesos más privilegiados y evitar los registros de sus transacciones. También se concluye que el desaprovisionamiento entendido este, como el retiro de los permisos o la eliminación de la entidad, es un componente que no se vió impactado por las amenazas seleccionadas.

Entendiendo en detalle las amenazas más importantes que obtuvieron puntaje de 5, la creación masiva de cuentas se realiza mediante los procesos de registro de cuentas en una aplicación. Posteriormente, las cuentas se utilizan indebidamente para generar spam de contenido, lavar dinero en efectivo y bienes, propagar malware, afectar la reputación, causar daños, y sesgar la optimización de los motores de búsqueda (SEO), las reseñas y las encuestas [30].

Seguidamente, el acceso elevado (Heightened Access) es la habilidad de un atacante de loguearse en un sistema bajo un nivel de acceso y explotar una vulnerabilidad para ganar un nivel superior de acceso [31]. Esta amenaza, en definitiva, obtiene una gran importancia al ganar un acceso desde la identificación de la cuenta hasta lograr obtener información sensible que se encuentra restringida a niveles superiores, incluso alternado la trazabilidad para no dejar rastro de sus operaciones.

Por último, el phishing o suplantación de identidad tomado como una de las principales técnicas para el robo de identidad busca capturar las credenciales del usuario en el caso del phishing tradicional o el robo del token del usuario en el phishing real time para enviarlos al atacante de inmediato o posteriormente [32].

3.1.4 Selección de amenazas y establecimiento de posibles IOA

Obtenidos los totales para cada una de las amenazas se seleccionaron las (3) que obtuvieron el mayor puntaje (5) en el número de componentes comprometidos y se buscaron situaciones que pueden asociarse a actividades potencialmente maliciosas y se definieron en cuanto a la cantidad, tiempo, lugar y condiciones técnicas para que fueran evidenciables y medibles en la aplicación del modelo de monitoreo.

Adicionalmente entendiendo que además del Phishing existen otras amenazas como Credential Cracking y Pass-the-hash attack (PtH), entre otras que buscan la apropiación de la cuenta, se agruparon todas estas en una categoría denominada: *Suplantación de identidad.* Los resultados obtenidos se presentan en la siguiente tabla 3.1.4:

AMENAZA	POSIBLES INDICADORES DE ATAQUE	IOA DEFINIDO
Relleno de credenciales (Credential Stuffing)	Alto volumen de intentos de inicio de sesión	20 o más intentos de inicio de sesión con una misma cuenta en 1 minuto.

	Bloqueos de cuentas por superación de los intentos de inicio de sesión	
Suplantación de identidad (Phishing, Credential Cracking, Pass-the-hash attack (PtH)	Inicios de sesión en horarios anormales o por fuera del horario laboral	Inicios de sesión en horarios por fuera del horario laboral definido de 08:00am a 6:00pm
	Inicios de sesión desde ubicaciones inusuales	Inicios de sesión desde ubicaciones geográficas diferentes a la ubicación de la oficina o la casa delimitadas en este caso para Colombia.
	Inicios de sesión desde múltiples ubicaciones en un período de tiempo corto	Inicios de sesión del mismo usuario en dos o más ubicaciones geográficas al mismo tiempo
	Cambios frecuentes de contraseña	Intentos de más de 10 cambios de contraseña para el mismo usuario hasta en 15 minutos.
Creación de cuentas (Account Creation)	Múltiples intentos de creación de cuentas desde la misma dirección IP	20 o más intentos de creación de diferentes cuentas desde la misma dirección IP dentro el rango de 15 minutos.
Acceso elevado (Heightened Access)	Solicitudes de acceso inapropiadas provenientes de cuentas estándar sin privilegios de administración	Más de 10 solicitudes de acceso a recursos que están definidos para roles o grupos de usuarios de otro nivel en un período de 30 minutos.

Tabla 3.1.4: Relación de IOA para amenazas seleccionadas

Como producto final de esta fase tenemos para las amenazas más sobresalientes algunos eventos que se tendrán en cuenta como posibles indicios de ataques informáticos en curso, que se utilizaron para validar la detección escenarios de riesgo en la aplicación del modelo de monitoreo.

3.2 Fase 2: Integración de soluciones IAM y SIEM Open Source

3.2.1 Recolección de información, comparación y selección de IAM Opensource

Como se mencionó en el capítulo de metodología, se realizaron varias búsquedas cercanas a los conceptos del “top ten de IAM”, “las mejores soluciones open Source de Identity and Access Management”, “opciones para la gestión de acceso e identidad de código abierto” y se revisaron varias páginas web de empresas de consultorías dedicadas a evaluar y enlazar las soluciones de software con las necesidades específicas de las organizaciones mediante las comparaciones de producto. Paso seguido, se examinó en la documentación de todas las soluciones propuestas si se encontraba el procedimiento para la habilitación del servicio de syslog y se validó la viabilidad de dicha configuración en la implementación de entornos contenerizados de cada una de las soluciones. De este primer filtro se obtuvieron como soluciones Open Source candidatas: FusionAuth, Keycloak, Openiam y Soffid.

A manera de contextualización general, FusionAuth es una plataforma moderna para la gestión de acceso e identidad de clientes (CIAM) que proporciona API y una interfaz de usuario web receptiva para admitir el inicio de sesión, el registro, el correo electrónico localizado, la autenticación de múltiples factores y la generación de informes [33]. Aunque sus características principales se encuentran habilitadas en la versión community, la conectividad y seguridad avanzada sólo se encuentran habilitadas para las versiones pagas, así como el soporte 7/24 y las asistencias.

Para el caso de Keycloak, hablamos de una solución de gestión de acceso e identidad de código abierto patrocinada por RedHat, lo que representa una ventaja en cuanto al diseño y soporte de su comunidad. En su documentación se define como una solución de inicio de sesión único para aplicaciones web y servicios web RESTful [34], que está basado en protocolos estándar y conexiones a directorio activo o LDAP. Posee una gran ventaja en cuanto soporta múltiples opciones de despliegue, entre las que se encuentra Docker, Podman, Kubernetes y Openshift.

Respecto a OpenIam, esta consiste en una plataforma de administración de acceso e identidad completamente integrada que se puede implementar localmente o en la nube. Sus principales características incluyen un portal de autoservicio, la autenticación Multifactor, el inicio de sesión único y la integración de APIs. La diferencia entre sus versiones community y la Enterprise es el soporte de los foros de la comunidad versus el soporte comercial bajo el cumplimiento de acuerdos de niveles de servicio.

Finalmente, la solución Soffid de acuerdo con el Instituto Nacional de Ciberseguridad (Incibe), fue catalogada por Gartner como la herramienta IAM más completa del mercado y la única que incluye PAM [35]. En su sitio web, se autodefine como plataforma IAM convergente que reúne la gestión de acceso (AM), el gobierno de identidad (IGA), el riesgo y el cumplimiento de identidad (IRC) y la gestión de cuentas privilegiadas (PAM) en una plataforma integral [36].

A continuación, para efectos de la selección se estableció un listado de las características evaluadas por las mismas empresas de consultoría para definir los mismos criterios de medición que permitieran establecer la solución más robusta en temas de seguridad y más completa en cuanto a funcionalidades que mejoren la experiencia de usuario; como la recuperación de contraseña, el inicio de sesión social y el soporte de estándares y protocolos nuevos de autenticación y autorización. La validación del soporte de estas funcionalidades se realizó contra las fichas técnicas y la documentación de cada solución IAM.

La descripción de esas funcionalidades y su valoración según la escala de calificación propuesta se encuentra en la tabla 3.2.1:

		PUNTAJE: 0: No soportado,1: Mínimamente Soportado, 2: Bien Soportado, 3: Ampliamente Soportado				
N°	**CARACTERISTICA**	**DESCRIPCIÓN**	**FUSIONAUTH**	**KEYCLOAK**	**OPENIAM**	**SOFFID**
1	Autenticación Multifactor	Utiliza dos o más métodos para validar la identidad del usuario en el inicio de sesión.	3	2	3	3
2	Inicio de sesión único (SSO)	Habilita el inicio de sesión para múltiples aplicaciones con un solo conjunto de credenciales.	2	3	3	3
3	Inicio de sesión social	Permite el inicio de sesión con las credenciales que tienen los usuarios en alguna red social.	3	2	3	0
4	Recuperación de contraseña	Permite al usuario gestionar un cambio de contraseña con herramientas como un portal de autoservicio.	0	3	2	3
5	Soporte de OpenID Connect	Protocolo que proporciona una capa de autenticación sobre OAuth 2.0 que involucra: el cliente, el usuario final y el proveedor de identidad.	3	3	3	3
6	Soporte de SAML (Lenguaje de marcado de acceso de seguridad)	Es un estándar de código abierto basado en XML para el intercambio de datos de autentificación y autorización [37].	1	2	3	3
7	Soporte de SCIM (Sistema para la gestión de identidades entre dominios)	Es un método estandarizado y automatizado para mantener sincronizadas identidades de usuario entre distintos sistemas y almacenes de datos [38].	0	0	2	3
8	Gestión de Cuentas Privilegiadas (PAM)	Permite controlar y monitorear la actividad de los usuarios privilegiados, incluido su acceso a los activos críticos y lo que hacen iniciada la sesión.	1	0	0	3
		TOTALES	13	15	19	**21**

Tabla 3.2.1: Selección de IAM Open Source

Podemos determinar entonces, que esta investigación sobre las principales características determina un nivel de funcionalidad alta para las soluciones OpenIAM y Soffid, siendo esta última la más integral al incluir funcionalidades como el Single Sign On Empresarial y la

Gestión de Cuentas Privilegiadas; la cual es soportada por pocos productos de distribución Opensource.

En consecuencia, se infiere que dicha solución permite implementar una herramienta a bajo costo que habilita varias posibilidades en cuanto al manejo de la identidad y su gobernanza para cualquier empresa.

3.2.2 Recolección de información, comparación y selección de SIEM Opensource

Tomando como punto de inicio las soluciones SIEM Opensource mencionadas, a saber; AlientVault OSSIM, Apache Metron, Mozdef y Wazuh, se tomaron dos criterios basándose en las tablas de clasificación de versiones de producto: primero que la solución no se tratara de un paquete de demostración con el fin de presentar una integración IAM-SIEM que pudiera ser implementada sin límites de tiempo en cualquier empresa, y segundo que la máquina o la imagen de la solución no presentara eliminación de funcionalidades en la versión free para poder competir en igualdad de condiciones con las otras opciones candidatas.

De esta evaluación preliminar se descartó la solución AlientVault OSSIM por sus limitaciones frente a su versión AlientVault USM, pues presenta una administración de registros limitada y no permitió la personalización de los eventos de identidad y control de acceso recibidos desde el IAM para entrenar la herramienta en la creación de alertas. En secuencia, el proyecto Apache Metron también se retiró de la lista, de acuerdo con su anuncio de retirar el proyecto desde el 2020-12 [39].

Igualmente, para el caso del proyecto Mozdef se encontró que su repositorio fue archivado por el propietario dejándolo como sólo lectura y sin mantenimiento por parte de Mozilla. La última entrada del repositorio fue realizada el 02 de noviembre de 2021 y la última versión 3.1.2 fue lanzada el 04 de octubre de 2019 [40]. Sumado a lo anterior, se pudo confrontar que en varios blogs de software Opensource como Open base y Open Source Agenda que el proyecto ya no es sostenido por su fabricante, por lo cual se suprime de la lista inicial.

Finalmente, se evaluó la solución Wazuh que, aunque se le conoce como un sistema de detección de intrusos basado en host (HIDS), en la actualidad es una solución SIEM integral que proporciona monitoreo, detección y alertas de eventos e incidentes de seguridad. Dentro de sus ventajas se encontró que utiliza varias tecnologías para la identificación de indicadores o compromisos lo cual posibilita la configuración de los indicadores de ataque definidos previamente, y adicionalmente según su documentación permite la aplicación de reglas para personalizar las necesidades de la organización lo que lo hace ajustarse a las necesidades específicas del proyecto.

Por lo anteriormente expuesto, se seleccionó a Wazuh como la solución de correlación de eventos apropiada para recibir los eventos y administrar las alertas de la solución IAM Soffid.

3.2.3 Implementación de la integración de las dos soluciones Opensource seleccionadas

De acuerdo con los totales obtenidos en la tabla 3.2.1 la solución IAM Open Source seleccionada es Soffid, que se puede implementar tipo servidor on-premise en sistemas Windows o Linux, en contenedores usando Docker o mediante Kubernetes. Para este caso se optó por la opción on-premise en servidores virtuales, con el fin de conformar una arquitectura de máquinas independientes que pueda escalar con la instalación de otras instancias requeridas en la etapa de validación del modelo de monitoreo.

