Modelo para la gestión de incidentes de seguridad en redes industriales SCADA a través del algoritmo de predicción Filtro Kalman

Stephen Quiroz Tascon

Julián Zapata Jiménez

Instituto Tecnológico Metropolitano

Facultad de ingeniería

Medellín, Colombia

2019

Modelo para la gestión de incidentes de seguridad en redes industriales SCADA a través del algoritmo de predicción Filtro Kalman

Stephen Quiroz Tascon

Julián Zapata Jiménez

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

Magíster en Seguridad Informática

Director (a):

Magíster Héctor Fernando Vargas Montoya

Línea de Investigación:

Línea de investigación en ciencias computacionales

Grupo de Investigación:

Automática, electrónica y Ciencias Computacionales

Instituto Tecnológico Metropolitano

Facultad de ingenierías

Medellín, Colombia

2019

(Dedicatoria o lema)

Queremos agradecerles a nuestras familias por la comprensión y el apoyo incondicional brindado en el desarrollo del proyecto.

Somos arquitectos de nuestro propio destino.

Albert Einstein

Agradecimientos

Queremos agradecerle a nuestro director de tesis Héctor Fernando Vargas el cual desde su conocimiento nos orientó pacientemente en el progreso del proyecto y la culminación de este.

Resumen

Este proyecto consiste en el desarrollo de un modelo de gestión de incidentes de seguridad en los sistemas de Supervisión, Control y Adquisición de Datos (SCADA) basado en predicción de eventos, es decir, a través de la recolección de información de posibles ataques informáticos, se hace una predicción con el modelo matemático Filtro Kalman (el cual realiza predicciones de variables lineales por medio de mínimos cuadrados recursivos), una vez se genera la predicción del posible evento de seguridad, se activa el proceso de manejo de incidentes; el resultado final, es un modelo de gestión de incidentes de seguridad basado en la detección temprana entregada por el filtro Kalman, caracterizado por niveles de impacto, los cuales definirán el procedimiento adecuado al nivel de criticidad de la predicción, permitiendo así lograr una integración y despliegue de las mejores acciones dependiendo del tipo de alerta que se genere y en este sentido, lograr una posible reducción en los niveles de exposición al riesgo y reducción de posibles impactos.

Palabras clave: Análisis de datos, Software de código abierto, Filtro Kalman, SCADA, Python, ecuación.

Abstract

This project consists of the development of a security incident management model in the Supervision, Control and Data Acquisition (SCADA) systems based on event prediction, that is, through the collection of information on possible computer attacks makes a prediction with the Kalman filter mathematical model (which makes predictions of linear variables by means of recursive least squares), once the prediction of possible safety event is generated, the incident management process is activated; The final result is a security incident management model based on the early detection delivered by the Kalman filter, characterized by levels of impact, which will define the procedure appropriate to the criticality level of the prediction, thus allowing an integration and deployment of the best actions depending on the type of alert that is generated, thereby achieving a possible reduction in the levels of exposure to risks and reduction of possible impacts.

Keywords: Equation, Data analysis, Open source software, Kalman Filter, SCADA, Python

Contenido

Pág.

Resumen ..... **IX**

Lista de figuras ..... **XIII**

Lista de tablas ..... **XV**

Lista de abreviaturas ..... **XVI**

Introducción **1**

1. Marco teórico y estado del arte **5**
1.1. Marco Teórico 5
1.1.1. Los sistemas industriales 5
1.1.2. Sistemas de detección de intrusos 6
1.1.3. Soluciones tecnológicas de IDS. 7
1.1.4. Filtro Kalman 11
1.2. Estado del arte 13

2. Metodología **17**
2.1. Identificación de los IDS 17
2.2. Construcción del filtro Kalman 19
2.3. Procedimiento para el manejo de incidentes de seguridad 20
2.4. Evaluación del sistema 21

3. Resultados **23**
3.1. Identificación de los IDS en los sistemas SCADA 23
3.1.1. Comparación de los IDS 23
3.1.2. Estructura e implementación de Sistema SCADA 24
3.1.3. Implementación SCADA Proyecto CONPOT 25
3.1.4. Instalación CONPOT 26
3.1.5. Integración del IDS al sistema SCADA 28
3.2. Construcción del filtro Kalman 35
3.2.1. Instalación y configuración de OpenCV 35
3.2.2. Caracterización de los ataques al sistema SCADA 37
3.2.3. Creación y configuración de reglas del IDS SNORT 38
3.2.4. Desarrollo de la herramienta de predicción 39
3.3. Modelo para el manejo de incidentes de seguridad en redes industriales 45
3.3.1. Comparación de los diferentes modelos de gestión de incidentes 45
3.3.2. Relacionar la estructura de procesos y operación de una red industrial SCADA 58
3.3.3. Creación del nuevo modelo para el manejo de incidentes de seguridad 63
3.4. Evaluación del modelo de incidentes 81
3.4.1. Generación de diferentes tipos de eventos simulados de intrusión al sistema SCADA 82

3.4.2. Validación de las salidas del Filtro Kalman respecto a criticidad e impacto..... 86

4. Conclusiones 88

5. Recomendaciones, lecciones aprendidas y trabajo futuro. 90

6. Bibliografía.....95

Lista de figuras

Pág.

Figura 1-1: Topología de Red. Fuente autores. 7
Figura 1-2: Diagrama de aplicación del filtro Kalman. Fuente autores 13
Figura 2-1: Metodología para el cumplimiento de los objetivos. Fuente autores. 17
Figura 2-2: Arquitectura propuesta del proyecto. Fuente autores. 21
Figura 3-1: Estructura Interna del Sistema CONPOT. Fuente autores. 24
Figura 3-2: Ejecución Sistema CONPOT. Fuente autores. 27
Figura 3-3: Deshabilitar LRO y GRO. Fuente autores. 29
Figura 3-4: Versión de SNORT. Fuente autores. 30
Figura 3-5: Validación configuración de SNORT. Fuente autores. 32
Figura 3-6: Inicio automático SNORT NIDS Daemon. Fuente autores 34
Figura 3-7: Inicio automático Barnyard2 Daemon. Fuente autores. 34
Figura 3-8: Instalación de dependencias OpenCV. Fuente autores. 35
Figura 3-9: Instalación de python3. Fuente autores. 36
Figura 3-10: Clonación del proyecto OpenCV desde Github. Fuente autores. 36
Figura 3-11: Validación instalación OpenCV + Python. Fuente autores 37
Figura 3-12: Lectura de datos al PLC Siemens 2700 con protocolo modbus. Fuente autores. 37
Figura 3-13: Sobrescribir de datos al PLC Siemens 2700 con protocolo modbus. Fuente autores. 38
Figura 3-14: Librerías necesarias para filtro Kalman en Python. Fuente autores. 40
Figura 3-15: Creación Store Procedure TablaPivote. Fuente autores. 41
Figura 3-16: Conexión a la base de datos SNORT. Fuente autores. 41
Figura 3-17: Datos generados por los ataques simulados. Fuente autores. 42
Figura 3-18: Datos de entrada Filtro Kalman. Fuente autores. 42
Figura 3-19: Filtro Kalman. Fuente autores. 43
Figura 3-20: Datos de entrada Filtro Kalman. Fuente autores. 43
Figura 3-21: Datos de entrada Filtro Kalman. Fuente autores. 44
Figura 3-22: Características principales de NIST SP800-61 e ISO 27035 [5], [42] 46
Figura 3-23: Etapa 1 Preparación NIST SP800-61[5], [42] 47

Figura 3-24: Etapa 2 Detección y análisis NIST y detección y reporte; evaluación y decisión de ISO 27035 [5], [42] 49
Figura 3-25: Etapa 3 Contención, erradicación y recuperación de NIST SP800-61 y la fase de respuestas de ISO 27035 [5], [42] 53
Figura 3-26: Etapa 4 post incidente de NIST SP800-61 y lecciones aprendidas de ISO 27035 [5], [42] 56
Figura 3-27: Flujo de proceso organizacional. Fuente autores. 60
Figura 3-28: Método OODA [44] 67
Figura 3-29: Procedimientos clave para la gestión de incidentes de seguridad. Fuente autores. 70
Figura 3-30: Flujo de detección, análisis y reporte. Fuente autores. 71
Figura 3-31: Ataque 1. Sobrescribir datos al PLC Siemens 2700 con protocolo modbus. Fuente autores. 82
Figura 3-32: Ataque 2. Lectura de datos al PLC Siemens 2700 con protocolo modbus. Fuente autores. 82
Figura 3-33: Comportamiento del sistema SCADA Laboratorio CONPOT. Fuente autores. 83
Figura 3-34: Dashboard de visualización. Fuente autores. 85

Lista de tablas

Pág.

Tabla 2-1 Ponderación de las características para la selección del IDS. Fuente autores..... 18

Tabla 3-1 Comparación de los principales IDS. Fuente autores..... 23

Tabla 3-2 Configuración de hardware Ubuntu Server 16.04 LTS..... 26

Tabla 3-3 Configuración de hardware Ubuntu Server 18.04 LTS..... 28

Tabla 3-4 Software de apoyo del sistema SCADA..... 28

Tabla 3-5 Fases del modelo para la gestión de incidentes..... 64

Tabla 3-6 Principales contactos a informar la detección de un posible incidente..... 66

Tabla 3-7 Incidentes por categoría..... 73

Tabla 3-8 Niveles de impacto..... 74

Tabla 3-9 Nivel de prioridad..... 76

Tabla 3-10 Roles y contactos que se deben informar..... 78

Lista de abreviaturas

Abreviatura	Término
API	Interfaz de programación de aplicaciones
BD	Base de datos
BTLE	Bluetooth de baja energía
CISO	Director de seguridad de la información
DNS	Sistema de nombres de dominio
DOS	Ataque de denegación de servicio
FMA	Modelo estadístico Promedio Móvil Finito
GRO	Descarga de recepción genérica
HIDS	Sistemas de detección de intrusos en el host
HMI	Interfaz humano máquina
HTTP	Protocolo de transferencia de hipertexto
ICMP	Protocolo de control de mensajes de Internet
ICS	Sistema de control industrial
IDS	Sistema de detección de intrusos
IP	Protocolo de internet
IPS	Sistema de prevención de intrusos
ISO 27035	Guía técnica colombiana de manejo de incidentes de seguridad información
LOG	Historial de eventos
LRO	Descarga de recepción grande
LST	Soporte a largo plazo
MD5	Algoritmo de Resumen del Mensaje 5
MI	Mensaje instantáneo
MITM	Ataque de hombre en el medio
MODBUS	Protocolo de comunicación utilizado para PLC, RTU y SCADA
NAT	Traducción de direcciones de red
NIDS	Sistemas de detección de intrusos en la red
NIST SP-800-61	Guía NIST de manejo de incidentes de seguridad informática
NNARX	Red neuronal
OISF	Open Information Security Foundation
OODA	Modelo de observación, orientación, decisión y acción
OPENCV	Algoritmo de código abierto de visión artificial
PLC	Controlador Lógico Programable
PMU	Puesto de mando unificado
RTU	Unidades Remotas
SCADA	Sistema supervisión, Control y Adquisición de Datos
SHA	Algoritmo de Hash Seguro

SNMP	Protocolo simple de administración de red
SSL	Capa de sockets seguros
TCP	Protocolo de Control de Transmisión
TI	Tecnología de la información
TIC	Tecnología de la información y las comunicaciones
VANET	Red ad-hoc vehicular
WI-FI	Conexión inalámbrica

Introducción

Las tecnologías de información y comunicaciones - TIC permiten a las organizaciones establecer procesos más efectivos, lo que implica que los datos e información van en circulación por las redes y los sistemas de almacenamiento, cualquier problema sobre esto, genera un riesgo para los procesos. Esta situación de riesgo puede aumentar en la medida que las empresas crecen y se vuelven complejas, para lo cual, ante un evento de seguridad, es necesario que se activen los procesos y protocolos para la atención de dicho incidente. Los procesos de atención a eventos de seguridad pueden ser claves en aquellas compañías cuyo objeto de negocio depende de los sistemas industriales, toda vez que éstos, poseen una función específica (muy electrónica) que cada día se va acercando a las redes de computadores y de telecomunicaciones para su gestión.

El presente proyecto se ha desarrollado en el cumplimiento de los siguientes objetivos:

Objetivo general

Proponer un modelo para el manejo de incidentes de seguridad una vez detectado de manera predictiva con el filtro Kalman, posibles intrusiones en las redes industriales en el sector eléctrico, con el fin de evitar posibles riesgos que afecten la disponibilidad, integridad y/o confidencialidad de la información.

Objetivos específicos

1. Identificar los diferentes sistemas de detección de intrusos que puedan integrarse a las redes industriales – SCADA.
2. Desarrollar el filtro Kalman para la detección de intrusos, así lograr predecir posibles eventos de seguridad.
3. Establecer la estrategia para de identificación, manejo y respuesta de los incidentes de seguridad.
4. Evaluar el modelo para el manejo de incidentes de seguridad una vez realizada la predicción de posibles ataques en el sistema de detección de intrusos en un ambiente controlado.

Actualmente, existe una tendencia que todos los dispositivos electrónicos poseen conexión a internet, lo que se denomina Internet de las cosas y hace referencia a una red de dispositivos físicos que poseen tecnología de capas que le ayudan a comunicarse e interactuar con otros dispositivos de similares características o personas, todo sobre una red de computadores y/o Internet. Ejemplos de estos dispositivos son las redes VANET (o vehiculares), sistemas de iluminación y refrigeración, sistemas de seguridad en empresas o de casas, televisores y teléfonos inteligentes. Quizás sean los equipos más comunes dentro de una lista mucho más extensa y en continua expansión en el ambiente tecnológico [1].

Adicionalmente, se debe entender que los datos y la información en las compañías son más que datos de ventas en valor, volúmenes en kilos, unidades vendidas, estadísticas que hacen referencia al comportamiento del mercado o hábitos de compra de sus consumidores, sino también la que se gesta al interior del negocio, como los datos que se crean o generan a partir de su funcionamiento, por ejemplo, la información de la maquinaria industrial que es de suma importancia para la compañía, porque a partir de ella puede conocer el comportamiento de cada elemento de su estructura en tiempo real. Estos datos son generados por PLC's (Controlador Lógico Programable) y administrados de forma gráfica por los HMI (Interfaz Hombre Máquina) y sistemas como SCADA.

Los sistemas SCADA (conocidos como sistemas de Supervisión, Control y Adquisición de Datos), comprenden todas las soluciones que recolectan medidas y datos operativos de equipos de control locales y remotos. Los datos recolectados se procesan con el fin de determinar si éstos hacen parte de los niveles de tolerancia y si es necesario, ejecutar medidas preventivas y/o correctivas para velar por la estabilidad y el control. La arquitectura básica y genérica para un sistema SCADA está compuesta por los PLC, uno o varios servidores, las consolas desde donde se visualiza y opera el sistema y un servidor con datos históricos de bases de datos, que almacena toda la información [2].

Los sistemas de control industrial son muy importantes para la industria de ciertos sectores productivos como eléctrico, aguas, petróleo, manufactura, entre otros, y su funcionamiento depende de unos pocos dispositivos comunicados entre sí. Si en algún momento ocurriera un fallo, se puede generar graves daños productivos, económicos, humanos y/o ambientales dependiendo

del sector en que se encuentre implementado dicho sistema. Para ayudar con la seguridad y su correcto funcionamiento, existen Sistemas de Detección de Intrusiones (IDS), que a través de análisis de tráfico en las redes, validan y generan alertas para que sean revisadas por el personal de seguridad y les ayude a identificar intrusiones en tiempo real, por lo que se convierte en una herramienta importante para los sistemas SCADA [1].

Considerando el informe de encuesta latinoamericana de seguridad de la información, donde participan diferentes sectores de varios países de Latinoamérica, los sectores industriales como alimentos, gobierno, retail, energía e hidrocarburos presentan riesgos asociados a la operación de un 33,7%, lo que indica alta probabilidad de exposición a diferentes ataques o amenazas de los que puedan ser víctimas y afectar sus operaciones. Adicionalmente, el 2,84% del sector energía e hidrocarburos realiza entre uno y cuatro análisis de riesgos al año, lo que incrementa las posibilidades de verse afectados por un ataque en sus redes [3].

La delicada situación de ciberseguridad por la que atraviesan actualmente los sistemas SCADA, permiten que códigos maliciosos como Spoofing, ataque de hombre en el medio (MITM) y los ataques de integridad sean el principal problema de seguridad a los que se deben enfrentar estos sistemas [4]. Esto hace que una falla de seguridad en algún dispositivo de infraestructura crítica de cualquier tipo de sector (eléctrico, agua, petróleo, manufactura, entre otros.) pueda producir graves daños en la información de la empresa. Este proyecto pretende desarrollar una fusión integral entre un sistema SCADA virtualizado o simulado, un IDS con el filtro Kalman y un modelo teórico de gestión de incidentes, con el objetivo de ayudar a los sistemas de seguridad a mejorar la detección de intrusiones y los comportamientos anómalos en las redes industriales del sector eléctrico principalmente.

Por su naturaleza, el filtro Kalman se encarga de realizar predicciones de variables lineales, donde el núcleo del filtro es la proyección por medio de mínimos cuadrados recursivos. Por lo tanto, es un algoritmo que estima sistemas dinámicos, los cuales son representados en la forma de estado-espacio, en la que el sistema se describe mediante variables o estados. La información relativa del sistema es contenido en el estado y ésta contiene el tiempo, así mismo, debe permitir la inferencia basado en el comportamiento pasado del sistema, con el fin de proyectar el futuro. De acuerdo

con lo anterior, se propone un modelo de gestión de incidentes basado en las mejores prácticas como NIST SP-800-61 e ISO 27035 con un componente innovador que consiste en darle valor a la fase de detección con una predicción posible del evento en curso y así poder iniciar acciones de análisis basados en la predicción del algoritmo [5], permitiendo llegar más rápidamente a las fases de contención, erradicación y recuperación de un incidente de seguridad, lo que se traduce en reducción del impacto que pudo generar el evento si no se hubiera atendido tempranamente.