Se realizaron como pasos de la implementación del sistema IAM Soffid, lo siguiente:

1. **Inicialización de la base de datos**

El motor de base de datos utilizado fue mariadb desplegado sobre Ubuntu Linux 20.04.5 en la versión 15.1. Luego en la consola del motor base de datos se creó la base de datos Soffid y se otorgó todos los privilegios al usuario administrador. Por último, fue necesario adicionar algunos parámetros en el archivo de configuración del manejador de bases de datos: my.cnf que se ubica el directorio /etc/mysql. Estos campos permiten manejar archivos grandes, incrementar el tamaño del archivo de log redo y configurar el conjunto de caracteres UTF para evitar problemas de funcionamiento. La figura 7 presenta los comandos ejecutados para realizar estas tareas descritas:

```
MariaDB [(none)]> create database soffid;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> use soffid;
Database changed
MariaDB [soffid]> grant all privileges on *.* to ADMIN_USER@'%'identified by'ADMIN_PASSWORD'with grant option;
Query OK, 0 rows affected (0.009 sec)
```

```
# Import all .cnf files from configuration directory
[mariadbd]
skip-host-cache
skip-name-resolve
max_allowed_packet=512M
innodb_log_file_size=256M
character-set-server  = Latin1
collation-server      = Latin1_general_ci
character-set-server  = utf8mb4
collation-server      = utf8mb4_general_ci
innodb_large_prefix   = 1
innodb_file_format    = Barracuda
innodb_file_per_table = 1
```

Figura 7: Parametrizaciones de la base de datos

2. Instalación de la consola IAM

De acuerdo con la documentación del fabricante, se instaló la versión actual de la consola Iam Soffid 3 con el requisito del javaruntime, sobre la misma máquina virtual con Ubuntu Linux 20.04.5 donde se instaló el motor de bases de datos y se inició el servicio soffid-iamconsole.service. Posterior a ello se configuraron los parámetros de conexión a la base de datos e inicio de sesión para el usuario de administrador con el asistente de configuración de Soffid. Las figuras 8 y 9 demuestra el proceso de instalación de la consola:

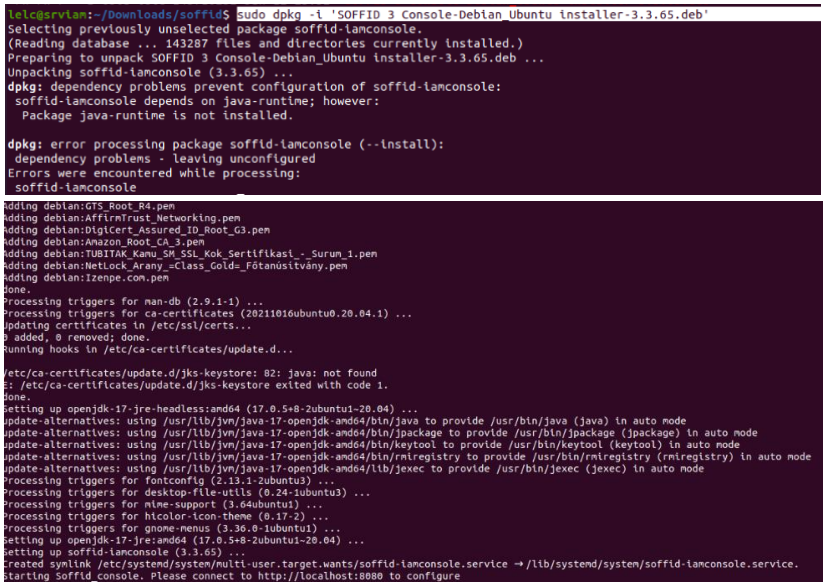

Figura 8: Instalación de la consola de Soffid 3

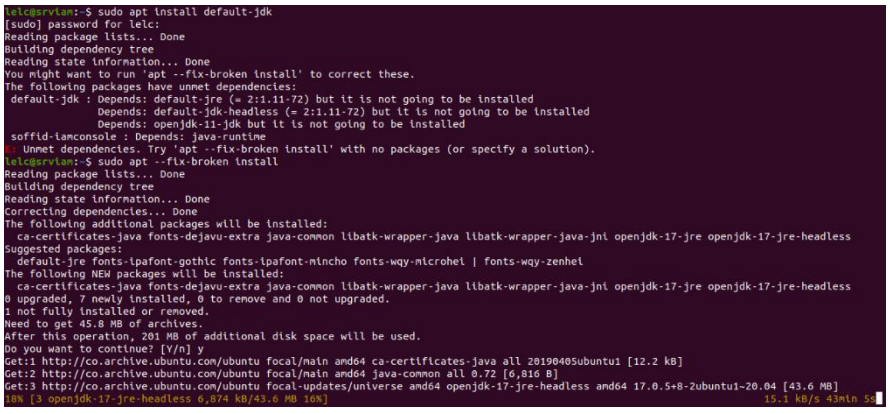

Figura 9: Instalación de java runtime

Figura 10: Configuración de la conexión a la base de datos

Figura 11: Configuración del administrador de Soffid

3. Parametrización del servidor syslog en Soffid

Por último, para la entrega de los registros de log se agregó el parámetro del servidor syslog de acuerdo con la implementación que se realizó del servidor destino que, para el proyecto, es el SIEM Wazuh. Para ello se accedió en el menú principal de Soffid a la opción Administración, luego Configurar Soffid, luego Ajustes globales y por último Parámetros Soffid. Se adicionó entonces el parámetro con los valores que se demuestran en la figura 12:

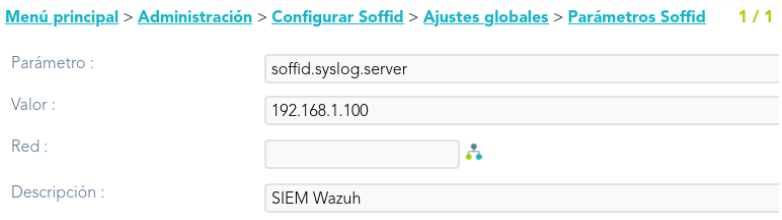

Figura 12: Configuración syslog IAM Console

Por otro lado, como se detalló en el capítulo 3.2.2 de este documento, se seleccionó a Wazuh como herramienta para el monitoreo de los eventos. Para su instalación se realizaron las siguientes actividades:

1. Instalación de Wazuh en modo single host

La plataforma de seguridad Wazuh permite dos métodos de instalación dependiendo si se quieren instalar los (3) componentes centrales en un solo servidor o cada componente en un servidor. Teniendo en cuenta que no se requiere una alta disponibilidad para distribuir los componentes en clúster, se seleccionó la instalación: single host. Se realizó entonces la implementación sobre un servidor virtual con Linux 20.04.5 instalando los componentes: indexer, dashboard y manager. En este caso como requisitos se debió contar con 8GB de memoria RAM y 50 GB de almacenamiento. El proceso de instalación con el asistente de instalación se muestra en la figura 13:

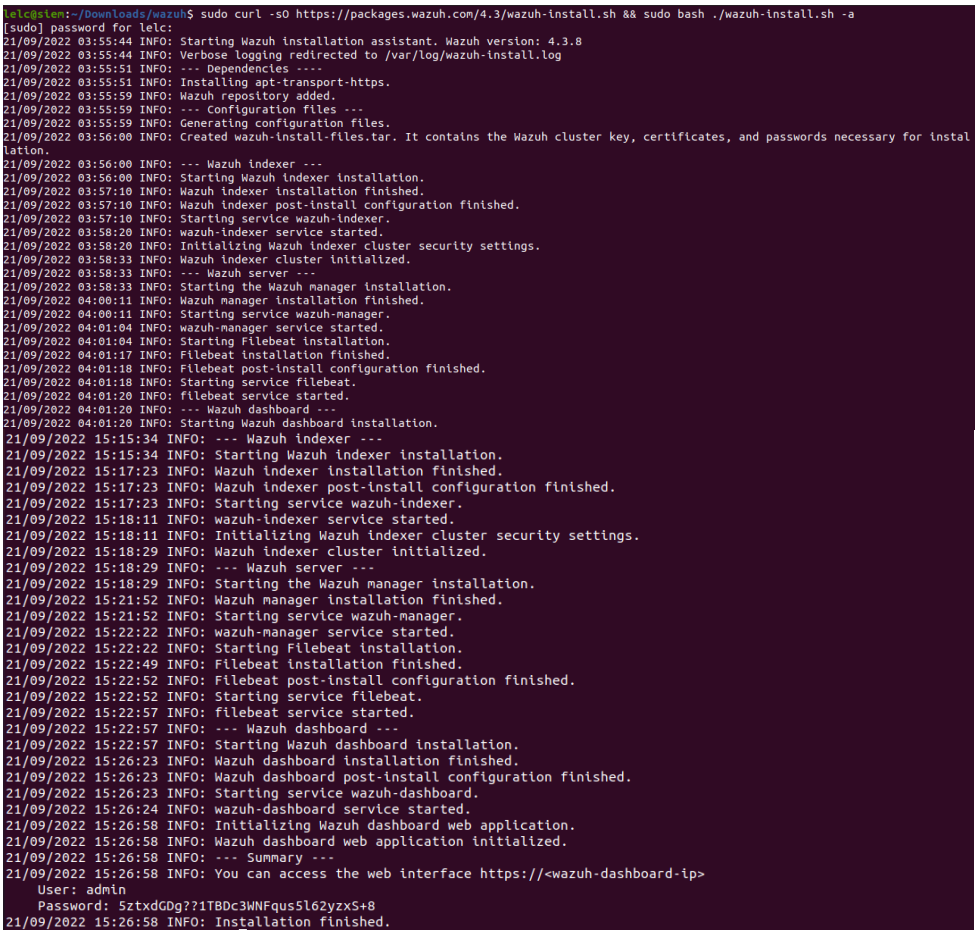

Figura 13: Instalación de Wazuh

2. Configuración de Wazuh Manager para recibir mensajes syslog

Como paso siguiente, se realizó en la máquina Linux de Wazuh la modificación del archivo de configuración general ossec.conf, ubicado en la ruta: /var/ossec/etc/ossec parametrizando las siguientes líneas en cada sección:

1. Sección: “global”
   - <logall>: Especificado en “yes” para almacenar todos los eventos incluso si estos no coinciden con alguna regla
   - <logalljason>: Especificado en “yes” con el fin de que las alertas también sean guardadas en formato json, que es el formato abierto JavaScript.

   La figura 14 muestra el estado de la sección global en el archivo después de las modificaciones requeridas:

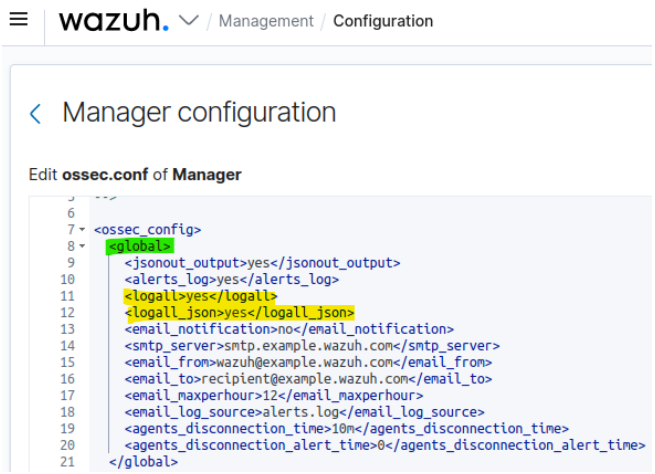

Figura 14: Configuraciones Sección global Wazuh

2. Seccion: “remote”
   - <connection>: Se modificó el valor por defecto de “secure” a “syslog”, para que de esta manera el Wazuh reciba los logs que serán enviados por este protocolo desde la solución Iam Soffid.
   - <port>: En vista de que el cliente Rsyslog que opera en Soffid utiliza el protocolo udp en el puerto 514, se ajustó en ese valor esta opción.
   - <protocol>: Especificarlo en udp, como se sustenta en el campo anterior.
   - <allowed_ips>: Corresponde al segmento de red o los hosts desde los cuales se permitirá la recepción de mensajes syslog, es por ello que aquí se registró la dirección ip versión 4 estática: 192.168.1.101 que corresponde al servidor Soffid.

- <local_ip>: Se parametrizó aquí la dirección ip versión 4 estática que corresponde al servidor wazuh: 192.168.1.100 que fue la dirección donde se escucharon las conexiones syslog.
- <queue_size>: Esta opción debe retirarse porque condiciona la capacidad de la cola del servicio remoto, cuando el tipo de conexión es por archivos es decir “secure” y no tipo “syslog” como en este caso.

El resultado de las modificaciones de la sección “remote” se observa en la figura 15:

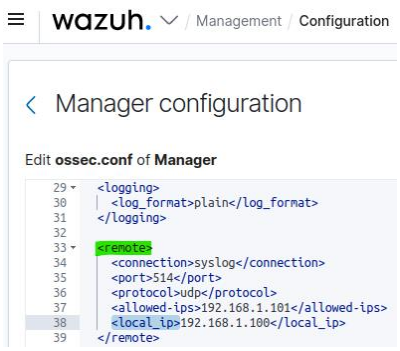

Figura 15: Configuraciones Syslog Wazuh

Cabe destacar que estas operaciones sobre el archivo de configuración general también pueden realizarse por el entorno gráfico de Wazuh, ingresando al navegador web a la url: https://localhost con las credenciales del usuario administrador y seleccionando en el menú principal la opción “management”, luego la columna “administration”, en la opción configuration.

Seguidamente, efectuados los cambios señalados se guardó y se reinició el servicio mediante la instrucción: “service wazuh-manager restart” si se realiza por línea de comandos, o mediante el botón: “restart manager” si se hace en el modo gráfico.

A continuación, se validó la recepción de los registros de logs mediante el protocolo syslog al servidor Wazuh mediante la verificación del archivo /var/ossec/logs/archives/archives.log:

Figura 16: Recepción de logs en Wazuh

Conforme a la documentación del fabricante, la habilitación del servidor syslog en los parámetros del Soffid Iam envía por defecto sólo el archivo de auditoria donde se reportan todas las acciones realizadas en la consola. Se realizó entonces la configuración del servicio de syslog tipo cliente en el Soffid Iam para enviar también todos los archivos de log ubicados en el directorio opt/soffid/iam-console-3/logs que registran todos los otros eventos como inicios de sesión exitosos y fallidos, operaciones sobre la base de datos, entre otros. Para ello se creó en el directorio del servicio de syslog: /etc/rsyslog.d un nuevo archivo para Soffid que incluyera las siguientes líneas, donde se especificaron entre otros parámetros la ruta de los archivos que se deben enviar, el protocolo, el puerto y la dirección ip versión 4 del servidor syslog que recibirá los archivos log. La estructura del archivo creado denominado: Soffid-logs.conf se muestra en la figura 17:

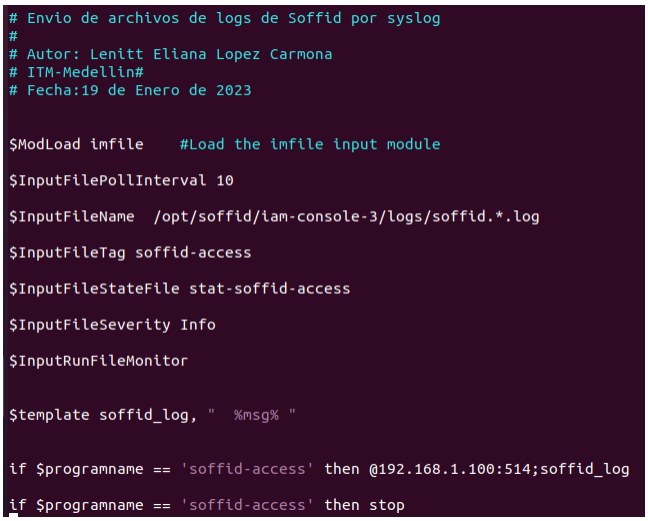

Figura 17: Configuración para reenvío de archivos a servidor syslog

Por último, se reinició el servicio de rsyslog y se verificó el contenido del archivo: /var/ossec/logs/archives/archives.log de nuevo y se pudieron ver los registros log de los otros archivos:

```
2023 Jan 22 05:06:15 siem->192.168.1.101                at jdk.proxy6/jdk.proxy6.$Proxy422.indexPendingProcesses(Unknown Source)
2023 Jan 22 05:06:15 siem->192.168.1.101                at com.soffid.iam.bpm.index.IndexerThread.run(IndexerThread.java:50)
2023 Jan 22 05:06:25 siem->192.168.1.101   22-Jan-2023 00:06:19.102 INFO [http-nio-8080-exec-3] org.opensaml.core.config.InitializationService
.initialize Initializing OpenSAML using the Java Services API
2023 Jan 22 05:06:25 siem->192.168.1.101   22-Jan-2023 00:06:20.999 INFO [http-nio-8080-exec-3] com.soffid.iam.tomcat.service.LoginServiceImpl
.authenticate master\test login rejected. Unknown account
2023 Jan 22 05:06:44 siem->192.168.1.101 1 2023-01-22T05:06:44.820Z soffiditm SOFFID - SOFFID3002 - [null] [soffiditm]Changed account admin on
 soffid
2023 Jan 22 05:06:45 siem->192.168.1.101   22-Jan-2023 00:06:20.999 INFO [http-nio-8080-exec-3] com.soffid.iam.tomcat.service.LoginServiceImpl
.authenticate master\test login rejected. Unknown account
2023 Jan 22 05:06:45 siem->192.168.1.101   22-Jan-2023 00:06:37.919 WARNING [IndexerThread] com.soffid.iam.bpm.service.BpmJobExecutorImpl$$Enh
ancerByCGLIB$$d8027c7.handleIndexPendingProcesses Error indexing
2023 Jan 22 05:06:45 siem->192.168.1.101                at org.apache.lucene.store.NativeFSLock.obtain(NativeFSLockFactory.java:171)
2023 Jan 22 05:06:45 siem->192.168.1.101                at org.apache.lucene.store.Lock.obtain(Lock.java:72)
2023 Jan 22 05:06:45 siem->192.168.1.101                at org.apache.lucene.index.IndexWriter.<init>(IndexWriter.java:695)
2023 Jan 22 05:06:45 siem->192.168.1.101                at com.soffid.iam.bpm.index.Indexer.flush(Indexer.java:114)
2023 Jan 22 05:06:45 siem->192.168.1.101                at com.soffid.iam.bpm.service.BpmJobExecutorImpl.handleIndexPendingProcesses(BpmJobExe
cutorImpl.java:217)
2023 Jan 22 05:06:45 siem->192.168.1.101                at com.soffid.iam.bpm.service.BpmJobExecutorBase$5.run(BpmJobExecutorBase.java:221)
2023 Jan 22 05:06:45 siem->192.168.1.101                at java.base/java.security.AccessController.doPrivileged(AccessController.java:318)
2023 Jan 22 05:06:45 siem->192.168.1.101                at com.soffid.iam.bpm.service.BpmJobExecutorBase.indexPendingProcesses(BpmJobExecutorB
ase.java:218)
2023 Jan 22 05:06:45 siem->192.168.1.101   22-Jan-2023 00:06:37.911 INFO [IndexerThread] com.soffid.iam.bpm.index.DirectoryFactory.isEmpty Dir
ectory /docs/index is empty
2023 Jan 22 05:06:45 siem->192.168.1.101                at java.base/java.lang.reflect.Method.invoke(Method.java:568)
2023 Jan 22 05:06:45 siem->192.168.1.101                at org.springframework.aop.support.AopUtils.invokeJoinpointUsingReflection(AopUtils.ja
va:287)
2023 Jan 22 05:06:45 siem->192.168.1.101   22-Jan-2023 00:06:37.911 INFO [IndexerThread] com.soffid.iam.bpm.service.BpmJobExecutorImpl$$Enhanc
erByCGLIB$$d8027c7.handleIndexPendingProcesses Index is empty. Regenerating
```

Figura 18: Archivo de logs de servido rsyslog

3. Configuración en el SIEM de los decodificadores y reglas para la interpretación de los mensajes syslog del IAM Soffid

Con el fin de analizar los registros entrantes y generar las alertas que corresponden, se crearon algunos decodificadores que se ajustaran a la estructura de logs de Soffid. Lo anterior se logró, adicionando en el archivo “local_decoder.xml” del Wazuh Siem, los bloques de sentencias para interpretar mediante expresiones regulares cada mensaje recibido. En la figura 19 se pueden visualizar algunos de los decodificadores creados según los eventos que suceden cuando se realizan cambios a la identidad y control de acceso:

```
<decoder name="soffid">
        <prematch>SOFFID</prematch>
        <type>syslog</type>
</decoder>

<decoder name="soffid_1">
        <parent>soffid</parent>
        <prematch>^siem</prematch>
        <regex offset="after_prematch">^->(\S+) \d (\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d.\d\d\dz) \w\w\w\w\w\w\w\w\w\w SOFFID - SOFFID\d\d\d\
d - [(\S+)] [\d\d\d.\d\d.\d.\d](\.+)</regex>
        <order>srcip,timestamp,srcuser,data</order>
</decoder>
```

Figura 19: Creación de decodificadores

A continuación, se adicionó en el archivo “local_rules.xml” las reglas para después del cumplimiento del patrón establecido por el decodificador, analizar el evento para catalogarlo dentro de una alerta y presentarla en el tablero de control del Wazuh Siem. La figura 20 representa algunas de las reglas creadas para el tratamiento de los eventos acordes al proyecto:

```
<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<group name="soffid">
        <rule id="100002" level="5">
                <match>login rejected. Unknown account</match>
                <description>Soffid:usuario no habilitado</description>
        </rule>

        <rule id="100003" level="5">
                <match>Create user</match>
                <description>Soffid:Creacion de usuario</description>
        </rule>

        <rule id="100005" level="5">
                <match>login rejected. Invalid password</match>
                <description>Soffid:Contrasena invalida</description>
        </rule>

        <rule id="100006" level="5">
                <match>login accepted</match>
                <description>Soffid:Inicio de sesion exitoso</description>
        </rule>

        <rule id="100007" level="7">
                <match>Granted rol SOFFID_ADMIN</match>
                <description>Soffid:Cambio de rol</description>
        </rule>

</group>
```

Figura 20: Creación de reglas

Como resultado de las configuraciones anteriores, se visualizó que cuando se realizaron cambios con las identidades del Soffid dentro de la consola del Iam, que estas alertas ya aparecen en el dashboard del Wazuh Siem en la figura 21:

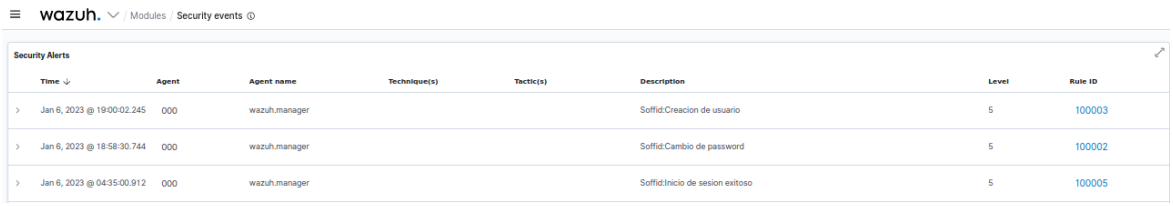

Figura 21: Eventos en el dashboard de Wazuh

3.3 Fase 3: Construcción del modelo de monitoreo

Durante esta actividad se dio lectura a las normas, publicaciones y guías sobre buenas prácticas para la definición, implementación y seguimiento al programa de monitoreo continuo de la seguridad de la información para posteriormente proponer un modelo de monitoreo. A continuación, se presentan los resultados de las actividades propuestas:

3.3.1 Búsqueda y selección de estándares y guías

En primera instancia, de la ISO se abordaron las normas sobre la gestión de seguridad y riesgos 27001 y la 27005. La primera, que describe las fases para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) nos resalta como punto de partida la identificación de activos y la tipificación de amenazas, luego el análisis del impacto, la implementación de controles y el tratamiento del riesgo. Por su parte la norma ISO 27005 aportó aspectos esenciales del monitoreo a los riesgos en la etapa “Check” del ciclo PDCA que son las verificaciones de nuevos activos, nuevas amenazas, la probabilidad de explotación de vulnerabilidades y el seguimiento a los incidentes de seguridad de la información. Finalmente, a pesar de que ambas normas ofrecen principios y marcos de referencia para la gestión de riesgos no aportan elementos detallados sobre la actividad específica del monitoreo.

En segundo lugar, se examinaron las publicaciones especiales NIST 800-61 revisión 2 y la NIST 800-137. De la primera, denominada “Computer Security Incident Handling Guide” se tomó en cuenta el ciclo de vida de respuesta a incidentes donde se contemplan las fases que se deberían adelantar para prepararse, detectar, analizar, contener, erradicar y recuperarse ante la ocurrencia de un incidente de seguridad de la información. Igualmente, de la segunda publicación titulada: “Information Security Continuos Monitoring (ISCM) for Federal Information Systems and Organizations”.

De la revisión de otras publicaciones relacionadas, se seleccionó el documento: “Cybersecurity Incident Response Playbook” de la agencia Cybersecurity and Infrastructure Security (CISA) que propone un proceso a manera de flujo para la respuesta a incidentes que se basa en el estándar NIST 800-137 que se tomó como referente pero que se adapta adecuando los requisitos propios del modelo de monitoreo para eventos de identidad y control de acceso e incorporando la clasificación de alertas para la asignación de puntajes de riesgo.

Las fuentes de información seleccionadas se encuentran relacionadas en la siguiente tabla 3.3.1:

N° FUENTE	AUTOR	NOMBRE DEL DOCUMENTO/ PUBLICACIÓN/ TRABAJO	AÑO
1	NIST	Computer Security Incident Handling Guide NIST SP800-61 revision 2 Capitulo 3.2	2012
2	CISA	Cybersecurity Incident Response Playbook	2021

Tabla 3.3.1: Matriz de estándares y guías seleccionadas

3.3.2 Creación del modelo de monitoreo

El modelo de monitoreo propuesto establece que en la etapa de preparación se deben establecer las herramientas y recursos requeridos; a saber, la integración entre las soluciones IAM y SIEM, el acceso a la solución IAM para realizar consultas sobre el contexto de las alertas y por último el personal entrenado para la atención específica de eventos sobre la identidad y control de acceso. Los anteriores se definen como requisitos, necesarios para poder operar el modelo.

Posteriormente, en las fases de detección y análisis se inicia tomando decisiones sobre las alertas utilizando la siguiente escala: 4 para las alertas donde la cuenta de usuario pertenece al grupo de cuentas de acceso privilegiado que fueron definidas para este proyecto como las cuentas de los administradores de las áreas de TI o las cuentas comerciales que requieren acceso a sistemas confidenciales como finanzas, recursos humanos que asignan, modifican o eliminan los roles a los usuarios en el IAM. Si la alerta no coincide con estas cuentas se evalúa si ésta consiste en intentos de acceso a recursos como sistemas de información, carpetas compartidas, impresoras, entre otros, a los cuales el usuario no tiene acceso dentro de la definición de su rol, en cuyo caso afirmativo se asigna el puntaje 3. Seguidamente, si la alerta no clasifica en los casos anteriores, se evalúa si las alertas obedecen a reportes sobre ataques a cuentas de usuario como inicios de sesión fallidos, múltiples intentos de cambios de contraseña, inicios de sesión en ubicaciones geográficas diferente a las definidas, entre otros, a los cuales se les asignará el puntaje de riesgo 2. En último término, se establecerá el puntaje 1 para las alertas restantes por tratarse de eventos que no se relacionan a las amenazas priorizadas en las etapas iniciales de este proyecto.