1. Marco teórico y estado del arte

1.1. Marco Teórico

1.1.1. Los sistemas industriales

Los Programmable Logic Controller-PLC son de gran cobertura en las empresas y sectores industriales, permiten a través de su memoria programable almacenar diferentes instrucciones y así, implementa funciones para el control de máquinas y procesos. Son dispositivos digitales diseñados con microprocesadores[6]. Los PLC proporcionan confiabilidad en su operación y están diseñados para el control industrial y producción de los sectores energéticos, agua, producción industrial en general, entre otros

Siendo necesario el control de los PLC, Supervisory Control And Data Acquisition (SCADA) es una aplicación software de control de producción, que interactúa con los dispositivos externos de campo y ejerce control en los procesos automáticamente desde la pantalla de cualquier computador. También entrega información del proceso a los usuarios dependiendo del rol, por ejemplo, operadores, supervisores de calidad, supervisión en general, mantenimiento, entre otros. [7]. Hace algunos años, los sistemas SCADA eran más seguros contra las intrusiones y ataques que sufrían las redes de la organización, esto no quiere decir que este sistema fuese mucho más resistente, sino que estaban aislados y eran inaccesibles desde las redes administrativas o internet. Actualmente, aún se manejan desde un segmento de red separado e implícitamente seguro, aun cuando el mismo computador donde se administre el sistema se encuentre instalado un cliente de servicio de correo electrónico y con acceso a internet.

Como cualquier red de datos hoy día, las redes industriales no son totalmente seguras o inmunes a software capaz de realizar acciones malintencionadas en los sistemas a través de accesos no autorizados a estos. Algunas categorías de malware o software malicioso son el ransomware, spyware, troyanos y gusanos [8]. Están en la capacidad de extenderse desde un computador o equipo a otras máquinas en una red o por internet, sustraer información y claves, eliminar archivos e incluso borrar toda la información del disco duro.

Los sistemas industriales no están exentos de padecer alguna de las acciones de un malware, puede considerarse como un incidente de seguridad una violación o amenaza inminente de violación de las políticas, uso aceptable o prácticas de seguridad de la información, el cual puede producir afectación de disponibilidad, integridad y confidencialidad de la información dependiendo de su nivel de compromiso [8].

1.1.2. Sistemas de detección de intrusos

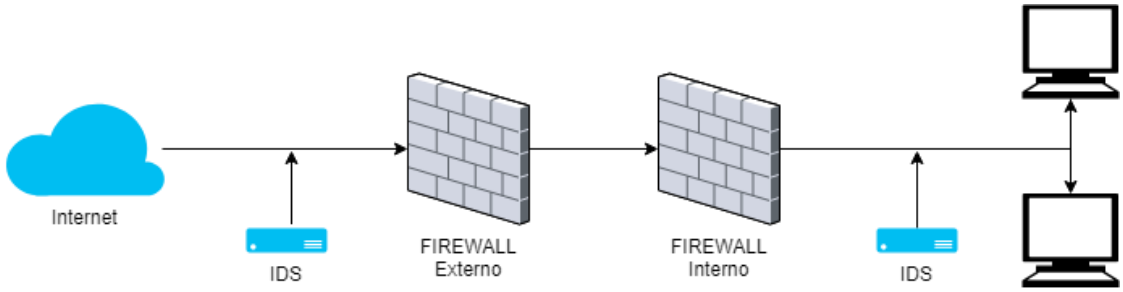
Para brindar ayuda en estos incidentes de seguridad, existen los sistemas de detección de intrusos. Un IDS es un dispositivo activo que analiza la actividad de las redes, sistemas y servicios informáticos, por accesos no autorizados o actividades maliciosas [9]. También ayuda a los sistemas a protegerse contra ataques cibernéticos y cualquier comportamiento anómalo que se encuentre en la red. Adicionalmente, puede monitorear la actividad, validar las configuraciones de los servicios informáticos y eventualmente encontrar vulnerabilidades. Los IDS detectan las anomalías dependiendo de la configuración y el ambiente tecnológico en que se implemente, sin embargo, su principal objetivo es identificar ataques de forma inmediata antes de que se materialice un daño en el sistema. Según los métodos de detección que se elijan, existen numerosos beneficios directos e indirectos de usar e implementar un IDS en cualquier organización.

Los sistemas de detección de intrusos (IDS) son un sistema que discretamente va monitoreando el tráfico en la red para detectar todas las actividades que se van realizando. Una característica principal en los IDS es supervisar el tráfico e informar sus resultados a un administrador, pero no toma medidas automáticamente para evitar que una vulnerabilidad sea explotada. Actualmente existen dos tipos de configuraciones para los IDS, los cuales son: los sistemas de detección de intrusos en la red (NIDS) que se encarga de la seguridad en la red y los sistemas de detección de intrusos en el host (HIDS) que actúa de forma local.

En el caso de los NIDS es necesario la instalación de un dispositivo (hardware o virtualización), el cual sirve para verificar cada uno de los paquetes de datos que van viajando en la red y está en la capacidad de detectar alguna actividad maliciosa. Los NIDS se pueden configurar en modo promiscuo, esto le ayuda a ser invisible en la red. Desde la topología de red, estos NIDS se pueden

encontrar en cualquier lugar, como dispositivos perimetrales que ayudan a analizar si se están realizando ataques internos o externos, como se muestra en la Figura 1-1

Figura 1-1: Topología de Red. Fuente autores.



El HIDS es un software que se encuentra instalado en un computador y puede operar en diferentes sistemas operativos. Este software analiza información de registro almacenada localmente y también es capaz de realizar capturas de red que ingresan y salen del dispositivo para verificar posibles señales de intrusión, como ataques DoS, Backdoors, Troyanos, entre otros.

1.1.3. Soluciones tecnológicas de IDS.

A continuación, se describen algunas soluciones tecnológicas que tienen las funcionalidades de sistemas de detección de intrusos – IDS.

SNORT

Es un sistema de detección de intrusiones de red de código abierto que se puede instalar en diferentes sistemas operativos como son Linux y Windows. Su funcionamiento inicia con la monitorización del tráfico, luego lo verifica contra un conjunto de reglas que se configuran previamente. Existen 3 diferentes tipos de reglas, como, reglas de la comunidad, reglas registradas y reglas comerciales para SNORT, todas disponibles en su página web [10]; también es posible personalizar las reglas para mejorar su capacidad de detección y minimizar los falsos positivos. SNORT puede generar alertas cuando se ve tráfico específico en la red; también puede detectar

escaneos de puertos, falsificación de datos ARP y datos confidenciales, como números de tarjetas de crédito e información sensible que se comparte en la red[11].

Suricata

Sistema de detección de amenazas en la red, opensourse, rápido y robusto. Adicionalmente es capaz de realizar tareas como detección (IDS) y contención/prevención (IPS) de intrusos. Su funcionamiento se basa en un lenguaje de firmas y un conjunto de reglas y soporta scripts Lua para la configuración de amenazas complejas. También cuenta con una comunidad activa. Esta herramienta está respalda por Open Information Security Foundation (OISF), una fundación sin ánimo de lucro que está comprometida a garantizar el desarrollo y el éxito sostenido de Suricata como un proyecto de código abierto[12].

Bro o Bro-IDS

Analizador pasivo de tráfico que inspecciona tráfico de red en profundidad y no sólo en relación con las conexiones cableadas, sino también a nivel de aplicación como sesiones HTTP, solicitudes y respuestas DNS, sesiones SMTP, certificados SSL, entre otras. Bro, brinda la posibilidad de definir la forma en que se puedan extraer los datos generados para facilitar la integración con otras herramientas, también permite realizar tareas personalizadas por medio de Python, aunque en su defecto viene preconfigurado con funciones o características estándar[13].

Kismet

Es un sistema de detección de intrusos y detector de redes inalámbricas que funciona con las tarjetas Wi-Fi (IEEE802.11), así como con dispositivos Bluetooth y BTLE (Bluetooth Low Energy), así mismo con receptores de radio para detectar sensores inalámbricos, termómetros y conmutadores. Del mismo modo que SNORT, este IDS se convirtió en un estándar para análisis de intrusiones en red y se ha ido convirtiendo en una referencia para IDS wireless. Un IDS Wireless tiene menos que ver con la carga de paquetes en sí, y más con los eventos que suceden en la red [14].

OSSEC

Es un sistema de detección de intrusos en Host (HIDS) open source y se puede utilizar en diferentes sistemas operativos, como Linux, Windows, OpenBSD, MacOS, entre otros. Posee un potente motor de correlación y análisis, la integridad de los archivos, supervisión de los registros de Windows, centralización de las políticas, detección de rootkits, alertas y respuesta en tiempo real [15].

Tripwire Opensource

Esta herramienta cuenta con dos versiones (open source y empresarial de pago). Este sistema fue uno de los pioneros para la tecnología HIDS y muchas de sus características se han convertido en estándares para la industria. La versión open source tiene menores opciones que la versión de pago, pero es capaz de competir con otras herramientas similares. Una de las principales falencias de esta versión es la falta de control, informes centralizados y características de automatización avanzadas [16].

Se debe considerar que esta no genera alertas en tiempo real y tampoco detecta intrusiones previamente existentes en el sistema para la función HIDS. Toda la información generada debe ser almacenada para su análisis posterior.

Samhain

Es un sistema de detección de intrusos (HIDS) basado en host que proporciona verificación de integridad de archivos y monitoreo / análisis de archivos de registro, así como detección de rootkits, monitoreo de puertos, detección de ejecutables de SUID fraudulentos y procesos ocultos. También está diseñado para monitorear múltiples hosts con sistemas operativos diferentes, brindando registro y mantenimiento centralizados, aunque se puede usar como una aplicación independiente y local. Una de sus mayores ventajas es que es multiplataforma de código abierto para sistemas POSIX (Unix, Linux, Cygwin / Windows) [17].

Fortinet

Configurado como Sniffer, FortiGate es capaz de detectar ataques e informar a los administradores, pero no realiza ninguna acción frente a ellas. Tampoco procesa el tráfico de red directamente, sino que se encuentra conectado a un puerto espejo o duplicado para no afectarlo. Con el modo Sniffer

activado, este rastrea y no procesa el tráfico en el puerto original, por tal motivo el escaneo no afecta el rendimiento y el tráfico de la red no se ve afectado si el IDS se desconecta. Esta herramienta es de pago de uso empresarial [18].

Radware

DefensePro es un dispositivo de prevención de intrusos en la red en tiempo real que evita que la infraestructura se deshabilite por ataques cibernéticos. También proporciona una protección contra la explotación de vulnerabilidades, el malware, el robo y entre otros ataques. Dicho dispositivo está basado en una tecnología de detección de firmas estáticas de estado y utiliza actualizaciones periódicas y actualizaciones de emergencia para proteger la red [19].

Palo Alto

Palo Alto cuenta con un servicio de prevención de amenazas que dispone de una inspección de tráfico que permite identificar y evitar amenazas conocidas independientemente del puerto, protocolo o cifrado SSL por medio de coincidencia de patrones con estado. Depende de una actualización diaria de una base de firmas individuales y su operación se centra en prevenir la entrega e instalación de malware. Las firmas de carga útil le permiten identificar futuras variaciones de malware por medio de patrones en el cuerpo de los archivos, lo que permite identificar malware polimórfico [20].

En complemento a un IDS, puede contemplarse un sistema de prevención de intrusos. Un IPS es un hardware o software que posee la capacidad de controlar diferentes accesos al sistema o redes de computadores, con ello, bloquear y alertar de posibles intrusiones. La tecnología de prevención de intrusos a diferencia de los IDS, permite el bloqueo en tiempo real de ataques cibernéticos [21].

Human Machine Interface o HMI, es un dispositivo o sistema que permite la comunicación por medio de una interfaz entre una persona y un dispositivo (máquina). Estos sistemas poseen paneles compuestos por comandos e indicadores que se interconectaban con la máquina o proceso [22]. Actualmente, dado que los dispositivos o máquinas en general están implementadas con elementos como controladores y dispositivos electrónicos que dan disponibilidad de comunicación

a través de puertas lógicas, así, es posible tener con sistemas robustos y eficaces. Además, permiten una conexión más sencilla y ágil con el proceso o la maquinaria. Los procesos se interactúan a través de las señales, se conducen al HMI a través de dispositivos tales como PLC, tarjetas de entrada y salida, RTU (Unidades Remotas de I/O), entre otros. Para el almacenamiento de la configuración, los HMI utilizan un formato propio que lo hace en tiempo real, pero en la actualidad, dicha información va almacenada en motores de bases de datos relacionales.

1.1.4. Filtro Kalman

Rudolf E. Kalman desarrolló un método matemático en 1960 y describe una solución basada en una función recursiva para el problema del filtrado lineal de datos discretos [23]. Dicho filtro hace parte de un contexto de modelos estado-espacio, donde el núcleo es la proyección o estimación que se hace con mínimos cuadrados recursivos. Dicha representación del sistema se define mediante un conjunto de variables que son denominadas estados. Cada estado tiene la información del sistema en cierto punto en el tiempo y esta información debe permitir la deducción de los diferentes comportamientos basado en el pasado del sistema (así predice su comportamiento futuro). El filtro Kalman tiene numerosas aplicaciones en tecnología, como guía, navegación y control de vehículos, especialmente en naves espaciales.

El filtro Kalman se compone de 2 fases. En la primera fase, por lo general llamada la fase de predicción, se genera un pronóstico del estado futuro en el tiempo, tomando en cuenta toda la información disponible en ese momento. En la segunda fase, denominada la fase de corrección, se calcula un pronóstico mejorado del estado, de tal manera que el error es minimizado estadísticamente.

En la fase de Predicción, se ha considerado los datos generados por los ataques simulados que se explicaron anteriormente, estos eventos comprometen la seguridad del sistema SCADA desde diferentes vectores de ataque al que se encuentra expuesto dicho sistema. Dicho esto, los datos son llamados desde la base de datos y almacenados en el vector de estados, representado en la ecuación (ver ecuación (1.1))

$$\boldsymbol{X_k^- = Fx_{k-1} + Bu_{k-1} + W_k} \tag{1.1}$$

Luego se determina la matriz de covarianza de error, la cual representa el aprendizaje para la corrección de errores (ver ecuación (1.2)).

$$\boldsymbol{P_k^- = FP_{k-1} + Q_{k-1}} \quad (1.2)$$

En la fase de corrección, el tiempo de actualización en la estimación del estado para la predicción se corrige en la matriz de covarianza del error y la diferencia del filtro Kalman se calcula para minimizar el error en la estimación del nuevo estado (ver ecuación (1.3)).

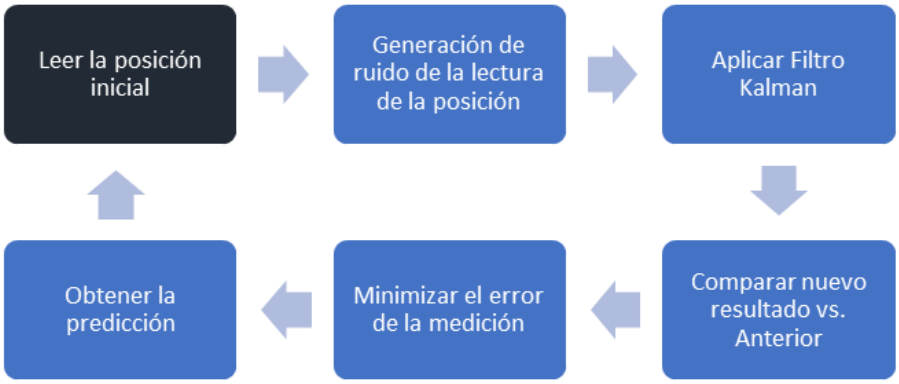
$$\boldsymbol{K_k = P_k^- H_k^T (H_k\, P_k^- H_k^T + R_k)^{-1}} \quad (1.3)$$

Para aplicar el Filtro Kalman se debe inicializar el vector de estados X_k , hay que tener en cuenta que la matriz de transición F relaciona el estado del sistema en el instante k para el instante $k+1$, además se debe generar ruido sobre la imagen (vector W_k) de forma que se pueda garantizar aprendizaje en cada iteración del sistema y se llegue a un mínimo error en la predicción. El vector es generado W_k con valores aleatorios. Así mismo, debe existir un valor observado Z_k como medida para comparar el filtro de predicción en cada instante de tiempo t . El valor de Z_k es creado con medidas directas de X_k, la variable de estado se complementa con la medición del ruido añadido al sistema (ver ecuación (1.4)).

$$\boldsymbol{Z_k = H_k X_k + V_k} \quad (1.4)$$

En conclusión, en la figura 1-2 se muestra los pasos de cómo funciona el filtro Kalman para realizar una predicción de forma más simple y sencilla en cada iteración.

Figura 1-2: Diagrama de aplicación del filtro Kalman. Fuente autores



1.2. Estado del arte

En el trabajo de [24] se argumenta que la implementación de Modbus/TCP en redes SCADA, es muy importante para la comunicación hombre-máquina (HMI) y los PLC, y para la regulación del IDS que asegure el intercambio de datos e información entre ellos. Para esto, desarrollaron un algoritmo que se centra en monitorear detalladamente la comunicación entre HMI y PLC, y capaz de determinar anomalías entre paquetes que no están dentro de su secuencia normal. Los resultados para los investigadores han sido positivos, pero no han intentado inyectar tráfico malicioso en la red, que interfiera en el funcionamiento del sistema SCADA y solamente han realizado pruebas en el sistema Modbus/TCP que se diseñó en el laboratorio.