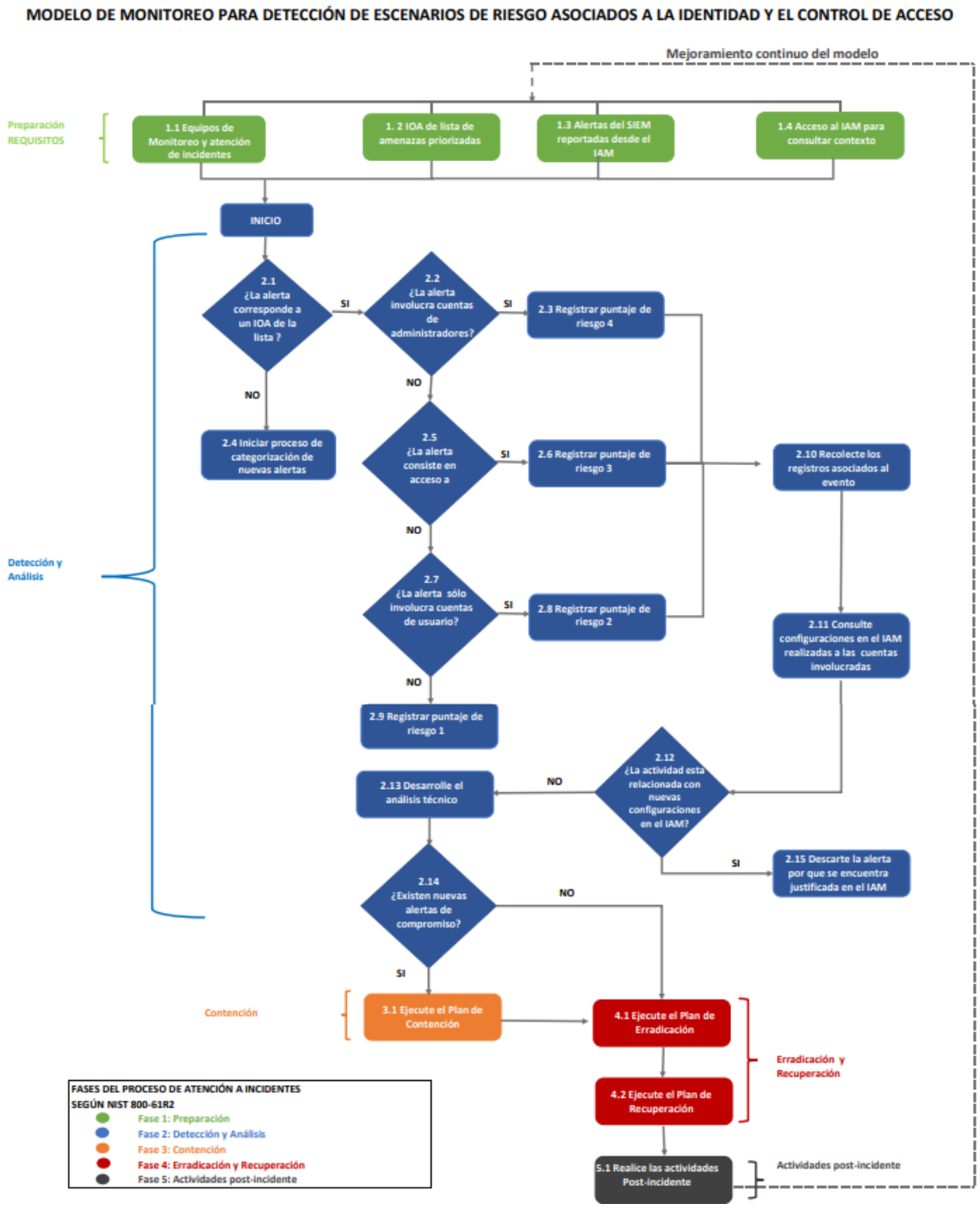

Figura 22: Modelo de monitoreo propuesto

3.4 Fase 4: Validación de detección de escenarios de riesgos con la aplicación del modelo

Para ejecutar la simulación de ataques informáticos propuesta en esta fase, se hace necesario primero definir el procedimiento basado en las metodologías referenciadas, luego ejecutar algunos ataques relacionados a las amenazas ya caracterizadas para que de acuerdo al modelo de monitoreo presentado en este proyecto se pueda asignar manualmente un puntaje de riesgo y se señale el flujo de trabajo que debe seguirse en un proceso de atención de incidentes aprovechando los beneficios de la integración de las soluciones Opensource implementadas. Los resultados conseguidos se presentan a continuación:

3.4.1 Construcción de la metodología de pruebas de seguridad

De acuerdo con lo planteado en el capítulo anterior, se seleccionaron tres metodologías y se obtuvo la secuencia de pasos que cada una propone para la realización de pruebas de seguridad. El resumen de esta investigación se presenta en la siguiente tabla:

Metodología NIST SP800-115	Metodología ISSAF	Metodología OSSTMM
Fase 1: Planeación Fase 2: Ejecución Fase 3: Post-ejecución	Fase 1: Planeación y preparación Fase 2: Evaluación Fase 3: Elaboración de informes, limpieza y destrucción de artefactos	Fase 1: Iniciación Fase 2: Interacción Fase 3: Investigación Fase 4: Intervención

Tabla 3.44.1.1: Tabla resumen de fases para las metodologías referentes

Con base en la información anterior se elaboró una metodología propia que propone las fases de planeación, evaluación y post-evaluación. En la siguiente tabla se describe cada etapa y se detallan los criterios y evidencias de cada una de ellas para el proyecto:

Fase de la metodología	Descripción	Detalle
Fase 1: Planeación	Consiste en la recolección de la información relevante para elaborar el plan de evaluación donde se definen: los activos, las amenazas, la selección de los objetivos (target) y las técnicas y tácticas de ataque que podría aplicarse.	**Inventario de Activos:** De hardware: Servidor Siem, Servidor Iam Console De Software: Base de datos del Iam, Sistema Iam Console, Sistema Siem **Amenazas asociadas a los activos:** Acceso no autorizado por contraseñas locales débiles o las establecidas por defecto, denegación de servicio por desbordamiento de recursos, operación

		inadecuada del servidor o el software por infección con código malicioso. **Objetivo (target) seleccionado:** Sistema Iam Console **Técnicas y tácticas de ataque seleccionadas de acuerdo con la matriz Mitre Att&ack:** Relleno de credenciales (T1110.004), suplantación de identidad (T1566), escalada de privilegios (TA0004) y la creación de cuentas (T1136).
Fase 2: Evaluación	En esta etapa se lleva a cabo las pruebas de penetración definidas en el plan de evaluación realizando las actividades asociadas a las técnicas de ataque seleccionadas.	El detalle de las actividades realizadas se incluye en el apartado 3.4.2 del presente documento.
Fase 3: Post-evaluación	Por último, en esta fase se documentan los resultados obtenidos y se elaboran los informes.	El informe debe recoger los hallazgos y presentar recomendaciones de controles para mitigar las situaciones encontradas.

Tabla 3.44.2.2: Metodología de pruebas de seguridad propuesta

3.4.2 Ejecución de algunos ataques informáticos asociados a la identidad y el control de acceso

Conforme a la metodología de pruebas definida en el capítulo anterior, en la fase de evaluación se encuentran las pruebas de penetración. Para este proyecto las pruebas realizadas corresponden a una simulación con el fin de visualizar frente a la presentación de algunos ataques informáticos asociados a la identidad y el control de acceso, cuál sería el comportamiento de la integración realizada de las soluciones IAM y SIEM y cómo tratar las alertas que generen de acuerdo con el modelo monitoreo propuesto.

Para lograr lo anterior, primero se definieron como herramientas el escáner de aplicaciones web de Owasp llamado Zed Attack Proxy (ZAP) y la extensión de Firefox Foxyproxy. La primera, además de las herramientas automatizadas, brinda la capacidad de diseñar y enviar pruebas manuales contra la aplicación web de destino para que el probador de penetración pueda ajustar sus pruebas [41]. Por su parte, foxyproxy nos permitirá redirigir la navegación que se realice desde la página del Iam Console al Owasp Zap que estará operando como proxy.

De acuerdo con los resultados obtenidos en la tabla 3.1.4, las amenazas seleccionadas de acuerdo a su puntaje fueron el relleno de credenciales (credential stuffing), la suplantación de identidad (Phising, Credential Cracking, Credential Stuffing, Pass-the-hash attack (PtH), la creación de cuentas (Account Creation) y el Acceso elevado (Heightened Access). En concordancia, se presentan a continuación los ataques informáticos realizados para cada una de ellas:

3.4.2.1 Ataque de relleno de credenciales

En primer lugar, teniendo en cuenta que se seleccionó como objetivo de ataque o target la consola de administración de Iam Soffid, se accedió a la página de acceso para tomar la dirección web y los campos del formulario:

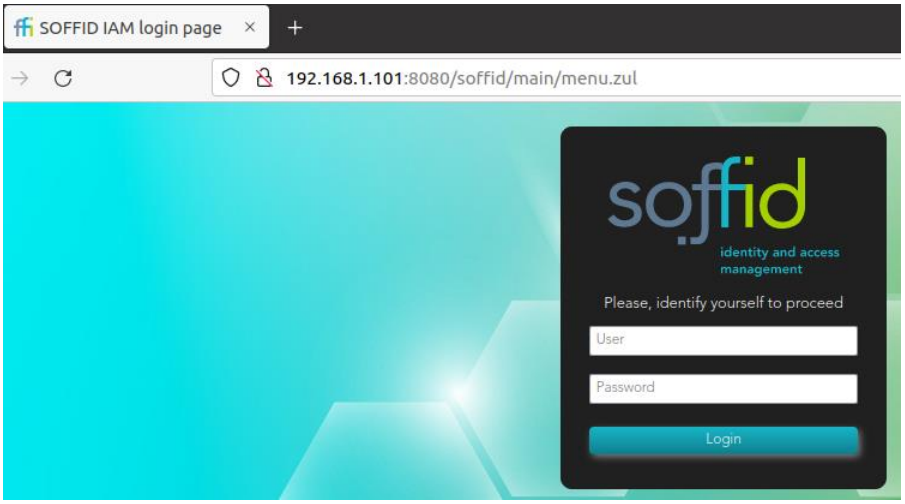

Figura 23: Formulario de acceso Consola Soffid

A continuación, se instaló y configuró la extensión Foxy proxy del navegador Firefox, para permitir al Zap proxy la captura del tráfico http. Para ello, se seleccionó la opción “add” y se configuraron los campos como se muestran en la figura 24:

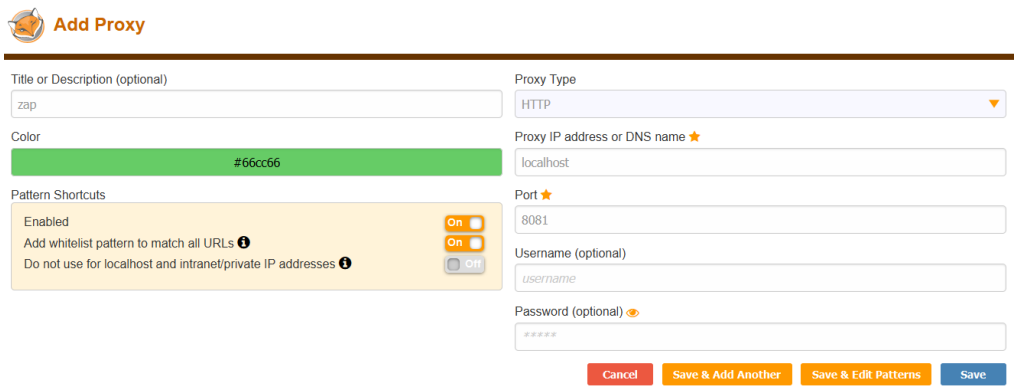

Figura 24: Configuración de Foxy proxy

Igualmente, se configuró en la herramienta Owasp Zap el proxy local con el mismo número de puerto especificado en el Foxy proxy, mediante la selección del menú Herramientas, luego en opciones, seguidamente la sección de Network y debajo de ella la opción: Local servers/Proxies. Allí se configuraron los parámetros de dirección y puerto como lo demuestra la figura 25:

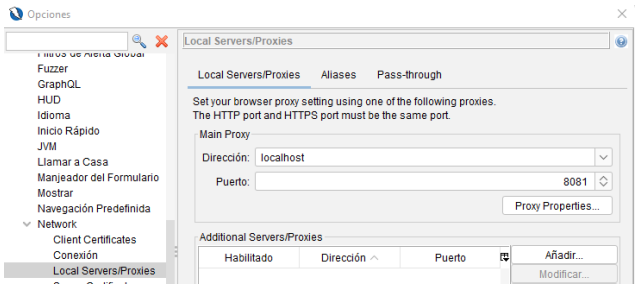

Figura 25: Configuración de Proxy en Zap

Luego, se obtuvo un mensaje de advertencia del Firefox de la falta de una conexión segura, a lo cual se seleccionó la opción de avanzado y aceptar el riesgo y continuar con el fin de poder habilitar el entorno de pruebas:

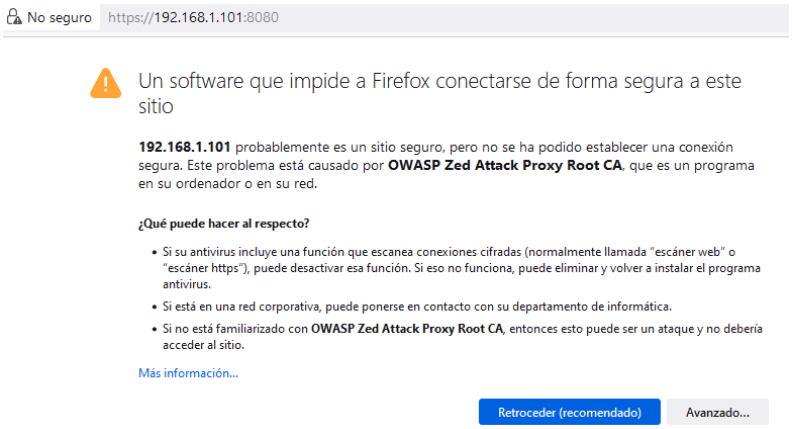

Figura 26: Advertencia de sitio no seguro Firefox

A continuación, se realizó en Owasp Zap la configuración del sitio, seleccionando la opción exploración manual del menú de bienvenida, especificando en el cambo “url a explotar” la dirección del formulario de acceso anterior y luego iniciar el navegador Firefox:

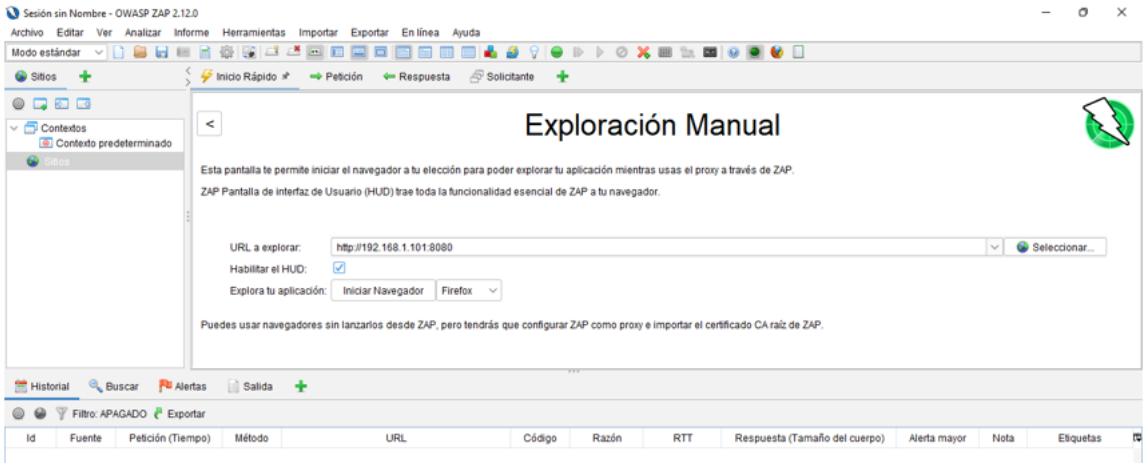

Figura 27: Configuración de Sitio para ataques en Zap

En este caso se utilizó la opción de fuzzing, que permite enviar muchos datos no válidos o inesperados a un objetivo, que para nuestro primer ataque será un envío de usuarios y contraseñas para realizar un relleno de credenciales (credential stuffing). Para ello se seleccionó en la opción herramientas, la opción Fuzz como lo muestra la figura 28:

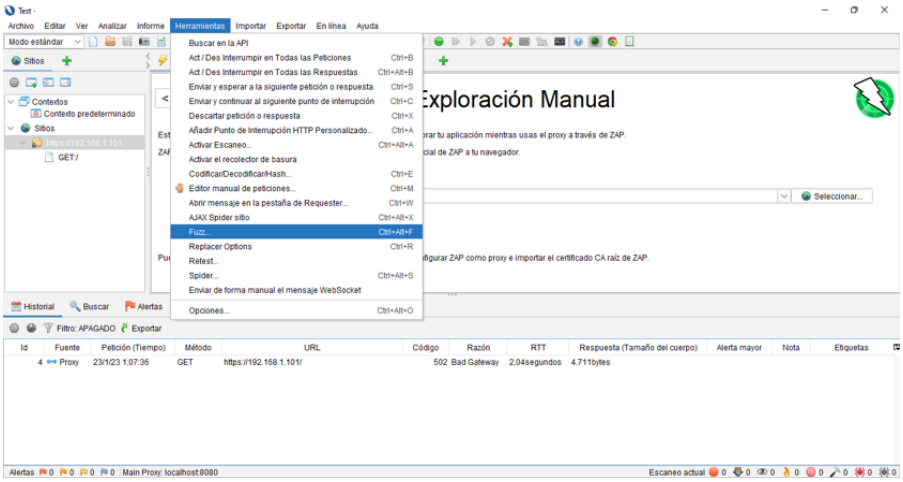

Figura 28: Selección de herramienta de fuzzing

Después, se seleccionó el sitio:

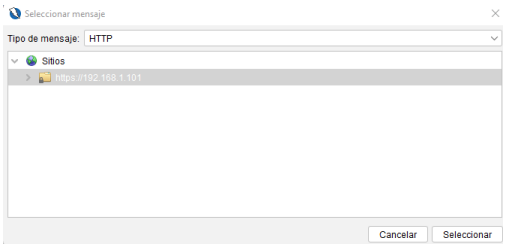

Figura 29: Selección del sitio destino del ataque

Luego se ingresaron un usuario y contraseña en los campos del formulario de logueo de la consola del Soffid Iam para capturar el método POST que se envía a la página:

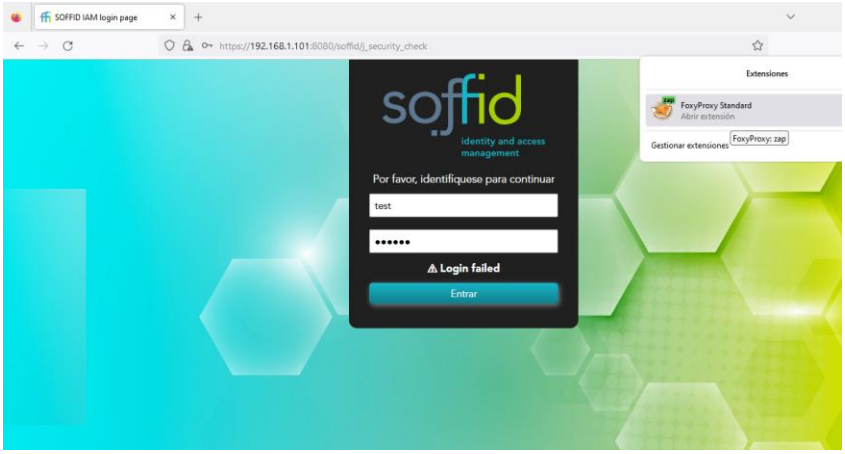

Figura 30: Generación de evento POST

A continuación, se buscó debajo de la carpeta del sitio el método “post” que corresponde a la autenticación realizada, luego se seleccionó la opción Atacar y luego Fuzz para configurar el ataque:

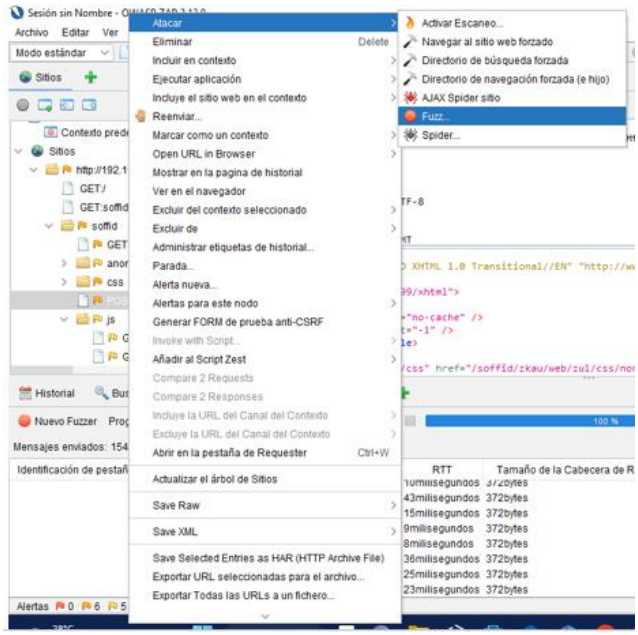

Figura 31:Selección de ataque Fuzz

Luego, en la ventana del Fuzzer se editó la cabecera del request del método post y se resaltó el nombre de usuario digitado en campo del formulario de “j_username”, que en este caso fue “test”:

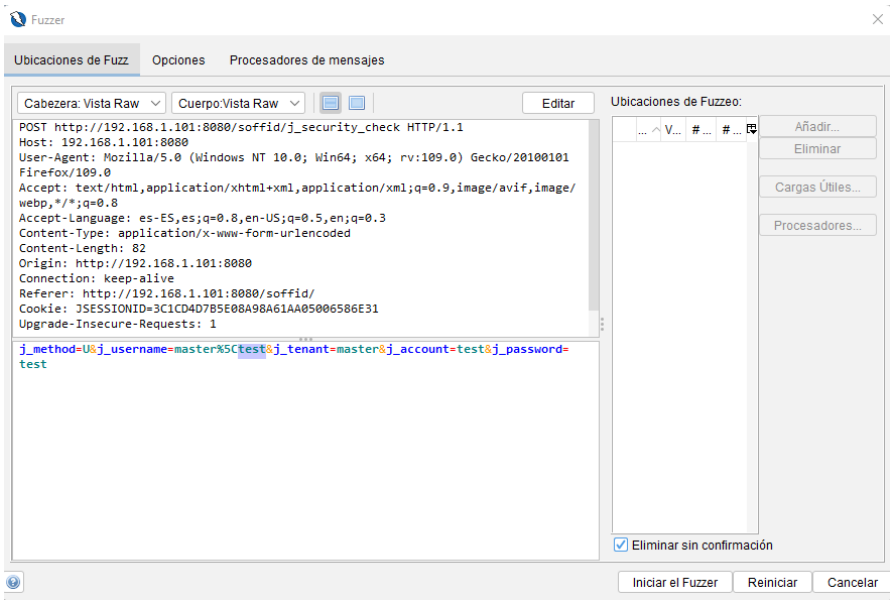

Figura 32:Selección del campo j_username

Después, se seleccionó el botón añadir y se creó una carga útil de usuarios tipo cadena para reemplazar ese campo y tratar de encontrar un usuario válido:

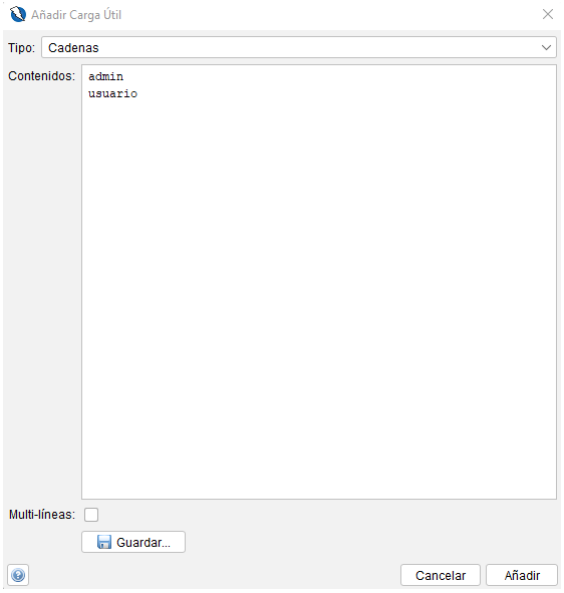

Figura 33: Carga de cadena para campo j_username

De igual manera, se realizó el mismo proceso seleccionando en el campo “j_account” la palabra “test” y se creó la carga útil tipo cadena con la misma lista de usuarios del paso anterior:

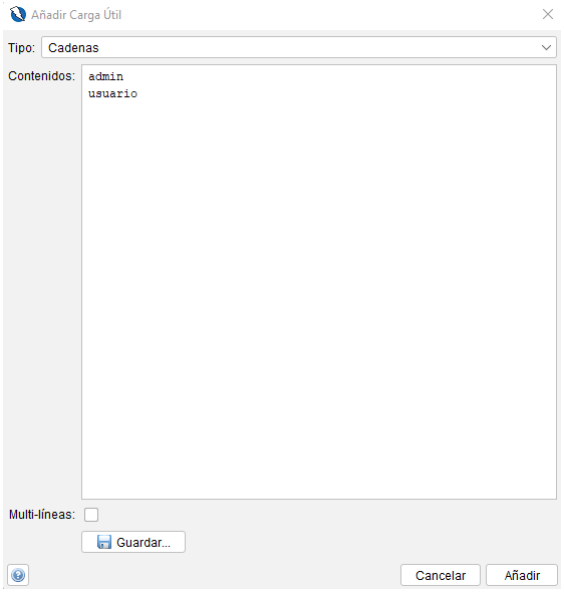

Figura 34: Carga de cadena para campo j_account

Luego, se seleccionó el contenido del campo “j_password” y se creó la carga útil tipo cadena con la lista de contraseñas:

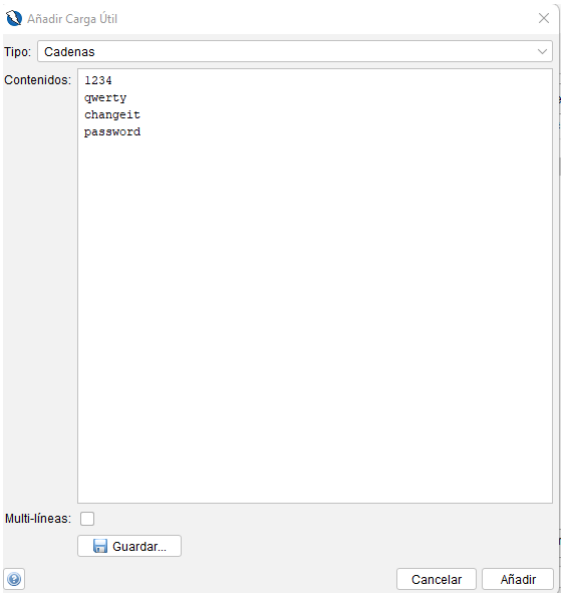

Figura 35: Carga de cadena para campo j_password

Después de tener los dos parámetros configurados como lo demuestra la figura 36, se seleccionó el botón iniciar el Fuzzer:

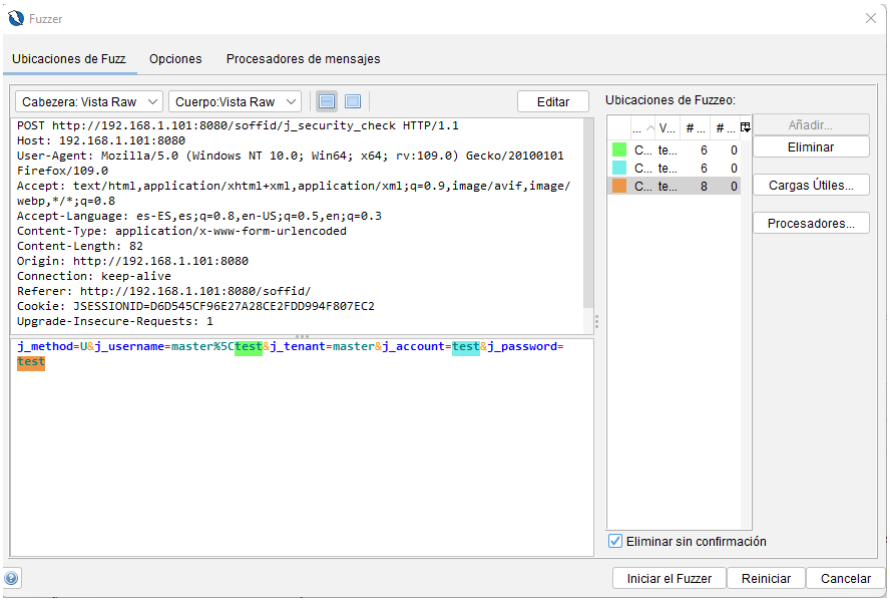

Figura 36: Inicio del proceso de fuzzer

Posteriormente, se obtuvo entonces los intentos de inicio de sesión contra el formulario de inicio de sesión en el Zap con las cadenas cargadas para los campos:

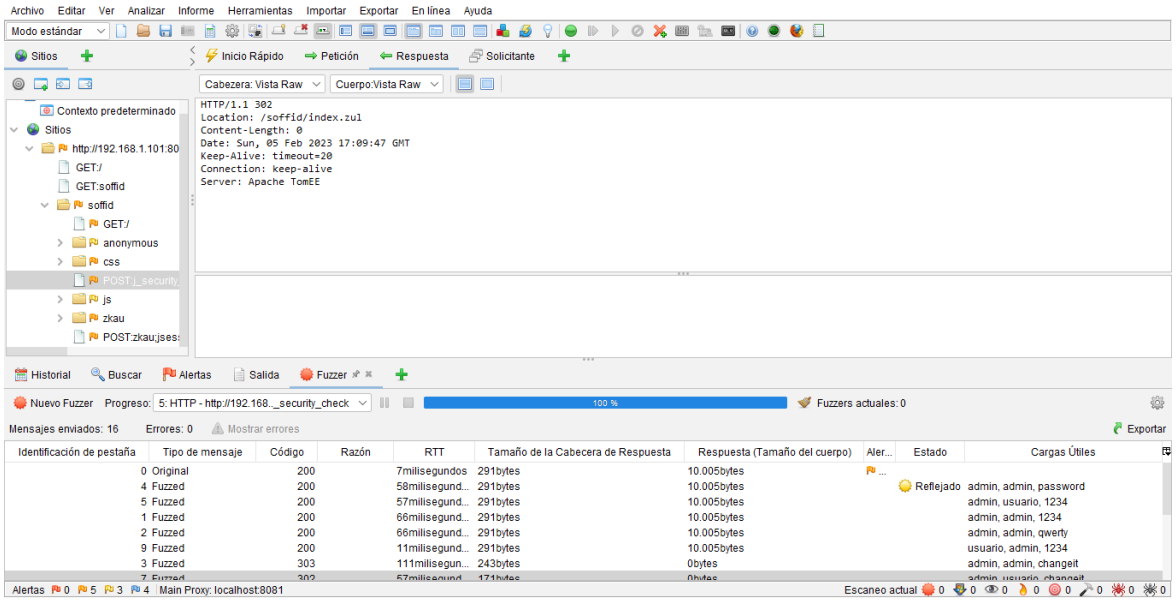

Figura 37: Resultado del Fuzzer

Luego, se ubicó la existencia de un mensaje con código de respuesta “302”, lo que indica que las credenciales fueron aceptadas y se entregó una redirección a una URL diferente para el usuario. Se verificó en la respuesta del mensaje el campo: location para conocer la url:

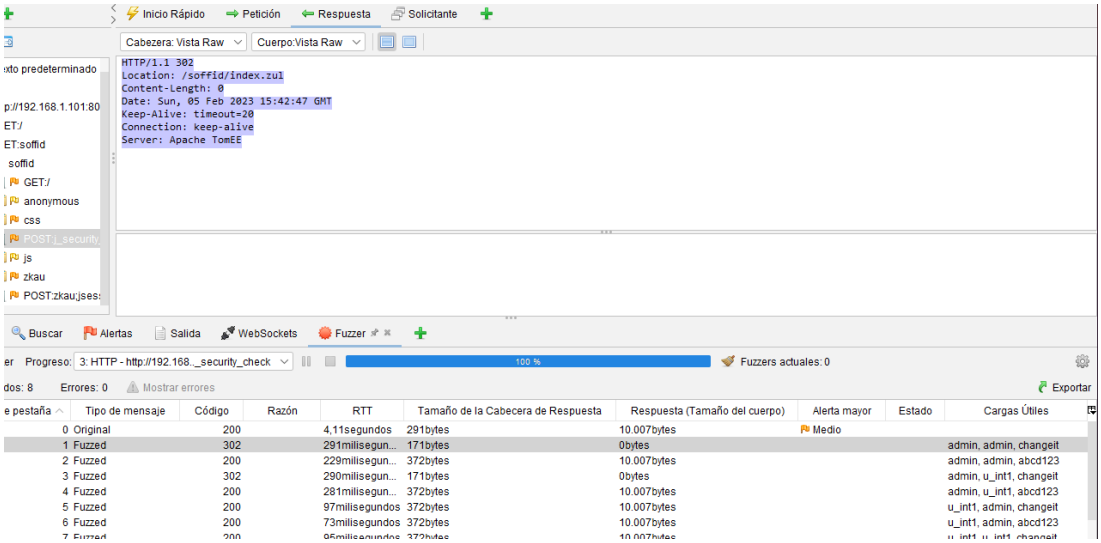

Figura 38: Selección de mensaje 302

A continuación, se verificó el acceso al login de la consola de Soffid con las credenciales obtenidas en el proceso de fuzzer y especificando en la url el campo “location” del mensaje http 302:

Figura 39: Acceso con credenciales del fuzzer

Por consiguiente, se obtuvo acceso al menú principal de la consola como se evidencia en la figura 40:

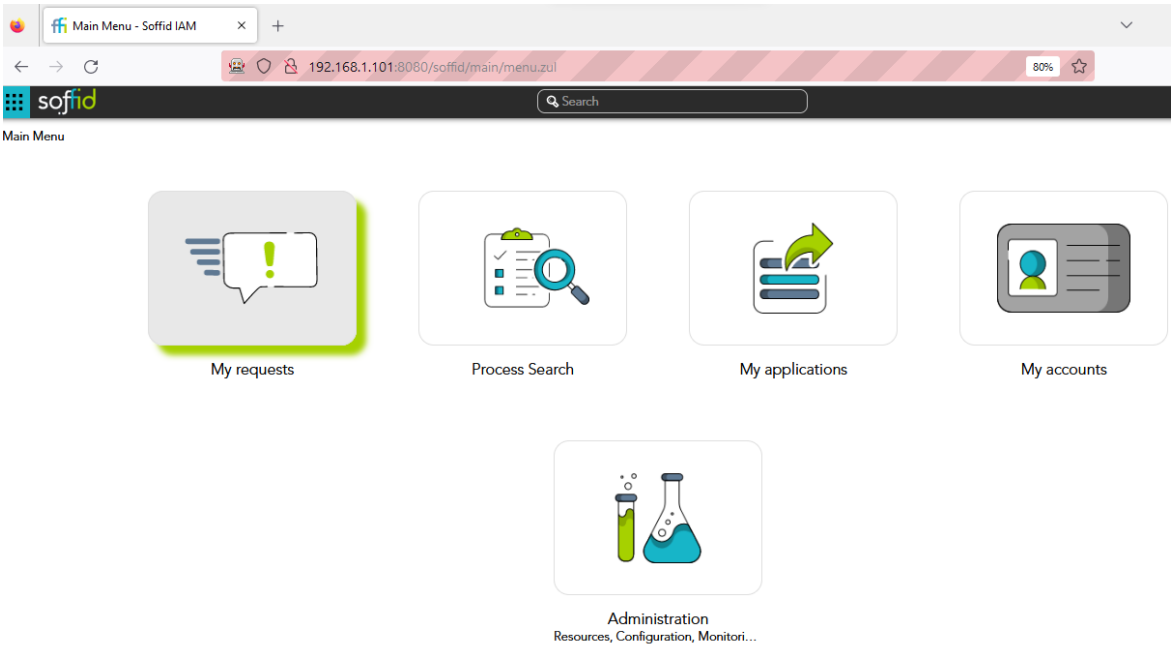

Figura 40: Menú principal Soffid

Finalmente, en lo que respecta a las alertas generadas por el ataque, se visualizaron las notificaciones de alertas en el Siem Wazuh del ataque de relleno de credenciales:

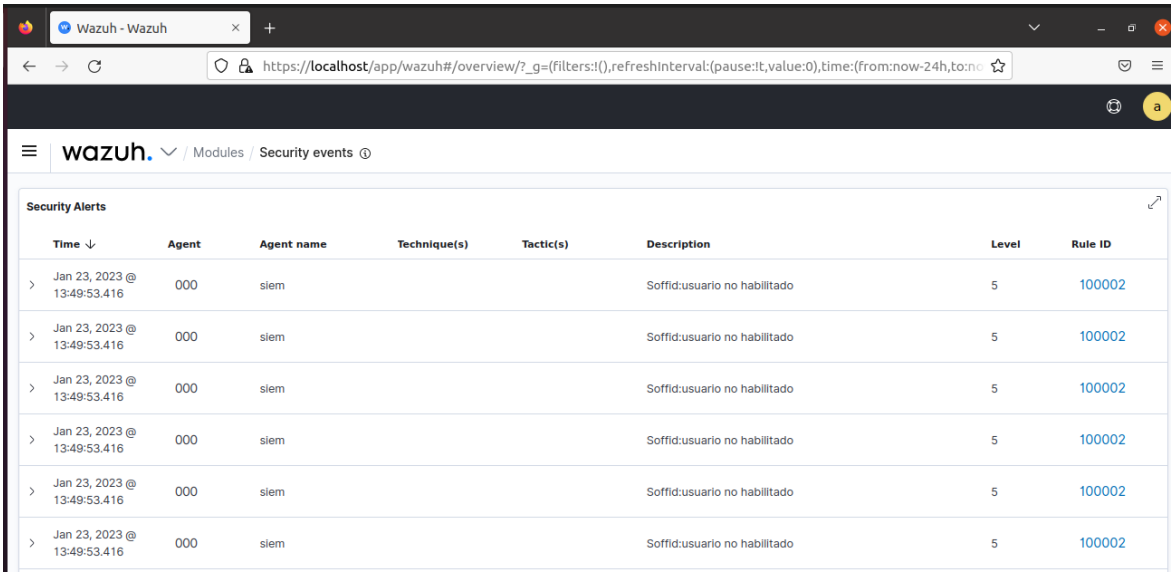

Figura 41: Alertas del ataque de relleno de credenciales en el SIEM

3.4.2.2 Ataque de suplantación de identidad

De acuerdo a la figura 38, donde se observan los resultados del Fuzzer, se logró un acceso con las credenciales del usuario: admin. En este caso, sin el conocimiento de unas credenciales validas se adivinaron las credenciales de acceso a la consola mediante el uso de una lista de contraseñas comunes. Se procedió con el ataque de suplantación de identidad usando las credenciales para obtener el ingreso al menú principal de la consola Iam que se presenta en la figura 42:

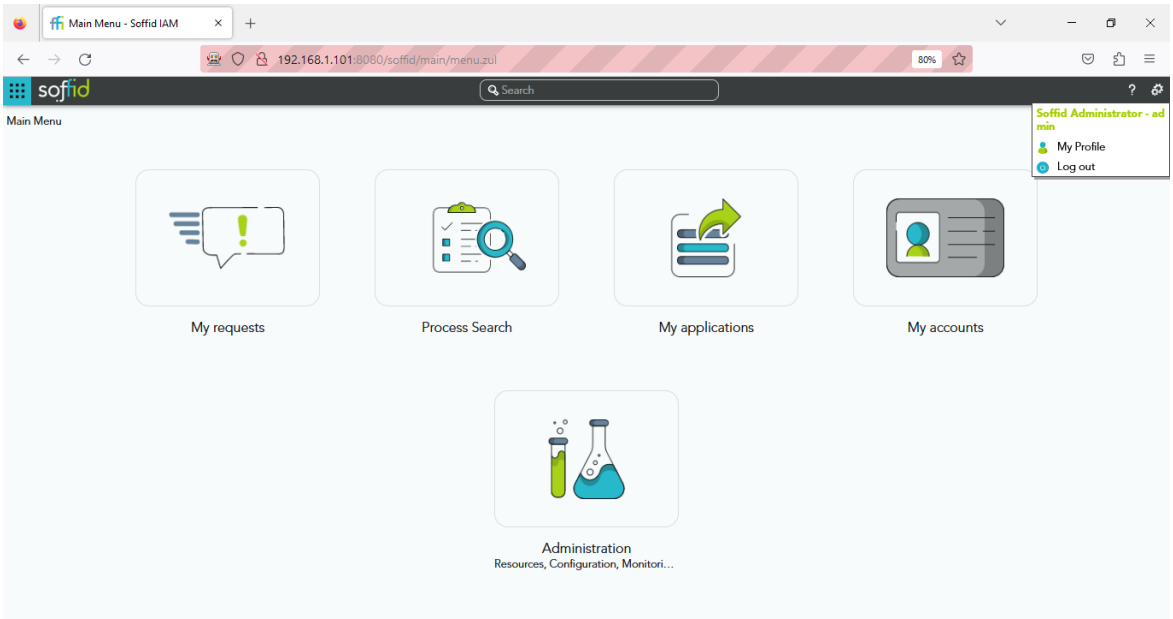

Figura 42: Acceso usuario admin consola Soffid

Como consecuencia, se generó la alerta en el tablero de control del Siem del acceso al sistema:

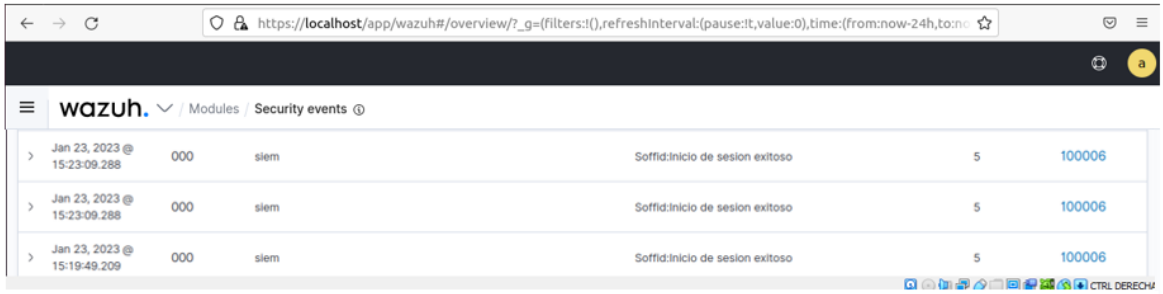

Figura 43: Alerta de acceso exitoso en el SIEM

Se concluye entonces, que cuando se comprometa alguna credencial de los usuarios la alerta de inicio de sesión también será reportada en el panel de eventos del Siem, para que, posteriormente se pueda verificar si se tratan de inicio de sesión autorizados o no.