[25] discuten acerca de la delicada situación de ciberseguridad por la que atraviesan los sistemas SCADA. Aseguran que los códigos maliciosos Spoofing, MITM y los ataques de integridad son el principal problema de seguridad a los que se deben enfrentar estos sistemas. Adicionalmente, proponen una metodología para aumentar su seguridad con un impacto mínimo en la eficiencia de este, el cual se basa en la autenticación mutua, confidencialidad, integridad de datos y la rendición de cuentas. Este proyecto ofrece una mejora en la seguridad del sistema SCADA con incorporación de nuevas políticas de administración y acceso, pero no proporciona un análisis de seguridad basado en un modelo de gestión de incidentes

En [26] proponen la integración de SCADA con IDS para crear un sistema de ciberseguridad por capas que se encargue de analizar el comportamiento de las redes inteligentes y las

infraestructuras críticas. Para el contexto de su investigación, las subestaciones de energía son nodos críticos esenciales para las funciones básicas de las redes eléctricas. En consecuencia, su funcionamiento fiable es esencial para asegurar la entrega de potencia que permanezca segura, estable y confiable. En este caso, la solución planteada muestra la integración de un sistema de control IDS que ayuda a mejorar la seguridad del sistema SCADA, mientras que este proyecto muestra una solución con mayor alcance.

El método planteado por [27] analiza la solidez de la prueba FMA (Finite Moving Average o Promedio Móvil Finito en español) a través de los datos generados por el filtro Kalman con algunos parámetros operativos en un sistema SCADA, incluyendo la duración del ataque, los perfiles de ataque, el proceso y las matrices de covarianza de ruido del sensor. El resultado del filtro no es óptimo cuando las innovaciones ya no son independientes y se debe recalcular la covarianza para alinear de nuevo los datos generados. Este proyecto solo evalúa el comportamiento del filtro para la disminución de ruido en las muestras que arroja el modelo FMA como su gran protagonista, mientras que el filtro Kalman guiará los resultados obtenidos en este proyecto como insumo de predicción de eventos para la gestión de incidentes de seguridad.

En el proyecto de [28] explican cómo los desastres naturales como las inundaciones amenazan constantemente la vida humana y como estos afectan eventualmente la economía. Para esta situación proponen un modelo de predicción de inundaciones utilizando NNARX (red neuronal) y un híbrido de NNARX con el filtro de Kalman. El modelo fue desarrollado usando datos generados en un sistema SCADA en tiempo real que fueron tomados del Departamento de Irrigación y Drenaje de Malasia. Aunque los resultados son positivos, el modelo se basa en datos ya generados y no están integrados al sistema SCADA como se propone en este proyecto.

Según [4] las organizaciones de infraestructura crítica dependen de los ICS (Sistemas de Control Industrial) mediante el uso de tecnologías operativas desarrolladas para sistemas comerciales en sus procesos diarios. Esto ha brindado una mayor oportunidad para los ciberataques contra los sistemas críticos actuales. El reciente cierre de Ukrainian Grid, demuestra que las amenazas cibernéticas a las redes eléctricas que operan bajo un sistema SCADA son reales. Esta investigación

se llevó a cabo en Arabia Saudita sobre los datos históricos de una empresa del sector eléctrico llamada National Grid SA, donde se realizaron ajustes en los modelos de ciberseguridad, pero no plantea un plan de gestión de incidentes.

[29] presentan la implementación de un modelo en LAB View para monitorear la temperatura de los sensores de fibra óptica de los devanados de un transformador. El sistema muestra de forma gráfica y ágil todos los resultados en un dashboard para que el administrador pueda gestionarlos e implementa el filtro Kalman para la reducción del ruido integrándolo con el sistema SCADA. El modelo solo muestra lo que está pasando sin ningún componente de predicción y sin presentar un modelo de gestión de incidentes a partir de los hallazgos encontrados.

En el proyecto de [30] evidencian lo difícil que es evitar que los atacantes se introduzcan físicamente en el sistema de control industrial (ICS), y además puedan conectar dispositivos externos al sistema para extraer información o inyectar datos falsos. En este documento, los autores proponen un método de detección de intrusión física para ICS, mediante el análisis de la señal de comunicación en la capa física. RS485, es uno de los bus serie más importante, más utilizado y está construido para representar la diferencia causada por la variación de los dispositivos y detectar los dispositivos intrusos. En su simulación se demuestra cómo se detecta un dispositivo intruso en un sistema RS485 de dos dispositivos, mientras que en este proyecto se realizará una detección basada en un comportamiento histórico, la cual ayudará a generar una predicción del comportamiento y se activará el modelo de incidentes de seguridad

En [31] comentan que con la llegada del mundo virtual, el mundo se ha convertido en una aldea global. Sin embargo, debido a los errores en la arquitectura de los sistemas SCADA, las infraestructuras críticas de los países son más propensas a los ataques cibernéticos. Lo cual expone una necesidad de generar y robustecer la seguridad cibernética para proteger información sensible y la infraestructura crítica de un país. En este documento, se analiza el terrorismo cibernético, las infracciones en los sistemas de redes SCADA y el concepto de resistencia cibernética para combatir los ataques cibernéticos como una revisión del estado del arte.

Por otro lado, [32]expresa la necesidad de afrontar los eventos de seguridad de una manera más proactiva, esto, consolidando diferentes procedimientos y procesos entorno al manejo de incidentes, y cómo estos deben ser ejecutados de manera periódica, por lo cual, crean una propuesta de alertas tempranas bajo la metodología de Ralph Kimball, visualizando las alertas y los niveles de seguridad para una red de computadores.

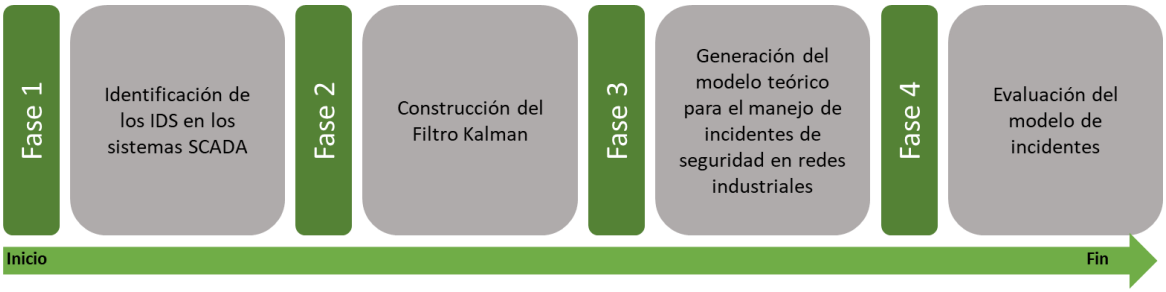
En ese sentido, el Centro de Ciberseguridad Industrial como organización independiente [33], hace un estudio sobre la Ciberseguridad Industrial en Colombia y en éste destacan la necesidad de contar con un CISO (chief information security officer) que permee todos los niveles de la organización, buscando reducir los impactos que pueden causar los eventos de ciberseguridad en la organización, y en especial, en los sectores que se enfocan o tienen su objeto de negocio en las infraestructuras críticas. En el mismo estudio, establecen que el 6.9% de las empresas que poseen alguna infraestructura crítica no posee un proceso para el manejo de incidentes de seguridad y el 17.2% actúa de manera reactiva ante los eventos, mientras que el 28% afirman estar definiendo los procesos.

Por lo anterior, definir y ejecutar un proceso para el manejo de incidentes de seguridad se vuelve fundamental, toda vez que las organizaciones requieren trabajar, de manera proactiva, en la reducción de riesgos de exposición ante ciberataques.

2. Metodología

Para lograr los objetivos propuestos, el proyecto se dividió en 4 fases (figura 2-1):

Figura 2-1: Metodología para el cumplimiento de los objetivos. Fuente autores.



A continuación, se describen cada una de las fases.

2.1. Identificación de los IDS

En la primera fase, se realizó una identificación de los diferentes sistemas de detección de intrusos que tengan su aplicabilidad en los sistemas SCADA, esto se obtuvo haciendo una búsqueda bibliografía en fuentes indexadas y en las páginas de los diferentes proveedores de seguridad (como Radware, SNORT, PaloAlto, entre otros), el resultado final es una tabla comparativa con diferentes aspectos considerados como sistemas IDS y sus funcionalidades. Para la tabulación de la tabla y la selección de los criterios se hizo uso de la suma ponderada (sistema de puntos) y con ello, se priorizó los IDS en temas de funcionalidades acorde a los sistemas SCADA.

Se evaluaron 10 sistemas de detección de intrusos, y a cada IDS se valoró en 12 aspectos diferentes (tabla 2-1). En consideración que el IDS a seleccionar debe estar en un ambiente industrial, es necesario que su implementación no afecte el rendimiento promedio del sistema SCADA, por lo cual, a cada aspecto se le dio el mismo peso (para un total de 100) ponderado acorde a la necesidad misma del proyecto.

El IDS seleccionado es aquel que obtenga el mayor número de puntos, si existiera 2 o más IDS con los mismos puntos, se revisan las características 3, 5, 6, 8 y 11, quién obtenga en éstas mayor puntaje será seleccionado.

Tabla 2-1 Ponderación de las características para la selección del IDS. Fuente autores.

No.	Características del IDS	Puntos	Consideración
1	Virtualización	9	Dada la facilidad de las plataformas o máquinas virtuales, el IDS debe poder ser instalado en este tipo de sistemas, con ello, se podría tener movilidad a la hora de fijar un IDS en otra red.
2	Alertas en tiempo real	9	Teniendo en cuenta que es un filtro predictivo, las alertas deben darse en tiempo real para poder actuar ante cualquier posible evento de seguridad.
3	Personalización de reglas	9	Los sistemas SCADA como elementos tecnológicos particulares, requieres de soluciones que se ajusten a sus necesidades, esto es, que se puedan personalizar reglas acordes al sistema y el proceso organizacional.
4	Modo NIDS	9	Parte fundamental de la detección es que se logre identificar desde la red cualquier posible anomalía, por ello debe tener funciones de NIDS (Network -IDS)
5	Solo IDS	10	La disponibilidad de la plataforma es lo primordial, por lo cual, los IDS debe ser configurados SOLO en modo lectura o monitoreo, no se puede permitir que queden en modo IPS (de forma nativa). Por esta razón, este factor (a diferencia de los demás) tiene un aumento en la puntuación. Un sistema IPS debe cursar el tráfico por el dispositivo, aumentando los falsos positivos hasta que el sistema se estabilice, pero esto puede tomar más tiempo de lo normal.
6	Open Source	9	Los presupuestos del proyecto son reducidos, por lo cual la necesidad es que el IDS pueda solventar dicha necesidad.
7	Multiprocesador	9	Muy alineado con la característica 1 y 9.

8	Protocolo Modbus	9	Los protocolos de comunicación de tipo Modbus son los usados para los sistemas PLC, por lo cual, es necesario que el IDS soporte dicho protocolo.
9	Multiplataforma	9	Es importante, en consideración con el ítem 1, que se permita la instalación del IDS acorde a los recursos y plataformas disponibles en la organización, para con ello dar más escalabilidad.
10	Automatización	9	Opción de poder automatizar tareas en la detección.
11	Experiencia de los investigadores	9	La experiencia en IDS para SCADA de los proveedores, comunidades o grupos de interés en fundamental para tener sistemas estables y actualizados.
	Total	100	

En esta misma fase, se hizo la instalación y configuración de un sistema SCADA y el IDS seleccionado (y la configuración de reglas) acorde a la tabla de características.

2.2. Construcción del filtro Kalman

En esta segunda fase, se realizó la construcción del filtro Kalman, el cual permite a través del modelo matemático, poder predecir eventos a partir de unas fuentes, dicho filtro se realizó como un programa software construido en Python3.7. Así mismo, en esta fase se configuró el IDS (con base en los resultados de la fase 1), para la configuración de las reglas de detección se generaron algunos ataques informáticos con el fin de validar, de manera unitaria, que el IDS está en funcionamiento. Finalmente, se integró el filtro Kalman al IDS, donde dichos sistemas de detección de intrusos fue la fuente para el filtro, con ello y las pruebas unitarias, se realizó una prueba de funcionalidad.

Dicho filtro se realizó en el lenguaje de programación Python, dada su versatilidad, funcionalidad y tiempo de respuesta a la hora de funcionar.

Para poner a prueba el laboratorio y la solución planteada en este proyecto, se seleccionan los siguientes ataques:

- Escaneo: Como primer vector de ataque, éste identifica qué dispositivos de la red industrial se encuentran disponibles y segmentarlos como posibles objetivos.
- Lectura: Este método pretende capturar la información real que generan los dispositivos del sistema SCADA, logrando obtener datos sensibles e importantes de la red industrial.
- Sobreescritura: Este explota una vulnerabilidad del protocolo modbus, el cual consiste en cambiar toda la información que se almacena dentro del PLC, comprometiendo su confidencialidad, disponibilidad e integridad.

Estos ataques se han seleccionado por considerarse la base o principios básicos e intermedios de una intrusión a sistemas de redes industriales SCADA.

2.3. Procedimiento para el manejo de incidentes de seguridad

En la tercera fase, se creó un procedimiento para la identificación y reacción ante eventos de seguridad, que es aplicable a los sistemas SCADA cuando se ha hecho una predicción de un posible ataque; dicho procedimiento se realizó a partir de la búsqueda selectiva en bases de datos de información sobre manejo de incidentes de seguridad y se revisaron las normas SP800-61 (de NIST), ISO 27035 y algunas recomendaciones de los proveedores (como Allient Vault).

Como resultado y en consideración que se trata de un modelo predictivo, esto es, el evento de seguridad o bien no ha sucedido o no ha generado el suficiente impacto, en consideración que el uso del filtro Kalman permite la predicción (de lo que pueda pasar en el futuro), algunas de las fases de los modelos para el manejo de incidentes de seguridad como contención, erradicación y recuperación no se contemplaron, dado que son fases que se ejecutan cuando un incidente de seguridad se ha consolidado y el modelo acá desarrollado es para una predicción. Las normas se cotejaron y se realizó un procedimiento que reúne lo mejor de ambas, de acuerdo con el contexto del proyecto.

Para la obtención del procedimiento se consideraron las diferentes etapas de las normas evaluadas, desde la planeación o preparación, hasta las lecciones aprendidas que permite retroalimentar el mismo proceso.

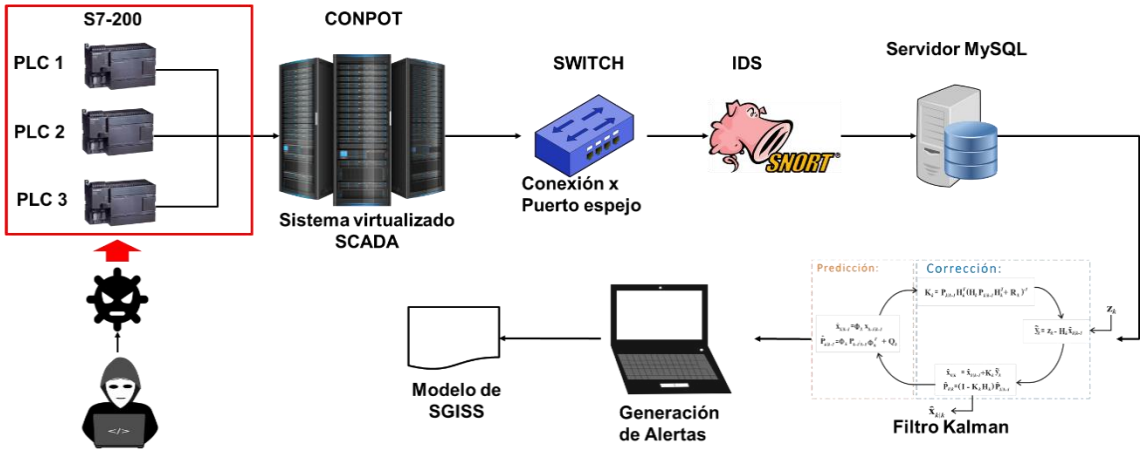
2.4. Evaluación del sistema

En la última fase se realizó la evaluación del sistema, partiendo de los resultados arrojados por la detección del IDS y pasado al filtro Kalman, generando una alerta predictiva de un posible ataque informático, con ello, se activa el proceso para el manejo de incidentes de seguridad.

Dicha ejecución del proceso se realizó a través de un caso de estudio. De acuerdo con lo anterior, se construyó un proceso de interacción para el manejo de incidentes una vez se ha detectado un evento con el filtro Kalman.

Para la validación, se implementó la siguiente arquitectura donde se integró cada uno de los componentes que facilita la metodología empleada (ver figura 2-2)

Figura 2-2: Arquitectura propuesta del proyecto. Fuente autores.



Para registrar los resultados de la evaluación del sistema, se hizo uso de una lista de chequeo [Anexo 1] que fue ejecutada por los autores con la participación del Director de Tesis, dicha lista considera la verificación del funcionamiento de cada uno de los componentes individuales de la

arquitectura, así como la integración de éstos con los demás elementos del proyecto, para así garantizar el flujo del proceso de predicción desde el momento en que se realiza un ataque a la red SCADA simulada con CONPOT hasta obtener la predicción del filtro Kalman y finalmente dependiendo del resultado de éste, es necesario activar el proceso para el manejo de incidentes de seguridad que se plantea en este proyecto.

3. Resultados

A continuación, se describen y entregan los diferentes resultados obtenidos acorde a la metodología planteada.

3.1. Identificación de los IDS en los sistemas SCADA

En este punto se realizará una comparación entre los diferentes IDS de acuerdo con unas características previamente establecidas, las cuales definirán el sistema de detección que mejor se ajusta a este trabajo. Finalmente, su configuración, implementación e integración con el sistema SCADA.

3.1.1. Comparación de los IDS

En la tabla 3-1 se hace la comparación de los diferentes sistemas de detección de intrusos consultados vs. las características evaluadas, que, acorde si cumple dicha característica, se fija una "x" para indicarlo.

Tabla 3-1 Comparación de los principales IDS. Fuente autores.

No.	Características	Peso	SNORT	Suricata	Kismet	Bro IDS	Ossec	Tripwire	Samhain	Fortinet	Radware	Palo Alto
1	Virtualización	9	x	x	x	x	x	x	x			
2	Alertas en tiempo real	9	x	x		x	x	x		x	x	x
3	Personalización de reglas	9	x	x		x	x					
4	Modo NIDS	9	x	x			x		x	x	x	x
5	Solo IDS	10	x		x	x				x		
6	Open Source	9	x	x		x	x		x			
7	Multiprocesador	9		x	x							x
8	Protocolo Modbus	9	x	x			x	x		x		x
9	Multiplataforma	9	x	x	x	x	x	x	x	x	x	x
10	Automatización	9	x	x	x	x	x	x		x	x	x

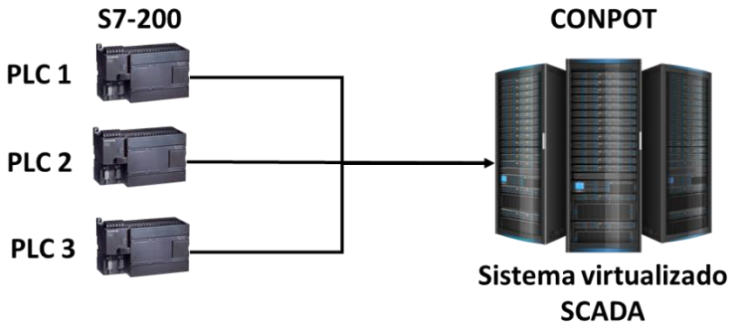
11	Experiencia de los investigadores	9	x									
Totales		100	91	81	46	64	72	45	36	55	36	54

En consideración con los pesos dados a las características y como se puede observar, el IDS SNORT es el más opcionado a ser implementado.

3.1.2. Estructura e implementación de Sistema SCADA

Como se ha mencionado anteriormente, los sistemas de control de supervisión y adquisición de datos (SCADA) se utilizan en las principales industrias y en infraestructuras críticas para lograr mayores niveles de eficiencia, seguridad y calidad [34]. Dicho esto, la implementación del sistema SCADA es de suma complejidad técnica y económica por la naturaleza del hardware requerido. Para este proyecto, se utilizará Conpot que es un honeypot de un sistema SCADA bajo un servidor interactivo diseñado para que sea implementado y configurado de una forma virtualizada y se pueda modificar y extender de acuerdo con la necesidad de cada proyecto. Igualmente puede proporcionar diferentes protocolos de comunicación como Modbus TCP, SNMP y HTTP. Además, es capaz de simular una infraestructura crítica compleja como es el sector eléctrico. También puede brindar la posibilidad de conectarse a una interfaz máquina hombre o HMI (por sus siglas en inglés) personalizada para emular un sistema real. Los tiempos de respuesta de los servicios pueden retrasarse artificialmente para imitar el comportamiento de un sistema bajo carga constante. Debido a que estamos proporcionando pilas completas de los protocolos, se puede acceder a Conpot con HMI productivos o con hardware real[35]. En la Figura 3-1 se puede observar cómo es su estructura.

Figura 3-1: Estructura Interna del Sistema CONPOT. Fuente autores.



Hace unos años, los sistemas SCADA eran más seguros a todo tipo de intrusiones y ataques que sufrían las redes de la organización, esto no quiere decir que este sistema fuese mucho más resistente, sino porque estaba desconectado y eran inaccesibles desde las redes administrativas o Internet. Actualmente estos sistemas aún se manejan desde un segmento de red separado e implícitamente "seguro", aun cuando el mismo computador donde se administra el sistema SCADA se encuentre instalado un cliente de servicio de correo electrónico y con acceso a internet.

En su inicio, su diseño se enfocaba en la funcionalidad y la seguridad física para limitar el acceso. Utilizaban tecnologías propietarias y poco probadas fuera de ambientes controlados. Esta metodología producía sistemas no preparados para ataques externos; con el fin de disminuir los costos, aumentar la implantación de mejoras y el desarrollo de nuevos sistemas, los sistemas SCADA hacen cada vez más uso de tecnologías estándar, como Microsoft Windows, TCP/IP, navegadores Web y las conexiones inalámbricas. De ese modo se consigue centrar los esfuerzos en la funcionalidad buscada, utilizando como base tecnologías ampliamente probadas y fiables. En la misma línea evolutiva, y gracias al tremendo avance de las comunicaciones y la conectividad de los últimos años, los sistemas SCADA han aumentado su conectividad a interconectarse con otros sistemas. Gracias a ello, ahora es posible utilizar sistemas SCADA distribuidos, o centralizar el control de instalaciones diversas, integrar los resultados del control de procesos en los sistemas administrativos y mejorar el rendimiento no sólo de la producción de toda la empresa.

3.1.3. Implementación SCADA Proyecto CONPOT

Desde el equipo de CONPOT recomiendan utilizar la distribución LINUX Ubuntu 12.04 LTS / 14.04 LTS como sistema operativo local para alojar el sistema SCADA[36], pero para el desarrollo de este proyecto se eligió Ubuntu Server 16.04 LTS por ser una distribución actualizada y estable que

mejora el rendimiento, este sistema operativo tendrá soporte hasta 2021 [37]. Para la instalación de este sistema operativo, se realizará a través de sistema de virtualización VMware Player 14.1.3 con la siguiente configuración, como se muestra en la tabla 3-2

Tabla 3-2 Configuración de hardware Ubuntu Server 16.04 LTS

Dispositivos	Descripción
Memoria RAM	512 MB
Processors	1
Hard Disk	20 GB
Network Adapter	NAT
IP	10.1.1.13
Mask	255.255.255.0

3.1.4. Instalación CONPOT

La instalación del sistema SCADA CONPOT en Ubuntu Server 16.04 LTS debe tener ciertos prerrequisitos que se cumplen con los siguientes paquetes:

```
$ sudo apt-get install git
$ sudo apt-get install cython
$ sudo apt-get install python-dev
$ sudo apt-get install python-pip
$ sudo apt-get install build-essential
$ sudo apt-get install libxml2-dev
$ sudo apt-get install libxslt1-dev
$ sudo apt-get install libevent-dev
$ sudo apt-get install snmp-mibs-downloader
```

Después de instalar las dependencias, se usó GIT para clonar modbus-tk, que es una implementación del protocolo Modbus en Python.

$ cd /opt

$ sudo git clone http://github.com/glastopf/modbus-tk.git

$ cd modbus-tk/

$ sudo python setup.py install

Después se debe clonar el proyecto desde **github** de CONPOT para su instalación

$ cd /opt

$ sudo git clone http://github.com/glastopf/conpot.git

$ cd conpot

$ sudo python setup.py install

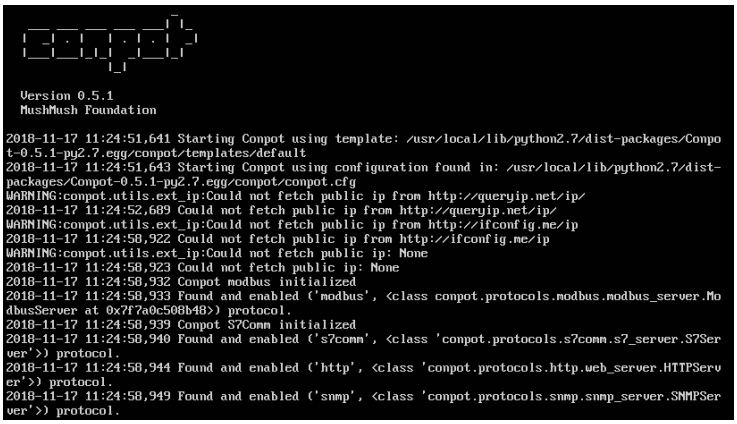
$ sudo conpot

Finalmente ejecutar la siguiente línea de comando para iniciar el sistema SCADA

$ sudo Conpot -t default

Si el proceso de instalación es correcto, se debe visualizar en pantalla como se muestra en la Figura 3-2.

Figura 3-2: Ejecución Sistema CONPOT. Fuente autores.



El proyecto Conpot simula un PLC SIMATIC S7-200 de Siemens. Si bien esto puede producir algunos datos interesantes, es aún más interesante que este dispositivo es el objetivo que va a recibir los ataques que se construirán (y serán explicados) durante el desarrollo de este trabajo.

3.1.5. Integración del IDS al sistema SCADA

De acuerdo con los resultados presentados en la tabla 2-1, SNORT es uno de los IDS más potentes y más adecuado para el propósito de este proyecto. Para la implementación y configuración de SNORT como N-IDS (sistema de detección de intrusos de red) y de acuerdo con la solución planteada desde la tipología de red, este N-IDS debe instalarse en una máquina independiente donde se encuentra el sistema SCADA. Para dicha instalación se configura una máquina virtual con las especificaciones que se muestran en la tabla 3-3

Tabla 3-3 Configuración de hardware Ubuntu Server 18.04 LTS.

Dispositivos	Descripción
Memoria RAM	512 MB
Processors	1
Hard Disk	20 GB
Network Adapter	NAT
IP	10.1.1.11
Mask	255.255.255.0

Además, se debe considerar la instalación de barnyard2, este software toma todos los datos generados por el N-IDS y los graba en una base de datos SQL y reduce la carga al sistema, mejorando significativamente su performance. En la tabla 3-4 se muestra las herramientas necesarias para la integración del IDS al sistema SCADA

Tabla 3-4 Software de apoyo del sistema SCADA.

Nombre	Versión
SNORT	2.9.9
Barnyard2	2-1.14
MySQL	Server versión 5.7.23-0ubuntu0.16.04.1 (Ubuntu)

Antes de iniciar el proceso de instalación de SNORT, se debe configurar debidamente la tarjeta de red para evitar que esta realice el reemsamblado de paquetes antes que sean procesados por el kernel. Por defecto, SNORT truncará paquetes más grandes que el tamaño predeterminado de 1518 bytes. Por tal razón se recomienda deshabilitar LRO y GRO en el archivo de configuración de red.

sudo nano /etc/network/interfaces

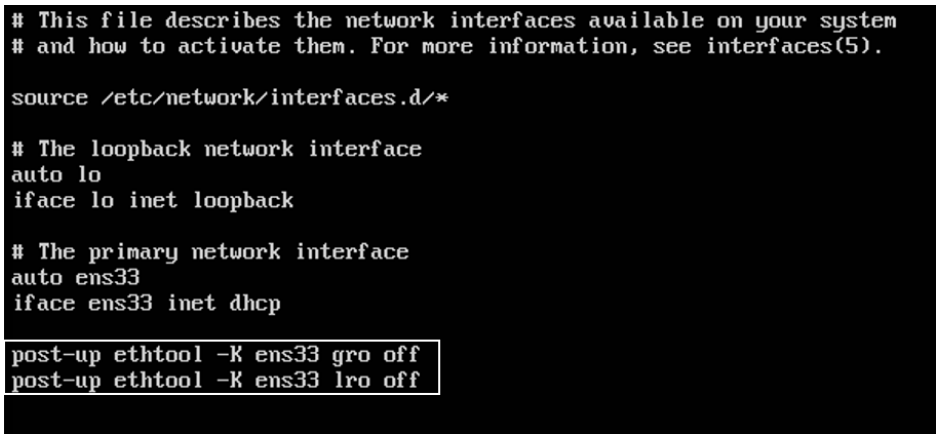
Y se agregan estas líneas al final del archivo

post-up ethtool -K ens33 gro off

post-up ethtool -K ens33 lro off

Finalmente se reinicia la red para verificar que tanto GRO, como LRO hayan sido deshabilitados correctamente, como se muestra en la figura 3-3

Figura 3-3: Deshabilitar LRO y GRO. Fuente autores.



Después de realizarlo, se debe continuar con los prerrequisitos

- build-essential
- ibpcap-dev
- libpcre3-dev
- libdumbnet-dev

- bison
- flex

Ahora ya está preparado el sistema operativo para la instalación del IDS SNORT. Para instalarlo en Ubuntu, es necesario instalar un requisito previo adicional que no se menciona en la documentación: zlibg, que es una biblioteca de compresión.

Hay cuatro bibliotecas opcionales que mejoran la funcionalidad: liblzma-dev, tres de las cuales proporcionan descompresión de archivos swf (adobe ash), openssl y libssl-dev que proporcionan firmas de archivos SHA y MD5. Esto se realiza con las siguientes líneas de comando:

```
sudo apt-get install -y zlib1g-dev liblzma-dev openssl libssl-dev
sudo apt-get install -y libnghttp2-dev
```

Ya con todo el sistema operativo preparado, solo queda la instalación de SNORT, a través de las siguientes líneas

```
cd ~/snort_src
wget https://snort.org/downloads/archive/snort/snort-2.9.9.0.tar.gz
tar -xvzf snort-2.9.9.0.tar.gz
cd snort-2.9.9.0
./configure --enable-sourcefire
make
sudo make install
```

Adicionalmente, se debe validar si el IDS está correctamente instalado, como se muestra en la figura 3-4.

Figura 3-4: Versión de SNORT. Fuente autores.

```
root@VM8:~# snort -v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.9.0 GRE (Build 56)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.7.4
           Using PCRE version: 8.38 2015-11-23
           Using ZLIB version: 1.2.8
```

Para la ejecución de SNORT en el sistema, se debe crear un usuario y un grupo sin ningún tipo de privilegios para que cuando se ejecute en modo Daemon, lo realice bajo snort:snort. Luego se crean una serie de archivos y directorios necesarios para su configuración, estableciendo los permisos necesarios para su funcionamiento. SNORT tendrá los siguientes directorios: Configuraciones y reglas en / etc / snort Las alertas se escribirán en / var / log / snort Las reglas se almacenarán en / usr / local / lib / snort dynamicrules.

Para poder simplificar la evaluación de este proyecto y la integración con el sistema SCADA, se deshabilitan todas las reglas que vienen por defecto en SNORT en su archivo de configuración snort.conf y se realiza con la siguiente sentencia:

sudo sed -i "s/include \$RULE_PATH/#include \$RULE_PATH/" /etc/snort/snort.conf

Adicionalmente se configura la red que se está monitoreando y se cambia por el rango que se está utilizando en el proyecto con mascara /24 con la siguiente línea:

ipvar HOME_NET 10.1.1.0/24

Se habilitan las siguientes rutas en el archivo de configuración snort.conf para que el IDS pueda leer las reglas que se crearán en el desarrollo de este proyecto

var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists

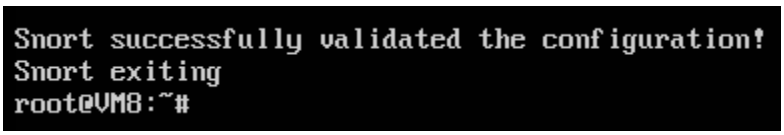
Y se habilita el archivo local.rules donde se crearán posteriormente las reglas de las que se alimenta SNORT
include $RULE_PATH/local.rules

Una vez que el archivo de configuración esté listo, se debe verificar que SNORT tenga un archivo de configuración válido y que todos los archivos de referencia necesarios sean correctos.

sudo snort -T -i ens33 -c /etc/snort/snort.conf

Se usa -T para probar el archivo de configuración, -c para indicarle a SNORT qué archivo de configuración debe usar, -i para especificar cual interfaz de red va a escuchar (nuevo requisito desde la versión 2.9.x). Si esto es correcto, la consola debe mostrar un resultado positivo como se muestra en la figura 3-5.

Figura 3-5: Validación configuración de SNORT. Fuente autores.



Ahora que el IDS SNORT está configurado y funcionando correctamente, se debe instalar la herramienta Barnyard2 para que los datos generados a partir de la detección del IDS, sean almacenados en una base de datos estructurada SQL independiente y de esta manera poder

realizar consultas de forma efectiva y ágil. Para realizar esta instalación se debe cumplir unos requisitos previos, como MySQL y sus librerías necesarias para su funcionamiento correcto

sudo apt-get install -y mysql-server libmysqlclient-dev mysql-client autoconf libtool

Después de instalar los paquetes anteriores, se debe configurar en el archivo snort.conf donde se le indique el tipo de salida de las alertas generadas por el IDS y debe ser unified2 con la siguiente línea

output unied2: filename snort.u2, limit 128

Luego se realiza la instalación de Barnyard

```
wget https://github.com/firnsy/barnyard2/archive/master.tar.gz -O barnyard2-Master.tar.gz
tar zxvf barnyard2-Master.tar.gz
autoreconf -f -v -i -I ./m4
automake --add-missing
aclocal
```

Cuando la instalación esté completa, se debe configurar MySQL creando una base de datos a partir del archivo que viene por defecto con Barnyard2, un usuario nuevo con el nombre de snort y adicionalmente, asignarle todos los privilegios para que se pueda poblar la base de datos sin ningún inconveniente, lo anterior se realiza con el siguiente código

```
$ mysql -u root -p
mysql> create database snort;
mysql> use snort;
mysql> source ~/snort_src/barnyard2-master/schemas/create_mysql
mysql> CREATE USER 'snort'@'localhost' IDENTIFIED BY 'MySqlSNORTpassword';
mysql> grant create, insert, select, delete, update on snort.* to 'snort'@'localhost';
mysql> exit
```

Posteriormente, modificar el archivo de configuración de Barnyard2 e indicarle donde se guardará los datos generados por el IDS

output database: log, mysql, user=snort password=MySqlSNORTpassword dbname=snort host=localhost sensor name=sensor01

Y por último, ejecutar SNORT en modo NIDS

$ sudo /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33

Finalizando este proceso, ya SNORT está configurado y listo para realizar la detección de intrusiones basado en las reglas que se encuentren creadas y configuradas en el archivo local.rules en la ruta /etc/Snort/rules. Para garantizar que el sistema de detección de intrusos de red siempre esté disponible y se inicie con el sistema operativo, se realiza la configuración en los archivos snort.service y barnyard2.service, como se muestra en las figuras 3-6 y 3-7.