3.4.2.3 Ataque de creación de cuentas

A este punto, con el acceso conseguido de un usuario administrador se pueden realizar todas las operaciones de creación, actualización y eliminación de usuarios. Se realizó entonces el proceso de creación de cuentas seleccionando la opción Administración, luego recursos, y por último usuarios. La figura 44 muestra el proceso para la creación de un usuario del tipo interno que pertenezca al grupo Enterprise:

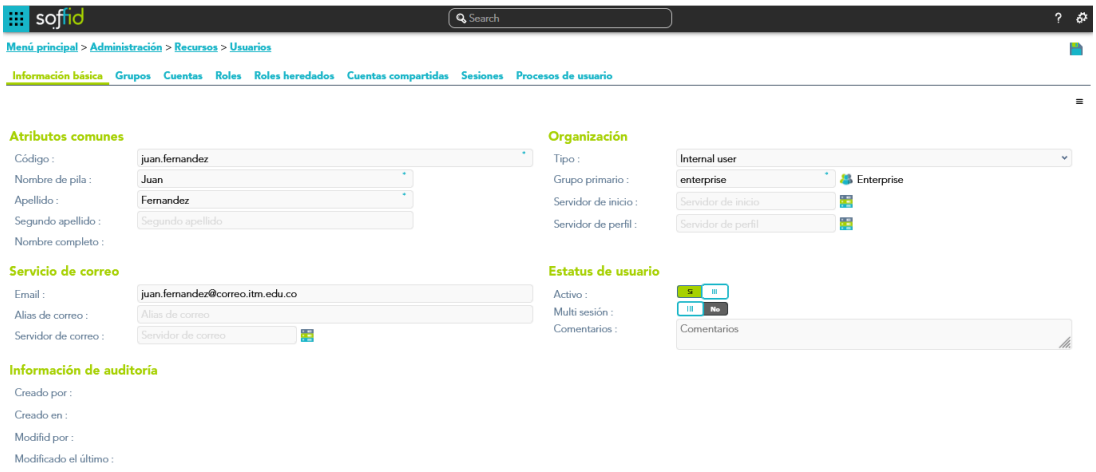

Figura 44: Creación de usuario Soffid

Posteriormente, se revisaron los eventos de seguridad del Wazuh y se observó que se generó la alerta en el tablero de control de la creación del nuevo usuario, como se observa en la figura 45:

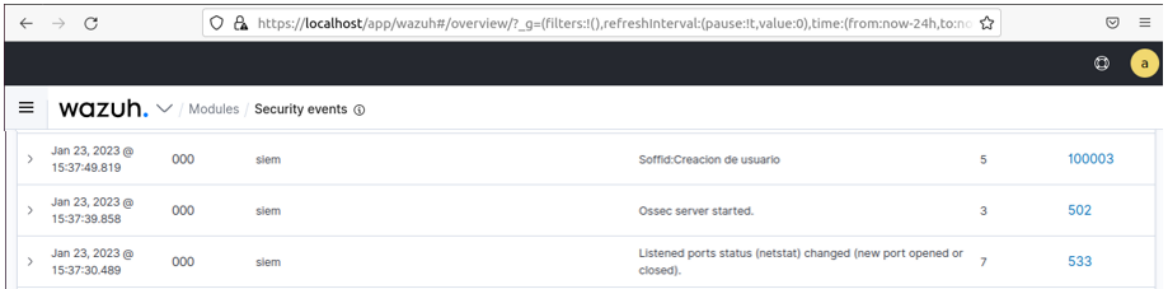

Figura 45: Alerta de creación de usuario

Así pues, se concluye que para visualizar este tipo de operaciones se hace necesario la inclusión de todos los archivos de log generados por el Iam para tener una cobertura total de todos los eventos que puedan afectar las identidades administradas.

3.4.2.4 Ataque de acceso elevado o elevación de privilegios

Con el fin de mantener el acceso, los atacantes utilizan técnicas como la persistencia y la escalada de privilegios, para lo cual crean varias cuentas y les otorgan permisos de nivel superior. Para este caso, se continuó con el cambio del rol del usuario creado en el paso anterior, para convertirlo en usuario administrador de Soffid para gestionar todas las configuraciones de la consola:

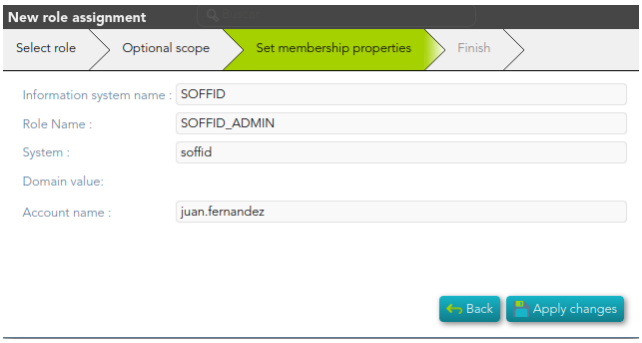

Figura 46: Asignación de rol soffid admin

En forma similar a las anteriores, se validó que la operación de elevación del rol a administrador de Soffid, diera lugar a la alerta en el tablero de control del Wazuh:

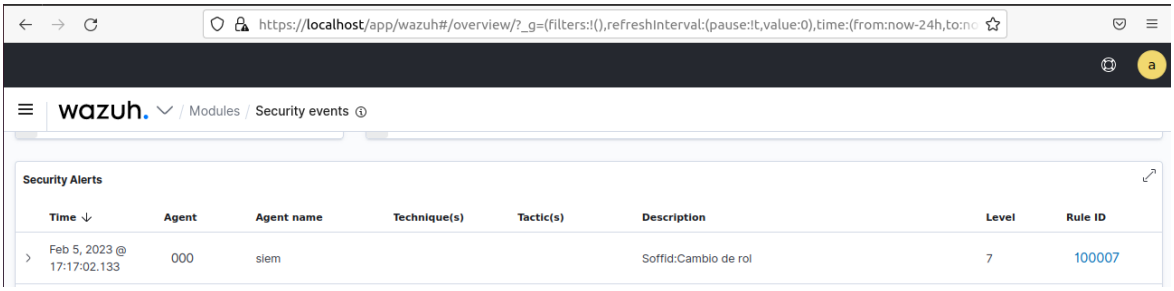

Figura 47: Alerta de cambio de rol

En conclusión, la simulación de ataques realizada en este capítulo, permite tener el insumo que en este caso son las alertas ya sea por intentos externos o por operaciones dentro de la solución Iam para la aplicación del modelo de monitoreo relacionadas a la identidad y el control de acceso que deben sortear diariamente los equipos de seguridad de TI o los centros de operaciones en seguridad SOC.

3.4.3 Validación y documentación de los resultados obtenidos

En esta etapa se ejecutaron las pruebas de validación del flujo de monitoreo propuesto, que cumpliendo con los requisitos de la fase 1, inicia en la actividad 2.1 de la fase de detección y análisis, va realizando el cuestionamiento en las opciones de decisión del modelo para tipificar la alerta y asignar un puntaje de riesgo acorde al acceso mayoritario a recursos que podría tener un posible atacante. Seguidamente, se va remitiendo en el flujo a las etapas de contención, erradicación, recuperación y actividades post-incidente. Para documentar el recorrido a través del flujo del monitoreo, la situación presentada o el resultado de la decisión en cada actividad se utiliza una planilla de validación de eventos para cada una de las alertas relacionadas a las amenazas seleccionadas para los ataques:

3.4.3.1 Alerta de ataque de relleno de credenciales

PLANILLA DE VALIDACIÓN DE EVENTOS ASOCIADOS A IDENTIDAD Y CONTROL DE ACCESO			
Fecha del monitoreo:	23 de enero de 2023	**Responsable del monitoreo:**	Eliana López
Id Alerta Siem:	d1Yv4IUBVhwlaCVQ5_cw		
Descripción alerta:	Soffid: usuario no habilitado		
Log Completo:	23-Ene-2023 19:16:27.990 INFO [http-nio-8080-exec-2] com.soffid.iam.tomcat.service.LoginServiceImpl.authenticate master\jperez login rejected. Unknown account		
Actividad del monitoreo		**Resultado**	
2.1 ¿La alerta corresponde a un IOA de la lista?		Si, se observan más de 20 intentos de inicio de sesión con un usuario desconocido (sospecha de ataque de relleno de credenciales)	
2.2 ¿La alerta involucra cuentas de administradores?		No, se consulta el Iam y la cuenta no existe	
2.5 ¿La alerta consiste en acceso a recursos?		No, la alerta indica corresponde a un usuario no habilitado	
2.7 ¿La alerta sólo involucra cuentas de usuario?		Si	
2.8 Registrar puntaje de riesgo 2		**Puntaje de riesgo: 2**	
2.10 Recolecte los registros asociados al evento		Sólo se encuentra un evento relacionado con la cuenta.	
2.11 Consulte configuraciones en el IAM realizadas a las cuentas involucradas		No hay configuraciones en el Iam porque la cuenta no existe	

2.12 La actividad está relacionada con nuevas configuraciones en el IAM?	No aplica porque la cuenta no existe
2.13 Desarrolle el análisis técnico	La alerta corresponde a un ataque de relleno de credenciales, se debe tomar los datos relevantes como la dirección ip Fuente, el usuario utilizado para las actividades de contención.
2.14 Hay nuevas alertas de compromiso?	No
3.1 Ejecute el Plan de Contención	Realice actividades de bloqueo de ip y bloqueo de inicio de sesión del usuario.
4.1 Ejecute el Plan de Erradicación	No aplica.
4.2 Ejecute el Plan de Recuperación	No aplica.
5.1 Realice las actividades Post-incidente	Proponga si es del caso acciones para mejorar el modelo.

3.4.3.2 Alerta de ataque de suplantación de identidad

PLANILLA DE VALIDACIÓN DE EVENTOS ASOCIADOS A IDENTIDAD Y CONTROL DE ACCESO			
Fecha del monitoreo:	23 de enero de 2023	**Responsable del monitoreo:**	Eliana López
Id Alerta Siem:	jlZM4IUBVhwlaCVQrPcc		
Descripción alerta:	Soffid: Inicio de sesión exitoso		
Log Completo:	23-Jan-2023 23:49:13.988 INFO [http-nio-8080-exec-3] com.soffid.iam.tomcat.service.LoginServiceImpl.authenticate master\admin login accepted		
Actividad del monitoreo		**Resultado**	
2.1 ¿La alerta corresponde a un IOA de la lista?		Si, se observa un inicio de sesión exitoso del usuario admin (sospecha de suplantación de identidad)	
2.2 ¿La alerta involucra cuentas de administradores?		Si, el usuario admin pertenece al grupo de Soffid_admin	
2.8 Registrar puntaje de riesgo 4		**Puntaje de riesgo: 4**	
2.10 Recolecte los registros asociados al evento		**Sólo se encuentra un evento relacionado con la cuenta.**	
2.11 Consulte configuraciones en el IAM realizadas a las cuentas involucradas		El usuario es administrador, no tiene alguna configuración que justifique la alerta.	

2.12 La actividad está relacionada con nuevas configuraciones en el IAM?	No.
2.13 Desarrolle el análisis técnico	El inicio de sesión no corresponde a un usuario autorizado, al parecer se encuentra comprometida la cuenta del usuario admin. Tome los datos relevantes del origen del ataque como la dirección ip para las acciones siguientes.
2.14 Hay nuevas alertas de compromiso?	No
3.1 Ejecute el Plan de Contención	Realice la copia de los archivos de log sobre las operaciones realizadas por este usuario, identifique datos relevantes de la conexión.
4.1 Ejecute el Plan de Erradicación	Realice cambio inmediato de clave del usuario admin y finalice sus sesiones abiertas.
4.2 Ejecute el Plan de Recuperación	Revise las operaciones realizadas por el usuario durante la conexión para devolver el sistema al estado previo a su irrupción.
5.1 Realice las actividades Post-incidente	Proponga si es del caso acciones para mejorar el modelo.

3.4.3.3 Alerta de ataque de creación de cuentas

PLANILLA DE VALIDACIÓN DE EVENTOS ASOCIADOS A IDENTIDAD Y CONTROL DE ACCESO			
Fecha del monitoreo:	23 de enero de 2023	**Responsable del monitoreo:**	Eliana López
Id Alerta Siem:	klZW4IUBVhwlaCVQXfe6		
Descripción alerta:	Soffid: Creacion de usuario		
Log Completo:	2023-01-23T20:33:46.177Z soffiditm SOFFID - SOFFID3519 - [admin] [127.0.0.1]Create user juan.fernandez		
Actividad del monitoreo		**Resultado**	
2.1 ¿La alerta corresponde a un IOA de la lista?		Si, se observa registro de creación exitosa de una cuenta nueva (sospecha de ataque de creación de cuentas)	
2.2 ¿La alerta involucra cuentas de administradores?		No.	
2.5 ¿La alerta consiste en acceso a recursos?		No, la alerta no indica acceso a algún recurso.	
2.7 ¿La alerta sólo involucra cuentas de usuario?		Si	

2.8 Registrar puntaje de riesgo 2	**Puntaje de riesgo: 2**
2.10 Recolecte los registros asociados al evento	Sólo se encuentra un evento relacionado con la cuenta.
2.11 Consulte configuraciones en el IAM realizadas a las cuentas involucradas	Se encuentra la cuenta configurada dentro del grupo de usuarios: World, con información de auditoria que indica que fue creada por el usuario “admin”.
2.12 La actividad está relacionada con nuevas configuraciones en el IAM?	Si, las fechas de creación y modificación son recientes.
2.13 Desarrolle el análisis técnico	La alerta corresponde a una creación de usuario precedido por una suplantación de identidad de la cuenta “admin”, se debe tomar los datos relevantes como la dirección ip fuente, y los datos de auditoria del usuario para actividades posteriores.
2.14 Hay nuevas alertas de compromiso?	No
3.1 Ejecute el Plan de Contención	Realice actividades de bloqueo de ip y bloqueo de inicio de sesión del usuario.
4.1 Ejecute el Plan de Erradicación	Elimine el usuario creado.
4.2 Ejecute el Plan de Recuperación	Realice cambio inmediato de clave del usuario admin y finalice sus sesiones abiertas.
5.1 Realice las actividades Post-incidente	Proponga si es del caso acciones para mejorar el modelo.