Figura 3-6: Inicio automático SNORT NIDS Daemon. Fuente autores.

```
[Unit]
Description=Snort NIDS Daemon
After=syslog.target network.target

[Service]
Type=simple
ExecStart=/usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i ens33

[Install]
WantedBy=multi-user.target
```

Figura 3-7: Inicio automático Barnyard2 Daemon. Fuente autores.

```
[Unit]
Description=Barnyard2 Daemon
After=syslog.target network.target

[Service]
Type=simple
ExecStart=/usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -q -w$

[Install]
WantedBy=multi-user.target
```

Luego se debe reiniciar los servicios que se acaban de crear para que inicien con el sistema operativo.

3.2. Construcción del filtro Kalman

En este punto se describe la implementación de las herramientas tecnológicas para la predicción, la configuración de las reglas del IDS SNORT y la caracterización de los ataques simulados que preparan un escenario bajo ataque para el proyecto.

3.2.1. Instalación y configuración de OpenCV

OpenCV (Open Source Computer Vision) es una librería de código abierto con licencia de BSD que incluye varios cientos de algoritmos de visión artificial basada en C++ y además contiene todas las librerías necesarias para el funcionamiento del filtro Kalman. Esta API puede ser utilizada en muchos lenguajes de programación cómo, C, C++, C#, Python, entre otros. A continuación, se explica la instalación y configuración [38].

Antes de iniciar la instalación, se debe remover la librería libx264-dev para garantizar que esta sea instalada en su última versión, esto se realiza con el siguiente comando

sudo apt -y remove x264 libx264-dev

Luego se debe instalar las dependencias como se muestra en la figura 3-8.

Figura 3-8: Instalación de dependencias OpenCV. Fuente autores.

```
sudo apt -y install build-essential checkinstall cmake pkg-config yasm
sudo apt -y install git gfortran
sudo apt -y install libjpeg8-dev libpng-dev

sudo apt -y install software-properties-common
sudo add-apt-repository "deb http://security.ubuntu.com/ubuntu xenial-security main"
sudo apt -y update

sudo apt -y install libjasper1
sudo apt -y install libtiff-dev

sudo apt -y install libavcodec-dev libavformat-dev libswscale-dev libdc1394-22-dev
sudo apt -y install libxine2-dev libv4l-dev
cd /usr/include/linux
sudo ln -s -f ../libv4l1-videodev.h videodev.h
cd "$cwd"

sudo apt -y install libgstreamer1.0-dev libgstreamer-plugins-base1.0-dev
sudo apt -y install libgtk2.0-dev libtbb-dev qt5-default
sudo apt -y install libatlas-base-dev
sudo apt -y install libfaac-dev libmp3lame-dev libtheora-dev
sudo apt -y install libvorbis-dev libxvidcore-dev
sudo apt -y install libopencore-amrnb-dev libopencore-amrwb-dev
sudo apt -y install libavresample-dev
sudo apt -y install x264 v4l-utils
```

Y continúa la instalación de python3 para preparar todo el entorno de desarrollo y la preparación de OpenCV (figura 3-9).

Figura 3-9: Instalación de python3. Fuente autores.

```
sudo apt -y install python3-dev python3-pip
sudo -H pip3 install -U pip numpy
sudo apt -y install python3-testresources
```

Después se ejecutan las siguientes sentencias en la línea de comando para clonar desde el portal de Github el proyecto de opencv y opencv_contrib, según la figura 3-10.

Figura 3-10: Clonación del proyecto OpenCV desde Github. Fuente autores.

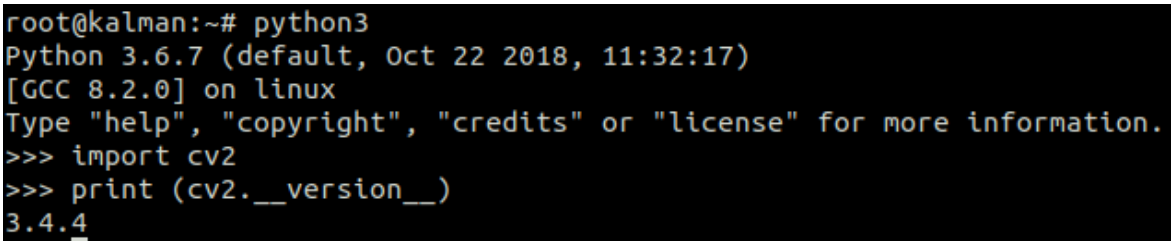
```
git clone https://github.com/opencv/opencv.git
cd opencv
git checkout $cvVersion
cd ..

git clone https://github.com/opencv/opencv_contrib.git
cd opencv_contrib
git checkout $cvVersion
cd ..
```

Por último, cambiar al directorio donde se descargó el proyecto y ejecutar el comando “make install” para que inicie el proceso de instalación de OpenCV en el sistema (esto puede tardar varios minutos). Con este proceso finalizado, el entorno del sistema operativo Linux se encuentra preparado para ejecutar Opencv desde el lenguaje de programación Python.

Es importante validar que la instalación y configuración del entorno sea correcto para su funcionamiento y se realiza con las siguientes instrucciones a través de una consola de comandos como se muestra en la figura 3-11.

Figura 3-11: Validación instalación OpenCV + Python. Fuente autores.



3.2.2. Caracterización de los ataques al sistema SCADA

El primer evento simulado muestra cómo a través del protocolo Modbus se puede acceder a los datos que recolecta el PLC Siamens 2700, este PLC es comúnmente utilizado en los sistemas SCADA que se encuentran alojados en cualquier infraestructura crítica como el sistema eléctrico, represas, entre otras. Para lograr leer dichos datos se utiliza el lenguaje de programación Python y se crea una rutina que captura la hora de inicio del evento y cuantas veces se desea repetir este ataque, luego de obtener el número de repeticiones inicia el ciclo donde se le indica la dirección IP donde se encuentra el dispositivo que se va a intervenir con la instrucción READ y %M100, la cual significa “lectura” más la posición de lectura, que va desde 1 hasta 29 (para este ejercicio se ejecutará aleatoriamente, en la figura 3-12 se muestra su codificación.

Figura 3-12: Lectura de datos al PLC Siemens 2700 con protocolo modbus. Fuente autores.

```
import subprocess
import time
from random import randint

FechaInicial=time.strftime("%H:%M:%S")+ " "+ time.strftime("%d/%m/%y")
veces = int(input("¿Cuántas veces quiere relizar la lectura de datos? "))
print("")
print("Inicio de lectura de datos " + str(time.strftime("%H:%M:%S")))

for n in range(veces):
    subprocess.call(["modbus read 10.1.1.13 %M100 "+ str(randint(1, 29))], shell=True)
    print("Lectura número: " + str(n+1) + " Hora: " + str(time.strftime("%H:%M:%S")))

FechaFinal=time.strftime("%H:%M:%S")+ " "+ time.strftime("%d/%m/%y")
print("")
print("Proceso Finalizado " + str(FechaFinal))
print("Inició    " + str(FechaInicial))
print("Terminó   " + str(FechaFinal))
```

Para el segundo evento, se utilizará el modo escritura con el comando WRITE, el cual sobre escribirá todos los datos del PLC y así generar información falsa cuando los datos sean consultados por el administrador del sistema (figura 3-13).

Figura 3-13: Sobrescribir de datos al PLC Siemens 2700 con protocolo modbus. Fuente autores.

```
import subprocess
import time
from random import randint

FechaInicial=time.strftime("%H:%M:%S")+ " "+ time.strftime("%d/%m/%y")
veces = int(input("¿Cuántas veces quiere relizar la escritura de datos? "))
print("")
print("Inicio de escritura de datos " + str(time.strftime("%H:%M:%S")))

for n in range(veces):
    subprocess.call(["modbus write 10.1.1.13 %M100 " + str(randint(0, 1)) + " " + str(randint(0, 1)) + " " +
        str(randint(0, 1)) + " " + str(randint(0, 1)) + " " + str(randint(0, 1)) + " " + str(randint(0, 1)) + " " +
        str(randint(0, 1)) + " " + str(randint(0, 1)) + " " + str(randint(0, 1)) + " " + str(randint(0, 1))], shell=True)
    print("Escritura número: " + str(n+1) + " Hora: " + str(time.strftime("%H:%M:%S")))

FechaFinal=time.strftime("%H:%M:%S")+ " "+ time.strftime("%d/%m/%y")
print("")
print("Proceso Finalizado " + str(FechaFinal))
print("Inició    " + str(FechaInicial))
print("Terminó   " + str(FechaFinal))
```

3.2.3. Creación y configuración de reglas del IDS SNORT

Como se mencionó en la configuración del IDS SNORT, el archivo local.rules será el que alojará las reglas personalizadas. Para el desarrollo de este proyecto, se configuró cuatro reglas para que sean detectadas por SNORT.

Regla 1 Escaneo: Esta regla detecta un ping o escaneo desde una IP externa al sistema SCADA.

alert icmp $HOME_NET any -> any any (msg:"ICMP Detectado"; GID:1; sid:50000001; rev:001; classtype:icmp-event;)

Regla 2 Conexión Modbus 1: Se identifica si algún dispositivo está intentando hacer conexión a través del puerto 502 que pertenece al protocolo Modbus.

alert tcp $HOME_NET any -> 10.1.1.13 502 (content:!"|02|"; offset:7; depth:1; flow:established, to_server; msg:" Conexión Modbus"; sid:1000001;rev:0;priority:5;)

Regla 3 Escribiendo datos en PLC: Esta regla escanea cada uno de los paquetes que viajan hacia el PLC a nivel binario, si el bit 7 en su cabecera muestra que ha cambiado por el valor “0f”, significa que la información ha sido intervenida y transformada, lo que significa que los datos son falsos.

alert tcp any any -> 10.1.1.13 502 (msg: "Escribiendo datos en PLC"; content:"|0f|";offset:7;depth:1; sid:1111102;rev:2;priority:5;)

Regla 4 Leyendo datos del PLC: Es igual a la regla anterior, solo que si el valor es “01” significa que el PLC está comprometido y los datos están siendo leídos comprometiendo la seguridad del sistema.

alert tcp any any -> 10.1.1.13 502 (msg:"Leyendo datos del PLC"; content:"|01|";offset:7;depth:1;sid:11111103;rev:2;priority:3)

3.2.4. Desarrollo de la herramienta de predicción

Conservando la integridad de la solución, se plantea que el desarrollo de la herramienta sea en Python. Este lenguaje de programación permite trabajar rápidamente e integrar sistemas de manera más efectiva y también es conocido por su gran comunidad que aporta a su crecimiento y evolución continúa [39].

Antes de iniciar el desarrollo es necesario la incorporación de las librerías *numpy y mysql.connector*

- numpy: Es el paquete fundamental para la computación científica con Python. También se puede usar como un eficiente contenedor multidimensional de datos genéricos y pueden definir tipos de datos arbitrarios que permite que NumPy se integre a la perfección con una amplia variedad de bases de datos. NumPy está bajo la licencia BSD, lo que permite su reutilización con pocas restricciones [40].
- mysql.connector: Este paquete sirve para crear la conexión al servidor de bases de datos MySQL que contiene los datos generados por los ataque simulados al sistema SCADA CONPOT.

Para iniciar con el desarrollo, primero se debe importar las librerías/paquetes como se muestra en la siguiente imagen (figura 3-14).

Figura 3-14: Librerías necesarias para filtro Kalman en Python. Fuente autores.

```
import numpy as np
import mysql.connector
```

Luego se establece la conexión remota con la base de datos SNORT que se encuentra en el servidor con la dirección IP 10.1.1.11. Para acceder remotamente a dicha base de datos, primero se debe crear un nuevo usuario y grupo de usuarios en la base de datos MySQL y se realiza con las siguientes líneas de comando desde el bash de la base de datos

```
$ mysql -u root -p
mysql> CREATE USER 'kalman'@'10.1.1.17' IDENTIFIED BY 'kalman';
mysql> grant create, insert, select, delete, update on snort.* to 'kalman'@'10.1.1.17';
mysql> exit
```

Inicialmente se concede al nuevo usuario “kalman” de la base de datos, todos privilegios para que pueda ejecutar cualquier sentencia en ella, pero cuando se finalice el proceso de desarrollo, sólo quedará con permisos de lectura y ejecución de procedimientos almacenados por seguridad e integridad de la base de datos.

Luego se crea el procedure TablaPivote que va a servir de entrada al filtro Kalman, esto también se realiza desde el bash de la base de datos (figura 3-15).

Figura 3-15: Creación Store Procedure TablaPivote. Fuente autores.

```
CREATE PROCEDURE `TablaPivote`(IN intLimite int)
BEGIN
    SELECT t.fecha,
        sum(if(cod='513', Contador, 0)) as '513',
        sum(if(cod='514', Contador, 0)) as '514',
        sum(if(cod='515', Contador, 0)) as '515'

    FROM(
            SELECT e.timestamp as fecha, e.signature as cod, COUNT(e.timestamp) as Contador
            FROM event e
            group by e.timestamp,e.signature
            ORDER BY e.timestamp DESC
        ) AS t
    GROUP BY t.fecha
    ORDER BY t.fecha DESC
    LIMIT intLimite;
END
```

Ahora que se ha creado el nuevo usuario en la base de datos, luego en la herramienta se configura el string de conexión y el objeto de conexión (figura 3-16).

Figura 3-16: Conexión a la base de datos SNORT. Fuente autores.

```
# Consultar datos en la Base de datos de Mysql
config_mysql = {
    'user': 'kalman',
    'password': 'kalman',
    'host': '10.1.1.11',
    'database': 'snort',
    }
conector = mysql.connector.connect(**config_mysql)
cursor = conector.cursor()
```

Se ejecuta el Store procedure que se creó anteriormente (figura 2-15) para traer la información de la base de datos, luego se declara la matriz *v_sql* con *numpy* y se llena con los datos de la base de datos. El vector *v_fecha* almacenará la información del *timestamp* en que se generaron los eventos de seguridad y por último se cierra la conexión a la base de datos (figura 3-17)

Figura 3-17: Datos generados por los ataques simulados. Fuente autores.

```
query = ("call TablaPivote('"+ str(intLimite) +"');")
cursor.execute(query)

i=0
for (fecha, evento513, evento514,evento515) in cursor:
    v_fecha[i] = str(fecha)
    v_sql[0][i]= evento513
    v_sql[1][i]= evento514
    v_sql[2][i]= evento515
    i = i +1
    #time.sleep(1)
cursor.close()
conector.close()
```

En este paso se prepara el filtro con valores iniciales para que se pueda calcular las matrices de transición y la de observación, adicionalmente se configura la variable *n_iter* para indicarle al filtro cuantas iteraciones debe hacer para mejorar el resultado, en este caso es igual a 5 pero puede ser configurado a voluntad. La matriz *measurements* es muy importante en este momento porque indica y entrega los datos reales para que el filtro realice la predicción generando los nuevos datos para el filtro como se muestra en la figura 3-18.

Figura 3-18: Datos de entrada Filtro Kalman. Fuente autores.

```
def inicio_kalman_xy():
    x = np.matrix('0. 0. 0. 0.').T
    P = np.matrix(np.eye(4))*1000 # Matriz de incertidumbre
    N = 20
    intAtaques=3
    v_sql = np.zeros((intAtaques,N))
    v_kalman = np.zeros((N,intAtaques))
    v_fecha = ['1','2','3','4','5','6','7','8','9','0', '1','2','3','4','5','6','7','8','9','0']
    true_x = np.arange(1, N + 1, 1)
```

- X es el vector de estado inicial
- P es la matriz de incertidumbre
- N es número de resultados que se desean evaluar simultáneamente
- IntAtaques es el número de incidentes o ataques que se están simulado

Luego de preparar los datos para el filtro Kalman, se llama la función *datos* con los vectores *v_fecha* y *v_sql* para llenarlos con valores desde la base de datos que se configuró anteriormente y se agrega ruido a la medición con la variable R. Después se hace un recorrido que va desde cero a dos para asignarle los valores en la posición *m* en el arreglo *observed_y* que contiene el número real de los eventos detectados por el IDS, más el ruido generado para que el filtro pueda realizar una predicción con mayor exactitud y se procede a llenar la matriz v_kalman con los valores de la predicción del filtro (ver figura 3-19).

Figura 3-19: Filtro Kalman. Fuente autores.

```
def kalman(x, P, measurement, R, motion, Q, F, H):
    # Actualización de  x, P basado en medición m
    # distancia entre la posición actual y la predicción
    y = np.matrix(measurement).T - H * x
    S = H * P * H.T + R  # covarianza residual
    K = P * H.T * S.I    # Aplicaión de nuevo del filtro Kalman
    x = x + K*y
    I = np.matrix(np.eye(F.shape[0])) # matriz de identidad
    P = (I - K*H)*P

    # predicción x, P basado en la variación
    x = F*x + motion
    P = F*P*F.T + Q

    return x, P
```

A continuación, se muestra la implementación del algoritmo completo en Python (ver figura 3-20).

Figura 3-20: Datos de entrada Filtro Kalman. Fuente autores.

```
    while (blnEstado == 1):
        datos(v_fecha,v_sql )
        observed_x = true_x
        R = 0.01**2
        for m in range(intAtaques):
            observed_y = v_sql[m] + 0.05*np.random.random(N)*v_sql[m]
            n=0
            for meas in zip(observed_x, observed_y):
                x, P = kalman_xy(x, P, meas, R)
                v_kalman[n][m]= x[1]
                n = n +1
        os.system('clear')
        encabezado()

        for i in range(N):
            print(str(v_fecha[i])
                  + "    " + str(g).zfill(4)
                  + "    Real 513 = "  + str(v_sql[0][i])
                  + "    Pred   {:,.2f}".format(v_kalman[i][0])
                  + "    Real 514= "  + str(v_sql[1][i])
                  + "    Pred   {:,.2f}".format(v_kalman[i][1])
                  + "    Real 515= "  + str(v_sql[2][i])
                  + "    Pred   {:,.2f}".format(v_kalman[i][2])

                  )
```

Para organizar visualmente el reporte donde se muestran los resultados, se utiliza el siguiente código de la figura 3-21 para mejorar la apariencia en el encabezado.

Figura 3-21: Datos de entrada Filtro Kalman. Fuente autores.

```
def encabezado():
    #print("\r\n ")
    print("\r\n ")
```

```
    print("  -------------------------------------------------------------")
    print("  | 513  Es un ataque DoS")
    print("  | 514  Es un ataque Escritura")
    print("  | 515  Es un ataque Lectura")
    print("  | Pred Muestra la predicción del filtro kalman")
    print("  -------------------------------------------------------------  \r\n")
```

Como se puede apreciar, el filtro genera 4 salidas por consola:

- 513 para ataques DoS
- 514 para ataques de escritura
- 515 para ataques de lectura
- Pred: muestra la predicción acorde a los ataques.

3.3. Modelo para el manejo de incidentes de seguridad en redes industriales

En esta parte se comparan, analizan y relacionan las guías para el manejo y gestión de incidentes de seguridad: ISO 27035 [41] y NIST SP800-61 [5], que servirán de base para la creación del nuevo modelo de detección de incidentes en relación con el sistema predictivo que se propone en este proyecto.

3.3.1. Comparación de los diferentes modelos de gestión de incidentes

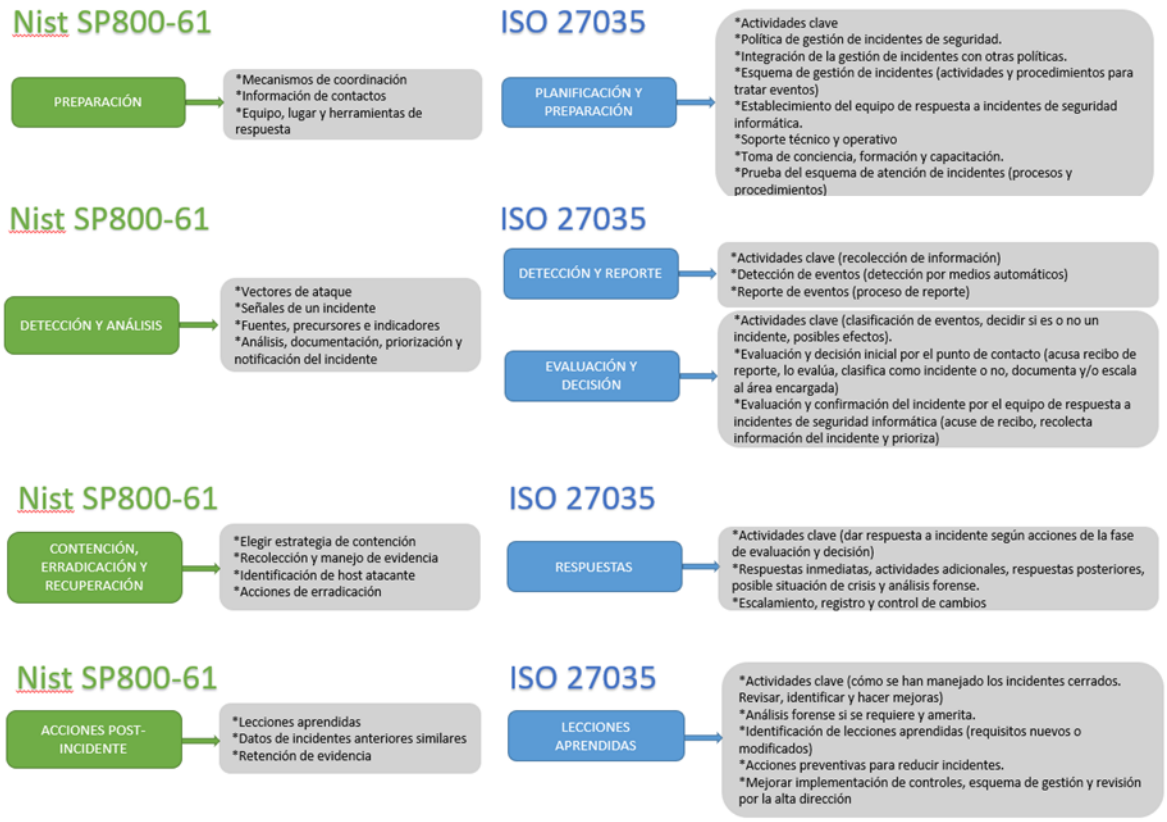
Para el modelo de gestión de incidentes de seguridad informática basado en predicción de eventos que se propone en este trabajo, se tomaron como base y referencia dos guías para el manejo y gestión de incidentes de seguridad: la ISO 27035 [41] y NIST SP800-61 [5], los cuales brindan un acercamiento y orientación de cómo afrontar y gestionar los incidentes de seguridad una vez se hayan identificado o materializado, es decir, la gestión o manejo reactivo a los incidentes de seguridad informática, así como un acercamiento al plan, políticas y procedimientos que deberán ser llevados a cabo por el equipo de respuesta según su estructura organizativa y funcional.

Las guías antes mencionadas son útiles en su totalidad cuando se trata de un incidente de seguridad que ha ocurrido o está ocurriendo. En el caso del modelo de gestión que se desarrolló en este trabajo, el componente de predicción es primordial y algunas fases de las metodologías antes indicadas no son tan útiles en la medida de que la predicción trata un acontecimiento que puede o no suceder, es decir, puede convertirse en un incidente o puede no llegar a serlo, por lo que algunos procedimientos de las guías de referencia son parcialmente eficientes cuando se trata de gestionar una predicción.

Es por lo anterior, se han revisado cada una de las metodologías o guías de gestión de incidentes de seguridad de la información mencionadas, tomando lo mejor de cada una de ellas y complementando el modelo para la gestión de incidentes de seguridad en redes industriales SCADA a través del algoritmo de predicción del Filtro Kalman.

A continuación, se presentan las características principales de cada una de las metodologías contempladas en este trabajo, dichas características se basan en las fases del ciclo de vida de la gestión tradicional de incidentes de seguridad de la información de NIST SP800-61 e ISO 27035.

Figura 3-22: Características principales de NIST SP800-61 e ISO 27035 [5], [42]



A continuación, se realiza una descripción de las fases definidas dentro del ciclo de vida de cada una de las guías o metodologías tomadas como referencia para la construcción del modelo de gestión basado en la predicción. Se resalta la relevancia de cada una de las fases de las guías y se

determina su utilidad en relación y aporte para el modelo que se construye tomando como prioridad su componente predictivo.

Existe una equivalencia entre las fases de ambas guías, las cuales se compararán para determinar las mejores prácticas en relación con la conveniencia y acercamiento al modelo que se plantea en este trabajo de la siguiente forma.

Se establece una equivalencia entre la fase de preparación de NIST SP800-61 y la fase de planificación y preparación de ISO 27035, donde se resaltan los siguientes aspectos:

Figura 3-23: Etapa 1 Preparación NIST SP800-61[5], [42]

En esta fase (figura 3-23) se describen de forma general los mecanismos que se deben tener en cuenta para establecer la coordinación y organización de las diferentes partes involucradas y que intervienen durante el proceso de gestión de incidentes, así como la información correspondiente a su contacto debe estar definido en esta fase. Igualmente se debe definir el equipo que dará gestión y tratamiento a los incidentes de seguridad, establecer su contacto y definir las herramientas que serán utilizadas para gestionar los incidentes de seguridad de la información, ya que el equipo encargado de la solución o gestión de los incidentes no necesariamente es el mismo que se encarga de la preparación, en esto se hace especial énfasis en esta fase de preparación.

Planificación y preparación ISO 27035

La fase de planificación y preparación de ISO 27035 define que deben existir una serie de actividades preparatorias que deben contemplar el mejoramiento o formulación de políticas de gestión de incidentes, formular esquemas de gestión de incidentes y sus procedimientos, definir estrategias de comunicación para preservar las relaciones internas como externas, entre otras. También contempla la integración de políticas en la organización, que consiste en incluir temas de

gestión de incidentes en políticas de gestión de riesgos, acuerdos de niveles de servicio, planes de recuperación de desastres y análisis de impacto de negocio.

Esta fase también propone definir las actividades y procedimientos para tratar los incidentes de seguridad, así como las partes interesadas y el grupo que se encargará de atender los incidentes y las recomendaciones para definir sus miembros y estructura de acuerdo al tamaño, estructura y naturaleza del negocio donde se implementará, así como definir los medios técnicos o herramientas que se dispondrán para que dicho equipo brinde respuestas rápidas y eficaces a los incidentes que se presenten. También contempla aspectos de capacitación y formación para los miembros del equipo y programas de toma de conciencia sobre seguridad para todas las personas de la organización.

Finalmente propone realizar pruebas regulares a los procesos y procedimientos de gestión de incidentes para destacar las fallas y problemas potenciales que puedan surgir durante la agestión de los incidentes de seguridad, estas pruebas se proponen bajo escenarios simulados y controlados basados en amenazas reales.

De las fases anteriores, se toman algunos aspectos que aportan al modelo propuesto enfocado en la predicción y que ayuda a definir de forma general la primera fase del modelo con aspectos como los siguientes:

- Información de contactos y partes interesadas, así como los escalamientos correspondientes que permitan orientar el flujo de los procedimientos según se requiera.
- Recomendaciones para el equipo que se encargará de abordar la gestión de incidentes de seguridad para definir adecuada y ágilmente el procedimiento para el tratamiento o gestión de los incidentes o predicciones que se reporten.
- Recomendaciones de adopción o inclusión de políticas de gestión de incidentes e integración con otras políticas.
- Sugerencias para mantener la formación y capacitación de las partes involucradas en la gestión de incidentes de seguridad.

- Definir procesos y procedimientos generales claves para un esquema de atención de incidentes

Figura 3-24: Etapa 2 Detección y análisis NIST y detección y reporte; evaluación y decisión de ISO 27035 [5], [42]

Se considera un relacionamiento entre las dos fases (figura 3-24), en el cual se resaltan los siguientes aspectos:

Detección y análisis NIST SP800-61

En esta fase se contempla inicialmente las definiciones más comunes de los métodos de ataque como base para definir los procedimientos más adecuados en la gestión de incidentes de seguridad. También se aborda la forma de detectar acertadamente un incidente de seguridad y sobre las formas en que se puede hacer de forma automática, al igual que las categorías de los incidentes de seguridad como lo son los precursores e indicadores. En relación con los *precursores*, son aquellos signos de que un incidente puede ocurrir en un futuro, mientras los *indicadores* son un signo de que un incidente pudo haber ocurrido o estar ocurriendo. En el caso de los primeros, se brindan algunos ejemplos de ellos y se indica que, si la organización puede detectar precursores, puede tener la oportunidad de evitar incidentes de seguridad informática modificando su postura de seguridad para hacer frente con acciones adecuadas según lo que se identifique.

En lo correspondiente al análisis de incidentes, se indica que el equipo encargado de la gestión debe determinar el alcance validando qué estuvo, está o estará comprometido; qué o quién lo generó y de qué forma funciona o afecta los sistemas involucrados. El análisis debe ser lo suficientemente amplio y brindar la mayor información posible para que el equipo priorice las actividades posteriores y pueda fluir la debida gestión de la mejor forma posible. Entre mejor y más detallado sea el análisis, más insumos se tendrán para superarlo y minimizar los impactos que

pueda generar. Se brindan una serie de recomendaciones para que el análisis de incidentes sea más fácil y efectivo, como perfiles base de redes y sistemas, correlacionadores de eventos, retención de logs, entre otros. Todas las acciones y cada paso que se tomen desde la detección hasta la solución final deben documentarse debidamente y con el mayor detalle posible.

El componente de análisis también incluye la priorización de los incidentes, ya que deben ser diferenciados según el impacto que puedan causar en la operación de los sistemas afectados o a mayor nivel, la continuidad del negocio de la organización, así como su reputación. En relación con esto, en esta fase, la guía de NIST presenta una serie de tablas con ejemplos de categorías de impacto que una organización podría utilizar.

Finalmente, luego del análisis y priorización del incidente, el equipo de respuesta deberá notificar a las partes interesadas adecuadas para que todos los involucrados desempeñen sus funciones adecuadamente, como mínimo se debe establecer qué se debe informar, a quién y en qué momento, así como el método de comunicación apropiado según se requiera.

Detección y reporte ISO 27035:

Esta fase plantea una serie de actividades clave que se relacionan con la recolección de información relacionada con el incidente y obtener la mayor cantidad de información que permita entregar un adecuado y ágil reporte al área encargada de la evaluación del incidente de seguridad.

La detección y reporte de una posible ocurrencia de un evento de seguridad de la información puede darse por medio del personal involucrado en los procesos de la organización, clientes o por las partes interesadas en general, también pueden darse de forma automática con la ayuda de sistemas de seguimiento como los sistemas de prevención de intrusos, sistemas de detección de intrusos, programas antivirus, programas antimalware, entre otros. En todos los casos, debe existir un procedimiento o canal por el cual se realiza el reporte y lo recibe el área encargada de su tratamiento. ISO 27035 plantea que este reporte sea por medio de un formulario físico o digital que permita incluir la mayor cantidad de información relacionada con el incidente, para los medios automáticos como los sistemas de detección de intrusos, se recomiendan otros medios como

correo electrónico o plataformas que reporten directamente al personal responsable de su tratamiento.

Una vez existe un reporte de un posible evento de seguridad, independientemente del medio por el que se haya recibido, se inicia un proceso de recolección de información por parte del grupo de personas del punto de contacto que son los encargados de recolectar la mayor cantidad de información relacionada con el evento de seguridad y que posteriormente aporte significativamente al proceso de evaluación de este. La recolección adecuada de la información debe contemplar todas las actividades, resultados y decisiones en relación con el reporte, así como el aseguramiento de la evidencia si es el caso.

Evaluación y decisión ISO 27035:

Se contempla actividades clave como la clasificación de los incidentes y las recomendaciones que permiten al equipo de trabajo poder decidir adecuadamente cuando se trata de un incidente y cuando no, plantea una serie de recomendaciones clave para que el diagnóstico de un incidente sea lo más preciso posible y que a su vez, se pueda lograr dimensionar las posibles consecuencias de dicho evento si se llegara a materializar completamente, dando esto, la herramienta principal para definir o clasificar un incidente de seguridad de la información de acuerdo a los efectos que éste pueda causar, siendo así una clasificación por los efectos que pueda causar el incidente de seguridad. La tipificación del incidente define si es un posible incidente, si es un incidente concluido o si es un falso incidente, lo cual es determinante durante el proceso de evaluación y para continuar según corresponda de acuerdo con el tipo de incidente. Es en este punto donde se debe acordar una escala de clasificación para los incidentes de seguridad y así poderlos categorizar de acuerdo con el impacto que éstos pueden tener en la organización, también se plantea una caracterización de los incidentes de seguridad considerando las amenazas como factores de categorización como lo son incidentes por desastre natural, incidente por disturbios sociales, entre otros.

Teniendo la tipificación del incidente de seguridad como incidente posible o concluido, una categorización de la amenaza y una clasificación por el impacto que el evento pueda tener, se deben tomar decisiones acerca de cómo se debería tratar el incidente de seguridad confirmado, por quién y con qué prioridad. En este punto se deben tener en cuenta la distribución de las responsabilidades, a través de la jerarquía del personal adecuado en las acciones y toma de

decisiones, así como contar con los procedimientos adecuados que debe seguir cada persona en esta parte del proceso.

El punto de contacto (PoC) como le llama ISO 27035 al grupo de profesionales encargados de la gestión primaria de incidentes de seguridad, será el responsable de la evaluación y decisión inicial respecto al tipo de incidente que se les ha reportado; como primer paso, éste grupo debe dar acuse de recibido al reporte del incidente para luego iniciar su proceso de gestión básico, el cual inicia con la evaluación del incidente que debe ser sometido a ciertos criterios para definirlo como incidente y determinar su posible impacto. El grupo o punto de contacto también se encarga de la documentación de lo hallado para facilitar y agilizar el proceso de gestión por parte del grupo de especialistas de seguridad que dará respuesta o tratamiento si es el caso.

Siendo así, el grupo de respuesta a incidentes de seguridad recibe por escalamiento el incidente de seguridad que se reportó y que el punto de contacto ha evaluado y clasificado. Este grupo de respuesta acusa recibido del reporte al área de punto de contacto e inicia las acciones correspondientes respecto a recolección de información que sea útil para dar respuesta al incidente y que permita priorizar en orden que se puedan reducir o evitar las consecuencias en su máxima capacidad, posterior a estas acciones de recolección de información y priorización del incidente, como quién lo originó, cómo se originó, qué afecta o puede afectar, su impacto real o potencial en la organización, vendrán las acciones de respuesta, aquellas que están definidas en la siguiente fase de la guía ISO 27035.

De la comparación de las fases anteriores, se toman algunos aspectos importantes de cada una de las guías, aspectos que van en consecuencia y relacionamiento con el modelo de gestión de incidentes que, aunque no es tan teórico y debe ser más ágil, la comparación de estas fases brinda algunas características importantes que deberán ser tenidas en cuenta para la segunda fase de nuestro modelo, como, por ejemplo:

- Los precursores como posibilidad de evitar la materialización de incidentes o de poder tomar decisiones en tiempos que permitan reducir los impactos que pueda ocasionar un incidente de seguridad

- Detección y reporte de forma automática como herramienta fundamental para mejorar los tiempos de evaluación y decisión relacionados al incidente.
- Recolección de información en forma precisa y óptima que permita agregar valor al reporte automático al relacionarlo con criterios de clasificación y priorización desde la concepción de las reglas de SNORT.
- Establecer claridad y un flujo ágil de los procesos de tipificación, categorización, clasificación, priorización y severidad de los incidentes de seguridad para optimizar los tiempos de esta fase y aprovechar completamente el comportamiento predictivo del modelo.