3.4.3.4 Alerta de ataque de acceso elevado o elevación de privilegios

PLANILLA DE VALIDACIÓN DE EVENTOS ASOCIADOS A IDENTIDAD Y CONTROL DE ACCESO			
Fecha del monitoreo:	23 de enero de 2023	**Responsable del monitoreo:**	Eliana López
Id Alerta Siem:	I1Za4IUBVhwlaCVQm_fk		
Descripción alerta:	Soffid: Cambio de rol		
Log Completo:	2023-01-23T20:38:26.184Z soffiditm SOFFID - SOFFID4097 - [admin] [127.0.0.1]Granted rol SOFFID_ADMIN@soffid to juan.fernandez (user juan.fernandez) (scope)		
Actividad del monitoreo		**Resultado**	
2.1 ¿La alerta corresponde a un IOA de la lista?		Si, se observa una concesión de otorgamiento de rol de administrador de Soffid a una cuenta que no	

	está autorizada para ello (sospecha de ataque de acceso elevado)
2.2 ¿La alerta involucra cuentas de administradores?	Si, la cuenta corresponde a una cuenta administrador con la ejecución del otorgamiento de rol
2.8 Registrar puntaje de riesgo 2	**Puntaje de riesgo: 4**
2.10 Recolecte los registros asociados al evento	Sólo se encuentra un evento relacionado con la cuenta.
2.11 Consulte configuraciones en el IAM realizadas a las cuentas involucradas	Se encuentra la cuenta configurada con el rol soffid@admin, con información de auditoria que indica que fue creada por el usuario “admin”.
2.12 La actividad está relacionada con nuevas configuraciones en el IAM?	Si, las fechas de creación y modificación son recientes.
2.13 Desarrolle el análisis técnico	La alerta corresponde a un cambio en los privilegios del usuario donde se le asigna el rol de Soffid admin por parte del usuario “admin”, se debe verificar la autorización de la operación para descartar de que se trate de una suplantación de la cuenta admin. Se debe tomar los datos relevantes como la dirección ip fuente, y los datos de auditoria del usuario para actividades posteriores.
2.14 Hay nuevas alertas de compromiso?	No
3.1 Ejecute el Plan de Contención	Realice actividades de bloqueo de ip y bloqueo de inicio de sesión del usuario.
4.1 Ejecute el Plan de Erradicación	Elimine el usuario creado.
4.2 Ejecute el Plan de Recuperación	Realice cambio inmediato de clave del usuario admin y finalice sus sesiones abiertas.
5.1 Realice las actividades Post-incidente	Proponga si es del caso acciones para mejorar el modelo.

De acuerdo con lo anterior, la asignación de los recursos para la atención de la alerta se hace más eficiente en tanto se ha incrementado la calidad de alertas realizando un filtro para recibir solo las alertas priorizadas según las amenazas que más comprometen los componentes de identidad y control de acceso permitiendo atender primero las más críticas en cuanto a privilegios.

Finalmente, el flujo propuesto permite orientar al operador de monitoreo para además de atender primero las alertas de mayor puntaje de riesgo, incorpore la integración de la solución IAM para aportar el contexto y tomar decisiones acordes a las configuraciones dinámicas que pueden tener las identidades.

4. Conclusiones y recomendaciones

4.1 Conclusiones

El panorama de las amenazas actual supone cada vez más un nivel superior de técnicas y tácticas con el fin de mejorar su propagación y persistencia. Para el caso de las amenazas vinculadas a la identidad y control de acceso se concluye que, comprometer el componente de identificación se convierte en la puerta de entrada para la violación de los demás, lo cual eleva la importancia de los controles sobre los mecanismos de autenticación como las contraseñas que, aunque siendo las más utilizadas también son la principal causa de muchos ataques cibernéticos.

Por otro lado, la gestión inteligente de las identidades y el control de acceso es un elemento determinante en la defensa contra los ciberataques. Es por ello que todas las empresas deben prepararse para implementar nuevas tecnologías como las propuestas en este proyecto que basadas en código abierto permite tener plataformas para la gestión de las cuentas y los permisos a los recursos, además de un correlacionador de eventos que recoge las alertas de posibles irregularidades y permite filtrar para aportar contexto en la toma de decisiones informadas en los equipos de atención de incidentes.

Ahora bien, cabe anotar que durante la simulación de los ataques informáticos para la generación de las alertas visualizables desde la solución Siem, se presentaron dificultades en tanto el diseño de la solución Iam Opensource sólo consideró el envío de eventos de log de la auditoria sobre operaciones de la herramienta, excluyendo registros importantes como los de acceso. Se hizo necesario entonces, implementar las configuraciones necesarias para sumar estos registros y ampliar la cobertura en cuanto a la protección de la interfaz de acceso a la consola que también resulta en un elemento vulnerable.

Adicionalmente, se puede señalar que este trabajo lleva a la práctica la aplicación de una de las guías más ampliamente utilizada del Instituto Nist, mediante la creación de un modelo de monitoreo que contempla todas las etapas del proceso de atención de incidentes. La validación del modelo demostró que tener un flujo de trabajo, agiliza los procesos de respuesta a incidentes al incrementar la eficiencia que genera priorizar las alertas y otorgar la secuencia de pasos a seguir para atender el compromiso de cuentas de mayor impacto.

4.2 Recomendaciones, lecciones aprendidas y trabajos futuros

Teniendo en cuenta que el modelo de monitoreo propuesto es de aplicación manual, recomiendo en un futuro revisar la posibilidad de automatizar algunas tareas con el fin de optimizar los tiempos en la atención de incidentes y de proponer actividades reactivas como bloqueos automáticos de cuenta, habilitación de formularios de captcha para evitar los bots.

Por el lado de las lecciones aprendidas de este proceso investigativo, es que la documentación de las soluciones Opensource a veces quedan limitadas al fabricante o a la comunidad que la soporta, por lo cual en ocasiones la información de algunas configuraciones es insuficiente o inexistente llevándonos a plantear la importancia de aportar a estos sitios o en su defecto crear blogs propios que puedan servir de apoyo a proyectos similares.

Por último, sugiero como trabajo futuro revisar la aplicación del monitoreo a otros tipos de alertas diferentes a las de identidad y acceso que permitan enriquecerse de integraciones de los Siem con otras soluciones.

5. Bibliografía

[1] Dimensional Research, «The State Of Identity: How Security Teams Are Addressing Risk A Survey Of Security Decision Makers,» 2019.

[2] C. Jones, «Expert Insights,» 20 01 2022. [En línea]. Available: https://expertinsights.com/insights/50-identity-and-access-security-stats-you-should-know/. [Último acceso: 15 04 2022].

[3] Ponemon Institute LLC, «Cybersecurity in the Remote Work Era: A Global Risk Report,» 2020.

[4] A. R. Almanza J., «XXI Encuesta Nacional de Seguridad Informática,» *Sistemas,* nº 159, pp. 20-64, 2021.

[5] C. H. Tarazona T, «Amenazas informáticas y Seguridad de la Información,» *Derecho Penal y Criminología,* vol. 28, nº 84, pp. 137-146, 2007.

[6] M. d. H. y. A. P. G. d. España, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información., Madrid: Ministerio de Hacienda y Administraciones Públicas Centro de Publicacione, 2012.

[7] OSA, «Threat Catalogue Overview,» 13 11 2008. [En línea]. Available: https://www.opensecurityarchitecture.org/cms/images/OSA_images/TC_Comparison.pdf. [Último acceso: 21 05 2022].

[8] OSA, «Open Security Architecture,» [En línea]. Available: https://www.opensecurityarchitecture.org/cms/library/threat_catalogue. [Último acceso: 15 05 2022].

[9] «Imperva,» [En línea]. Available: https://www.imperva.com/learn/application-security/cyber-attack/. [Último acceso: 20 07 2022].

[10] S. Salinas, «Exabeam,» 21 09 2021. [En línea]. Available: https://www.exabeam.com/information-security/what-are-ttps-and-how-understanding-them-can-help-prevent-the-next-incident/. [Último acceso: 20 07 2022].

[11] A. Koot, «IDPro Body of Knowledge 1(6),» 2020. [En línea]. Available: https://bok.idpro.org/article/id/42/. [Último acceso: 07 03 2022].

[12] I. O. f. Standardization, «ISO/IEC 24760-1:2019 - A framework for identity management,» 2019.

[13] A. Cameron y O. Grewe, «An Overview of the Digital Identity Lifecycle (v2),» 2022. [En línea]. Available: https://bok.idpro.org/article/id/31/.

[14] I. M. Institute, «https://identitymanagementinstitute.org/,» 02 2022. [En línea]. Available: https://identitymanagementinstitute.org/identity-and-access-management-report-2022/. [Último acceso: 05 03 2022].

[15] E. Kost, «Upguard,» 22 12 2021. [En línea]. Available: https://www.upguard.com/blog/what-are-indicators-of-attack. [Último acceso: 10 04 2022].

[16] Cyberark, «Privileged Access Management,» [En línea]. Available: https://www.cyberark.com/what-is/privileged-access-management/. [Último acceso: 29 10 2022].

[17] National Institute of Standards and Technology, Computer Security Incident Handling Guide, 2012.

[18] G. González Granadillo, S. González Zarzosa y R. Diaz, «Security Information and Event Management (SIEM): Analysis,Trends, and Usage in Critical Infraestuctures,» *Sensors,* p. 21, 2021.

[19] Solarwinds, [En línea]. Available: https://www.solarwinds.com/resources/it-glossary/syslog. [Último acceso: 29 07 2022].

[20] C. Onwubiko, «CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process,» *International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA),* pp. 1-8, 2018.

[21] K. Okereafor y O. I. Adelaiye, «Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era,» *International Journal of Recent Engineering Research and Development,* vol. 05, pp. 61-72, 2020.

[22] U. G. F. Frattini y C. Vincenzo, «Facing Cyber-Physical Security Threats by PSIM-SIEM Integration,» *15th European Dependable Computing Conference (EDCC),* pp. 83-88, 2019.

[23] L. Vítek, *Integrace IAM v podnikovém IS,* Praga, 2020.

[24] SailPoint, «SailPoint and Splunk An Integrated Approach to Identity Governance Monitoring and Auditing,» 2020.

[25] *Integrating IAM(Okta) with SIEM.* [Película]. LogRhythm, 2018.

[26] S. Basu, «Astra,» 19 07 2022. [En línea]. Available: https://www.getastra.com/blog/security-audit/security-testing-methodologies-explained/. [Último acceso: 27 07 2022].

[27] OSSIG, Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1, 2006.

[28] ISECOM, The Open Source Security Testin Methodology Manual, 2010.

[29] K. Roberts, «F5,» 21 04 2022. [En línea]. Available: https://community.f5.com/t5/technical-articles/bots-fraud-and-the-owasp-automated-threats-project-overview/ta-p/294520. [Último acceso: 30 07 2022].

[30] OWASP, «OWASP Automated Threat Handbook Web Applications version 1.2,» 15 02 2018. [En línea]. Available: https://owasp.org/www-project-automated-threats-to-web-applications/. [Último acceso: 30 07 2022].

[31] M. Chapple, Access Control and Identity Management Third Edition, Jones and Bartlett Learning , 2021.

[32] C. A. Tobón Betancu, Modelo de administración de identidad digital (IdM) sobre blockchain para la mitigación del riesgo por suplantación en sistemas e-banking, Medellín, 2020.

[33] FusionAuth, «Documentation Getting Started,» [En línea]. [Último acceso: 30 07 2022].

[34] Keycloak, «Server Administration Guide,» 27 07 2022. [En línea]. Available: https://www.keycloak.org/docs/latest/server_admin/. [Último acceso: 30 07 2022].

[35] Incibe, «Catálogo de empresas y soluciones de ciberseguridad,» [En línea]. Available: https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listado-empresas/soffid-iam. [Último acceso: 30 07 2022].

[36] Soffid, «Soluciones Sofidd,» [En línea]. Available: https://www.soffid.com/. [Último acceso: 30 07 2022].

[37] «IONOS,» 14 05 2019. [En línea]. Available: https://www.ionos.es/digitalguide/servidores/seguridad/saml/. [Último acceso: 18 07 2022].

[38] «Thingworx,» [En línea]. Available: http://support.ptc.com/help/thingworx_hc/thingworx_8_hc/es/index.html#page/ThingWorx/Help/Composer/Security/Provisioning/SCIM.html. [Último acceso: 18 07 2022].

[39] «Apache Metron,» [En línea]. Available: https://metron.apache.org. [Último acceso: 09 09 2022].

[40] «Mozilla Mozdef,» [En línea]. Available: https://github.com/mozilla/MozDef. [Último acceso: 09 09 2022].

[41] J. Faircloth, Penetration Tester's Open Source Toolkit (Fourth Edition), Syngress, 2017, pp. 179-214.

[42] N. I. o. S. a. Technology, «NIST,» 09 2012. [En línea]. Available: https://doi.org/10.6028/NIST.SP.800-30r1.

[43] INCIBE, «INCIBE,» 18 05 2021. [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf.

[44] M. J. Haber y D. Rolls, Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution, Apress, 2020.

[45] G. Dobbs, «IAM Reference Architecture,» 2021. [En línea]. Available: https://bok.idpro.org/article/id/76/. [Último acceso: 07 03 2022].