Figura 3-25: Etapa 3 Contención, erradicación y recuperación de NIST SP800-61 y la fase de respuestas de ISO 27035 [5], [42]

Se establece una comparación entre las fases (figura 3-25) donde se resaltan las siguientes características de cada una:

Contención, erradicación y recuperación NIST SP800-61

Se plantea de forma muy general una serie de recomendaciones para definir una estrategia de contención que permita dar respuesta adecuada a los incidentes de seguridad que se presenten. Es importante que el equipo de respuesta a incidentes tenga preparación y claridad respecto a las decisiones que debe tomar en el proceso de contención y erradicación de un incidente de seguridad, cómo por ejemplo apagar el sistema, desconectar algún activo de la red, desactivar funciones, entre otras. Estas decisiones son más fáciles de tomar si existen previamente como una estrategia de contención y erradicación, basada en el comportamiento o tipo de incidente y en qué tiene más impacto, si apagar el sistema o dejar que el incidente continúe y también en relación con la recuperación, la cual es de vital importancia en estas decisiones de contención y erradicación. Aunque la prioridad durante un incidente de seguridad es la contención, erradicación y recuperación del sistema, también es importante recolectar evidencia que permita estudiar y

conocer el ataque para llevarlo a la base de datos de conocimiento y estar preparado para futuros incidentes similares, además de poder llevar a instancias judiciales las evidencias recolectadas si es el caso (NIST SP800-86 que brinda técnicas de integración forense en la respuesta a incidentes de seguridad).

Posterior a la contención, vienen actividades de erradicación y recuperación, las cuales comprenden procedimientos para eliminar componentes del incidente como Malware, cuentas de usuarios y cualquier procedimiento ilícito que se haya realizado durante el evento, así como la corrección de las vulnerabilidades que fueron explotadas si es el caso, de lo contrario, considerar las recomendaciones o acciones posteriores correspondientes para evitar eventos similares relacionados con las vulnerabilidades ya identificadas.

Luego de la respectiva erradicación, el proceso de recuperación comprende retornar los sistemas a su estado de operación normal y puede involucrar procesos de restauración de sistemas, reemplazo de archivos comprometidos, restauración de copias de seguridad, instalación de parches, cambio de contraseñas, entre otros. Este proceso puede tomar bastante tiempo dependiendo del nivel de compromiso y el daño causado por el evento de seguridad. El principal objetivo del equipo de respuesta a incidentes es poder lograr la recuperación de la operatividad normal de los sistemas en el menor tiempo que sea posible.

Respuestas ISO 27035

La fase de respuestas de ISO 27035 contempla de manera similar a la fase anterior, una serie de actividades clave que brindan una guía y recomendaciones para dar respuesta adecuada a los incidentes de seguridad de la información según lo que se haya determinado en la fase anterior en relación a la criticidad, prioridad e impacto que pueda causar el incidente, ya que dependiendo de esto, será crucial saber qué tipo de acciones y respuestas se deberán llevar a cabo para evitar, erradicar o superar el incidente con el menor impacto posible a los sistemas, operación o continuidad del negocio de la organización.

Las fases anteriores son fases que intervienen en el modelo o guías de gestión de incidentes de seguridad en la forma en que se da tratamiento, gestión o respuesta a un incidente de seguridad que ha ocurrido, está ocurriendo o ya ocurrió. En este orden, son útiles las fases anteriormente descritas, ya que se requiere de forma imprescindible la presencia de un incidente de seguridad de la información.

Este trabajo plantea un modelo de gestión de incidentes de seguridad que se basa en un componente predictivo, esto contempla que un incidente de seguridad de la información pueda o no tener consecuencias, es así entonces que contemplar actividades relacionadas con la respuesta a incidentes, sería parcialmente efectivo en el modelo y es determinante limitarlo hasta el punto donde se requiera notificar la posibilidad de materialización de un incidente a un equipo de respuestas, que esté ya definido o se pueda definir para el adecuado tratamiento del incidente de seguridad.

Este modelo de gestión de incidentes de seguridad contempla dicha gestión hasta el punto donde la predicción aún es efectiva y rinde sentido hasta la evaluación y clasificación de un incidente de acuerdo con su posible impacto luego de su posible ocurrencia, es indispensable en este modelo, definir y clasificar por prioridad e impacto de los eventos que se detecten, se notifiquen como predicciones del filtro Kalman y que un equipo de gestión a incidentes con sus acciones de respuesta puedan gestionar adecuadamente la materialización de dichos eventos.

De acuerdo con lo anterior, estas fases no se tomarán recomendaciones o mejores prácticas para el modelo, ya que las acciones de contención, erradicación y recuperación no serán componentes activos para la gestión de incidentes de seguridad basado en predicciones del filtro Kalman, por considerar que la predicción de un incidente de seguridad no implica la materialización de este. Sin embargo, se tendrán en cuenta algunos aspectos relacionados que pueden servir de insumo o elementos clave para un equipo de respuesta a incidentes, que sea ajeno a este modelo y pueda tener información que permita desplegar rápidamente acciones de respuesta ante un incidente de seguridad de la información en curso.

Finalmente, se realiza una comparación entre la fase acciones post incidente de NIST SP800-61 y la fase lecciones aprendidas de ISO 27035 (figura 3-26) donde se destacan los siguientes aspectos

Figura 3-26: Etapa 4 post incidente de NIST SP800-61 y lecciones aprendidas de ISO 27035 [5], [42]

Fase acciones post incidente NIST SP800-61

Propone que las partes interesadas deben llevar a cabo reuniones de lecciones aprendidas donde se realice el cierre del incidente presentado o los que se hayan presentado entre una reunión y otra y así revisar lo que ha ocurrido, lo que se realizó para intervenir y qué tan efectivas fueron las acciones tomadas. Principalmente se deberán abordar temas como exactamente qué sucedió y en qué momentos, que tan bien se desempeñó el personal durante el proceso de respuesta, cómo fueron abordados los procedimientos y si fueron adecuados, hubo acciones que afectaron o pudieron afectar la recuperación, entre otras. Son algunas de las preguntas que deben ser planteadas en estos espacios para poder determinar qué se puede mejorar y registrarlo como lecciones aprendidas.

Los resultados de estos espacios son importantes para capacitar a nuevos miembros del equipo de cómo los integrantes más experimentados del equipo responden ante los incidentes presentados. Otra parte importante de las lecciones aprendidas es que pueden servir como insumo para actualizar las políticas y procedimientos en relación con la respuesta de incidentes en relación con la seguridad informática.

El proceso de lecciones aprendidas debe ser frecuente y constante debido a la naturaleza cambiante de la tecnología y los cambios en el personal, lo que hace que esta fase sea de vital importancia para mantener actualizadas las demás fases y procedimientos en relación con el

proceso integral de gestión de incidentes de seguridad y de los procesos paralelos que tengan relación directa o indirecta con la seguridad de la información. Adicionalmente, se contempla también una serie de factores que pueden ser considerados para adoptar una política de retención de evidencia de los incidentes de seguridad que permitan tomar acciones legales.

Finalmente, en esta fase de NIST SP800-61 se especifica una lista de verificación del manejo de incidentes, el cual está enfocada en proporcionar los principales pasos a realizar en una respuesta a incidentes y proporcionar a los equipos de respuesta a incidentes una posible ruta a seguir durante las acciones de respuesta, aunque no siempre sea aplicable por completo dada la naturaleza o tipo de incidente que se esté gestionando, pero si es de importancia en la etapa de lecciones aprendidas para mejorar los procedimientos y capacitar al equipo de respuestas.

Fase lecciones aprendidas ISO 27035

Esta es la última fase de esta guía y se lleva a cabo cuando los incidentes de seguridad de la información se han solucionado o cerrado, es por eso se contempla una serie de actividades principales como: análisis forense de ser requerido, revisión general de mejoras para implementación de controles nuevos o actualizar los existentes al igual que la política de gestión de incidentes.

Se revisa la eficacia de los procesos y procedimientos para mejorar el esquema de gestión de incidentes de forma tal que permita responder mejor en la evaluación y recuperación de cada incidente, conduciendo así a reducir los impactos que pueda generar un incidente de seguridad. También es importante considerar instrucciones o refuerzo en planes de capacitación y de toma de conciencia hacia las partes interesadas y fortalecimiento de directrices o normas. Los controles que resulten de esta fase deberán ser implementados lo antes posible y aquellos que por diferentes razones deban ser aplazados, deberán seguir siendo considerados como necesarios para mejorar el proceso de gestión de incidentes de seguridad de la información.

Dada la comparación de las fases de acciones post incidente de NIST SP800-61 y lecciones aprendidas de ISO 27035, se consideran algunos aspectos importantes en relación con el mejoramiento del proceso de gestión de incidentes respecto al valor y alcance *predictivo* del modelo propuesto. Las acciones de mejoramiento estarán enfocadas en lograr optimizar el proceso

en las fases que interviene el modelo y no en las mejoras que surgen luego del cierre o solución de incidentes de seguridad, dado que no se contempla fase de contención, erradicación, recuperación, respuesta o similar en el alcance del presente modelo como se indica al principio de este punto.

- Controles de mejoramiento o construcción de reglas de SNORT que permitan mejorar la detección de nuevos incidentes de seguridad dado el análisis e investigación preventivo que realice el equipo de seguridad.

Las etapas post-indicentes y lecciones aprendidas se pueden potencializar en el modelo predictivo, dado que, una vez se genere la alerta de un posible evento de seguridad a través del filtro Kalman, es necesario tomar diferentes acciones y realizar validaciones en los sistemas, con el objetivo de establecer posibles impactos si el incidente se consolida, buscar posibles vulnerabilidades y establecer los planes de remediciones, catalogar cómo, cuándo y dónde puede suceder el ataque o la eventualidad, con ello, hacer una reducción de la probabilidad de ocurrencia y los niveles de impacto, ejecutando acciones que logren identificar el problema y erradicar si es del caso.

3.3.2. Relacionar la estructura de procesos y operación de una red industrial SCADA

En la actualidad, la gestión de procesos en las compañías ha cobrado una importancia significativa en el afán de tener mejores servicios o productos, creando así la necesidad de que los procesos y procedimientos en las empresas sean intervenidos para que cada vez sean mejores. El mejoramiento o las acciones en beneficio sólo se pueden realizar si se tiene un control sobre los procesos, pero para llegar a este punto es necesario poder tener conocimiento y medición de lo que pasa en ellos.

Lo anterior se puede interpretar bajo la necesidad de medir los procesos, de tener los indicadores adecuados y específicos que puedan brindar los insumos para su control. Una vez existe control o gobierno de los procesos se pueden tomar acciones para intervenirlos y mejorarlos. Es en esta medida que las empresas pueden tener diferentes estructuras de procesos aún si su core de

negocio es similar, porque está direccionado a que la diferencia sea en los procesos que se lleven a cabo.

De acuerdo con lo anterior, es importante aclarar que para una empresa cuya operación esté basada o utilice redes industriales SCADA para proveer servicios o productos, ésta puede contar con estructuras de procesos diferentes a otra empresa que también tenga redes industriales SCADA como su núcleo de operaciones. Esto nos lleva a proponer un relacionamiento general y de alto nivel entre la estructura de procesos y la operación de una red industrial SCADA.

Se relaciona inicialmente una estructura organizacional general en la cual se identificarán tres focos principales para diferenciar su propósito en relación con los procesos de la organización y así segmentarlos claramente con base a su relación con la operación, que para este caso es enfocada en el sector eléctrico. Los focos o segmentos principales en los cuales se divide la estructura propuesta son direccionamiento, núcleo de negocio y soporte.

- Direccionamiento: Este segmento enmarca todos aquellos roles y responsabilidades relacionados con el direccionamiento estratégico del negocio en general, es decir, se relacionarán todos aquellos roles que sean los encargados de direccionar el futuro del negocio en el mercado, roles en relación con el entorno y relacionamiento empresarial, de comportamiento de mercado a un nivel de planeación estratégica y continuidad de negocio.

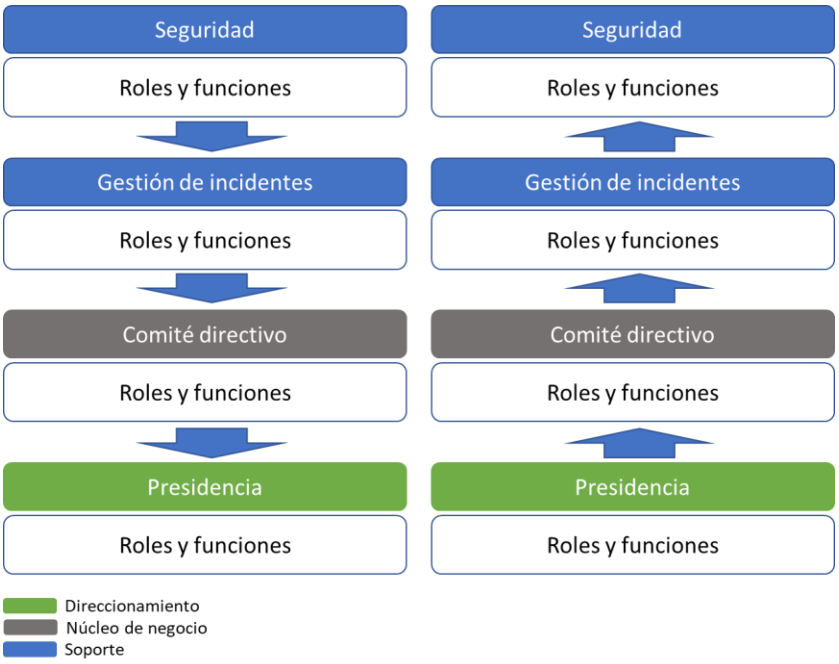
- Núcleo de negocio: En este nivel de la estructura organizacional se concentran aquellos roles que están en función de mantener la continuidad del negocio, que tienen como insumo el servicio o producto de la organización para impulsar su crecimiento y mantener su estabilidad comercial y financiera, es todo aquel rol que está relacionado con hacer del servicio o producto su insumo o materia prima para trabajar y dar valor a la organización, se enmarcan todos aquellos aspectos de planeación y programación de la operación, así como los relacionados con el área financiera, comercial, de mercadeo y ventas de la organización.

- Soporte: El segmento de soporte dentro de la estructura organizacional corresponde a aquellos roles que tienen relación con soportar la base de la operación, aquellos encargados de que lo fundamental funcione para permitir al negocio su operación y continuidad, consiste en las unidades de apoyo que son fundamentales para que los servicios o productos estén disponibles para que el resto de la organización pueda cumplir con sus procesos, en este orden podemos considerar aquellos roles de talento humano, auditorías internas, gestión de servicios, logística y tecnología por mencionar algunas.

Una vez se han descrito estos segmentos de la estructura organizacional, los cuales son importantes y necesarios dentro de cualquier organización, se realiza profundidad en los roles de tecnología asociados al segmento de soporte, el cual nos permitirá centrarnos en el propósito de relacionar la estructura de procesos con la operación de una red industrial SCADA, ya que ésta hace parte de las unidades de apoyo que soportan la operación del negocio.

A continuación, en la figura 3-27, se realiza una representación gráfica de la estructura organizacional de procesos que permite identificar fácilmente la descripción general de la estructura que se propone, teniendo en cuenta que el flujo de procesos en el organigrama puede invertirse en casos especiales, que desde los roles de direccionamiento se presenten indicaciones que requieran llevarse al nivel de soporte.

Figura 3-27: Flujo de proceso organizacional. Fuente autores.



De acuerdo con el diagrama anterior, la dirección de tecnología estará en relación directa con la operación de la red industrial SCADA en cuanto al soporte y gestión de su operación tecnológica y de seguridad informática, por lo que en este punto se hace enfoque específicamente en el relacionamiento del área de tecnología con la operación y seguridad de la red SCADA. Aunque puede existir relacionamiento directo o indirecto entre la operación del sistema SCADA y otras unidades organizativas, no serán del alcance de este relacionamiento que va en función de la gestión de incidentes de seguridad informática en redes industriales SCADA.

El área de tecnología de la organización es la encargada de velar por la normal operación y gestión correspondiente a la disponibilidad de la red SCADA garantizando los recursos adecuados y requeridos para este propósito, incluyendo personal de redes, infraestructura y seguridad informática, como todos aquellos recursos que se consideren necesarios para mantener los niveles de servicio. Así mismo deberá mantener canales de comunicación sólidos, estables y permanentes con otras áreas de dirección del nivel de núcleo o incluso hasta de direccionamiento (si se considera necesario), esta comunicación puede centralizarse conformando un comité directivo para temas especiales que impliquen tomar decisiones importantes sobre la operación de la red industrial que

repercutan en la continuidad del negocio o que su impacto afecte la normal operación de la organización.

Este relacionamiento es relevante ante situaciones de eventos de seguridad o aquellos que afecten de forma general la operación de la red, la producción o servicio hasta la continuidad del negocio. El personal involucrado en el proceso de manipulación, lectura, supervisión o cualquier actividad que contemple interacción con la red industrial deberá tener claridad sobre los procedimientos que debe llevar acabo para reportar o gestionar eventos sobre la red SCADA y a su vez deberán estar contemplados como un canal por el cual se reciben reportes de incidentes físicos y que son complementarios al sistema de detección automático propuesto en este proyecto.

Es así como la detección de incidentes puede darse tanto por el personal que interactúa con la red industrial SCADA como por el sistema de detección de intrusos y su posterior reporte al personal correspondiente por medios electrónicos. La principal diferencia es que los reportes realizados por el personal deberán seguir un procedimiento que excede los alcances de este proyecto y que además relacionan eventos de tipo físico, mientras que los reportes de posibles eventos lógicos sobre la red, los realizará el proyecto propuesto del modelo de gestión de incidentes de seguridad basado en la predicción que relacionan directamente eventos de tipo lógico y cibernético sobre la red.

La importancia de que existan diferentes modos de detectar o recibir notificaciones de alerta sobre posibles eventos o incidentes sobre la red industrial SCADA, permitirá al equipo de Tecnología determinar la idoneidad del personal para tratar los eventos según el tipo, es decir, eventos de tipo físico o mecánico sobre la red industrial deberán ser gestionados por un grupo diferente al que gestiona los eventos de seguridad informática, que incluso de ser el caso, puede ser un grupo no dependiente estructuralmente del área de tecnología sino de operaciones por ejemplo. En cualquier caso, ambos deben tener constante comunicación para garantizar la estabilidad y disponibilidad de los servicios y la continuidad del negocio.

3.3.3. Creación del nuevo modelo para el manejo de incidentes de seguridad

El modelo para el manejo de incidentes de seguridad contempla un componente activo en su etapa inicial. Su fase de detección y registro incorpora un sistema de detección de intrusiones y un algoritmo de predicción que agrega valor a la detección de incidentes, ya que éste puede arrojar una estimación cada segundo de lo que puede suceder en relación con el incidente en términos de intensidad y tiempo, es decir, si el ataque continúa en las condiciones iniciales, en un mediano plazo se podría esperar una situación. Si el ataque varía en intensidad, la estimación de la situación varía en relación con el tiempo, es decir, si la intensidad aumenta considerablemente, la situación de posible materialización o impacto será en un corto plazo.

La salida del filtro Kalman arrojará una alerta sobre lo que se ha detectado y corresponderá adicionalmente al modelo de gestión de incidentes de seguridad en redes industriales SCADA, proporcionar orientación sobre cómo abordar las predicciones realizadas por el algoritmo del filtro Kalman y así, poder aprovechar este componente predictivo y contribuir en la reducción de los impactos generados que puedan generar la materialización de un incidente de seguridad en la operación de la red industrial SCADA.

El objetivo principal de este modelo para el manejo de incidentes de seguridad basado en la predicción de posibles incidentes que afecten o interrumpan la operación de una red SCADA es detectar, registrar, predecir, clasificar y reportar las alertas detectadas por el sistema activo sobre una posible intrusión, incidente o afectación sobre la red SCADA y proporcionar las recomendaciones necesarias para la gestión del incidente hasta donde corresponda su alcance. Esto permitirá minimizar el impacto que pueda generar la materialización de un incidente en la operación de la red SCADA.

El modelo de gestión de incidentes descrito aplica para los eventos que se detecten de forma automática por el sistema de prevención de intrusos y que luego del análisis realizado por el filtro de predicción, se clasifiquen como potenciales incidentes de seguridad que interrumpan o puedan interrumpir el servicio u operación de la red industrial SCADA

A continuación, se relaciona de forma general las fases del modelo para la gestión de incidentes de seguridad en redes industriales SCADA a través del algoritmo de predicción filtro Kalman (tabla 3-5).

Tabla 3-5 Fases del modelo para la gestión de incidentes

Fase 1: Preparación	Fase 2: Detección, análisis y reporte	Fase 3: Gestión de reportes	Fase 4: Lecciones aprendidas y mejoramiento
-Actividades clave de configuración de plataforma. -Criterios de admisión filtro Kalman y equivalencia de categorías IDS. -Actividades clave para la gestión de reportes. -Información de contactos para escalamientos. -Escalamientos funcionales y jerárquicos	-Detección automática con herramienta IDS -Almacenado de eventos en base de datos -Identificación de incidentes por categoría de IDS y equivalencia de entrada al filtro Kalman. -Predicción con filtro Kalman. -Reporte de eventos en tiempo real al grupo de gestión de incidentes.	-Categorización del incidente. -Prioridad de incidentes basada en impacto y urgencia. -Diagnóstico inicial y eficiencia en la gestión de reportes por medio de OODA. -Escalamiento a grupo de respuesta a incidentes de seguridad.	-Ajuste a los procesos de observación, orientación, decisión y acción (OODA) -Actualización de reglas SNORT -Ajustar niveles de criticidad del modelo. -Gestión de las notificaciones -Capacitación del equipo de gestión de incidentes. -Actualización de la base de contenido

Fase 1: Preparación

La fase contiene todas aquellas acciones relacionadas con la preparación de los sistemas, equipos de trabajo y procedimientos que intervendrán en la gestión de los incidentes. Esta fase es fundamental para el adecuado funcionamiento del modelo y la gestión de los incidentes de seguridad, ya que los lineamientos que se determinen impactarán de forma directa el funcionamiento del modelo en su totalidad.

La adecuada configuración de las reglas del sistema de prevención de intrusos es parte fundamental de la preparación del sistema, ya que es necesario contar con las reglas suficientes y actualizadas que permitan realizar una adecuada identificación de intrusiones. La configuración y actualización de estas reglas está en relación con las vulnerabilidades conocidas del sistema, es decir, las vulnerabilidades que se tengan identificadas en la red SCADA; estas deberán ser tenidas en cuenta para configurar reglas en el sistema que permitan identificar ataques que puedan explotar esas vulnerabilidades a las que está expuesta la red SCADA.

Una vez el sistema de detección de intrusos está configurado para detectar las intrusiones, es necesario realizar una equivalencia de las categorías de reglas del IDS con los criterios de admisión del filtro Kalman, que para el alcance de este proyecto se definieron: DoS, lectura y escritura.

El tipo de entrada “DoS” serán aquellos ataques relacionados con la observación o inspección de los servicios, la entrada “Lectura” está relacionada con aquellos eventos que comprendan lectura de datos del sistema y la entrada de “Escritura”, será en su proporción la más crítica dado que busca sobrescribir datos del sistema SCADA comprometiendo su integridad.

Corresponderá al equipo de seguridad informática de la organización o de quien haga sus veces, realizar la equivalencia de las reglas del sistema de detección de intrusos con cada una de estas tres definiciones de entrada de datos del filtro, es decir, se debe establecer qué reglas o grupo de reglas corresponden a cada uno de los modos de entrada del filtro Kalman. Una vez se tienen los sistemas preparados y configurados para su adecuado funcionamiento, es necesario precisar a quién se debe notificar y qué hacer una vez se obtiene una alarma del sistema predictivo. La

información de los contactos a notificar deberá estar fácilmente visible y al alcance del personal que reciba la alarma del sistema o que esté realizando el constante monitoreo del sistema.

Dependerá del tipo de alerta a quién se notifica inicialmente. A continuación, se relacionan los posibles contactos y partes interesadas que pueden participar en la notificación inicial de la detección del sistema. El orden no es necesariamente como se expresa, ya que es posible que se notifique en orden diferente dependiendo del tipo de detección y el posible impacto que éste pueda llegar a generar a la operación del sistema. Se puede dar una notificación secuencial y/o paralela a los siguientes contactos:

Tabla 3-6 Principales contactos a informar la detección de un posible incidente

Contacto	Correo electrónico	Teléfono fijo o extensión	Teléfono móvil (WhatsApp, Telegram, otros)	Observación
Equipo técnico de respuesta a incidentes				
Gestor de seguridad informática				
Gestor de operaciones del sistema SCADA				
Jefe de seguridad informática				
Gerente de TI				

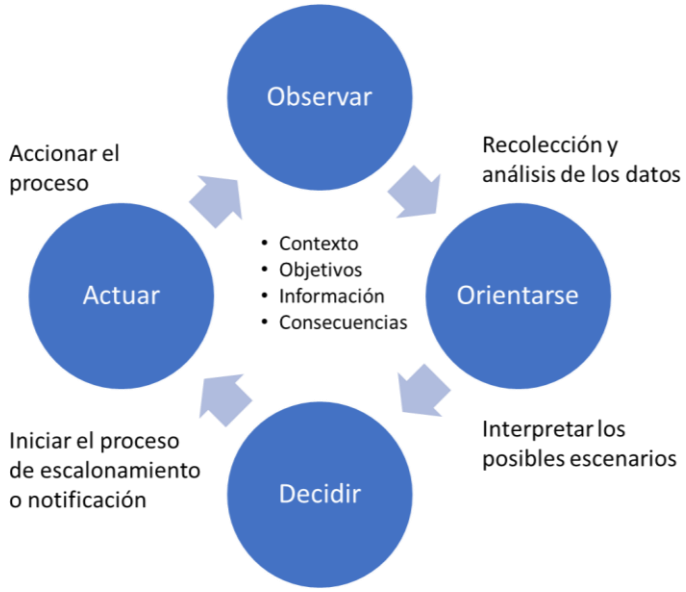
Esta información permite igualmente basar los escalamientos, que pueden ser funcionales o jerárquicos, facilitando y orientando el flujo de los procedimientos según sea requerido. El escalamiento funcional está relacionado con aquellas notificaciones o requerimientos de apoyo que se realizan a las partes interesadas para solicitar ayuda en algún procedimiento relacionado

con la gestión de incidentes. El principal objetivo del escalamiento funcional es poder contar con el apoyo de expertos o personal con mayor conocimiento para lograr reducir los impactos que pueda generar un incidente.

El escalamiento jerárquico contempla aquellas notificaciones o comunicados que se realizan a los roles con perfil directivo y estratégico en la organización que siempre deben estar enterados de las situaciones o eventos que están ocurriendo. Normalmente este tipo de escalamiento se realiza para situaciones de alto impacto o criticidad mayor, que involucren afectación de la continuidad del negocio o hasta por situaciones de reputación que deben ser tratados adecuadamente por quienes están mejor preparados para ello. También busca informar o notificar a superiores de las situaciones que ocurren o pueden ocurrir de cara a la afectación del servicio o continuidad del negocio, pero nunca buscando un apoyo técnico, una gestión de procesos o procedimientos relacionados para este caso con la gestión de incidentes de seguridad.

El grupo de trabajo que reciba las notificaciones del filtro Kalman deberá tener claridad de los escalamientos que se deben contemplar según el evento que se esté reportando. Igualmente, este equipo deberá estar lo suficientemente preparado para tomar la mejor decisión respecto al evento observado, para estos casos, se recomienda el uso del método OODA, que consiste en Observar, Orientarse, Decidir y Actuar, lo cual le permitirá a la persona observar el reporte y rápidamente analizarlo para orientarse sobre lo que puede llegar a presentarse con ese evento que está gestionando, posteriormente debe tomar una decisión que vaya en consecuencia del mejor escalamiento o notificación que corresponda a dicho evento, y finalmente actuar, poner en marcha el escalamiento indicado para el caso que ha determinado [43] como se puede observar en la figura 3-28.

Figura 3-28: Método OODA [44]



El equipo de respuesta a incidentes normalmente es quien recibe estas notificaciones o escalamientos, también existe la posibilidad de que sea el mismo equipo de seguridad o de respuesta a incidentes quienes reciban las alertas del filtro y realicen el procedimiento OODA, generando así mayor agilidad en la gestión del incidente y permitiendo una mejor armonía del modelo.

Este grupo de respuesta a incidentes, como se ha mencionado antes, no se contempla en el alcance de este proyecto, ya que existe la posibilidad de que los eventos recibidos puedan no llegar a convertirse en un incidente de seguridad que afecte la operación de la red industrial SCADA, haciendo así parcial su funcionalidad, es por esto que el modelo presentado llega hasta la notificación al área encargada de diagnosticar detalladamente el reporte y darle continuidad como incidente de seguridad y seguir los procedimientos que tenga ya definidos la organización o si determina que el reporte no es un incidente y se gestiona como una posibilidad de mejoramiento o de identificación de posibles correcciones al sistema a nivel de seguridad.

La recomendación para las organizaciones y el grupo de gestión de incidentes es contemplar la adopción o inclusión de políticas de gestión de incidentes que vayan en consecuencia con su estructura organizacional, los procesos relacionados a la seguridad y operación de la red SCADA,

esto permitirá tener claridad, alcance y gobierno de los procesos involucrados en la gestión de incidentes. También se debe contemplar la integración de estas políticas con otras políticas que se consideren en relación, por ejemplo, las políticas de crisis, continuidad de negocio o recuperación de desastres, las cuales deben estar relacionadas para lograr alineación de las estrategias del área de tecnología con las del negocio en general.

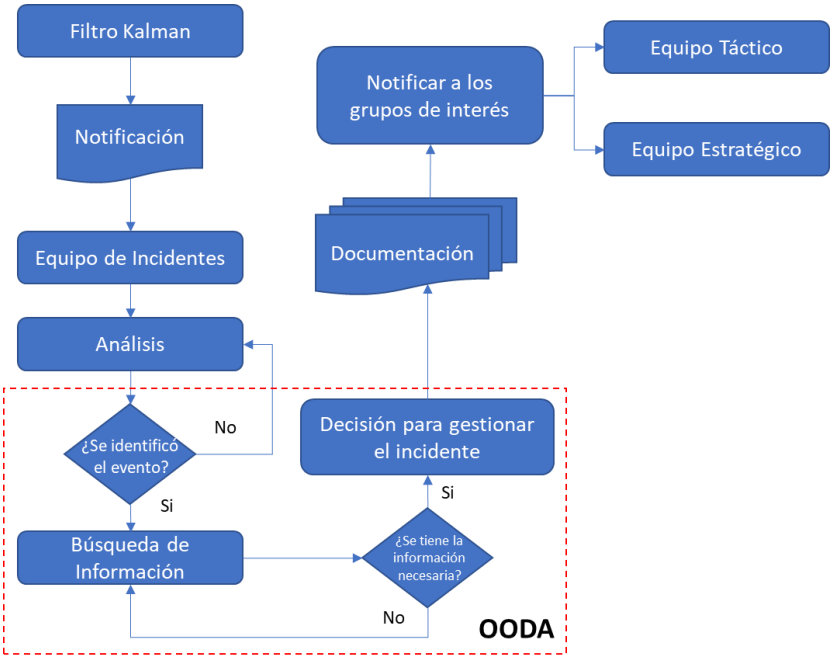
La organización y el área de tecnología deben procurar mantener una constante preparación y capacitación para el personal que interviene en los procesos de gestión de incidentes, así como contar con unos adecuados planes de capacitación para los nuevos integrantes. Debe existir una estrategia clara y precisa para garantizar una gestión del conocimiento adecuada entre los integrantes del equipo de gestión y respuesta a incidentes.

Los procedimientos clave para una adecuada preparación para la gestión de incidentes de seguridad desde el momento en que se observa la alarma del filtro Kalman hasta que se reporta o escala el evento van en concordancia con el método OODA y que pueden ser los siguientes:

- Una vez se presenta la alarma que reporta el filtro Kalman se debe realizar una interpretación adecuada de acuerdo con lo observado en el reporte e identificar lo que se está presentando. Es fundamental que el personal que recibe la alarma tenga plena capacidad y conocimiento de entender o interpretar lo que arroja el filtro.
- Cuando sea clara la situación que se presenta, se requiere orientación para asociar la mayor cantidad de información de criticidad o impacto que se pueda generar si el evento se llega a presentar, lo que proporcionará al personal una idea del paso que se debe seguir. Esto se logra teniendo en cuenta el tipo de evento que se presente de acuerdo con la salida del filtro Kalman.
- Posteriormente es necesario tomar una decisión rápida respecto al qué hacer y tener la seguridad de que es la mejor forma de continuar con el proceso de gestión del incidente.
- Finalmente se ejecutan las acciones correspondientes. Se identifica en el nivel de escalamiento quien o quienes deben conocer la situación, es decir, si aplica escalamiento jerárquico o solamente escalamiento funcional para la gestión del evento y las acciones de documentación, diligenciamiento de formatos y demás que sean necesarios según el

esquema estructural que tenga la organización y si el equipo que recibe las alertas es el mismo equipo encargado de dar respuesta a los incidentes de seguridad (figura 3-29).

Figura 3-29: Procedimientos clave para la gestión de incidentes de seguridad. Fuente autores.



Estos anteriores, se consideran los procedimientos clave de preparación para un adecuado esquema de atención inicial de las predicciones del filtro Kalman que podrán ser posibles incidentes de seguridad. La agilidad y eficiencia es de vital importancia en este punto del ciclo de vida del modelo, ya que se debe aprovechar al máximo el componente predictivo y así poderse anticipar a un posible incidente o en otros casos más complejos, reducir los impactos que pueda generar su materialización.

Fase 2: Detección, análisis y reporte

La fase de detección, análisis y reporte abarca el principio de la funcionalidad operativa del modelo de gestión de incidentes por sus componentes tecnológicos de IDS, base de datos y modelo matemático para el filtro Kalman. Estos componentes permiten la posibilidad de tener precursores

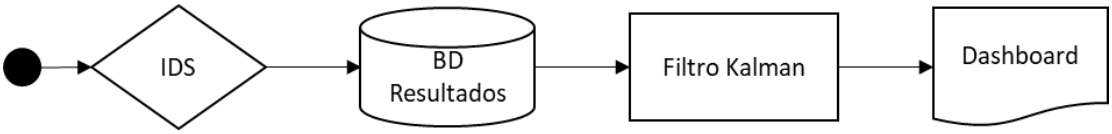
para reducir la materialización de incidentes de seguridad o poder tomar decisiones que puedan contribuir positivamente en la reducción de los impactos que pueda ocasionar un incidente.
La detección, análisis y reporte de forma automática como herramienta fundamental para mejorar los tiempos de decisión y acciones relacionados al incidente son de gran importancia en esta fase del modelo ya que permiten tener una gran agilidad y además tener un componente de predicción, que permite aún más la reducción de posibles materializaciones de incidentes o de los impactos que éstos puedan generar.

La optimización y puesta a punto de los componentes tecnológicos del modelo son sumamente importantes ya que de éstos depende la calidad y objetividad del reporte y su predicción. Es fundamental comprender el flujo del proceso de esta fase que consta básicamente de los siguiente:

- La detección con el IDS permite tener una coincidencia de un ataque con una o varias reglas del sistema, la entrada al IDS es tráfico de red que se procesa y analiza, la salida es una alerta de seguridad.
- La salida del IDS es la alerta de seguridad que se almacena en una base de datos como repositorio de todos los eventos detectados por el IDS, esta base de datos es el insumo para el filtro Kalman.
- El filtro Kalman toma las variables que necesita de la base de datos, según la categoría del evento registrado por el IDS se establece la relación con el criterio de admisión (DoS, lectura o escritura) y se ejecuta el modelo matemático para las variables tomadas y se obtiene la predicción que realiza el filtro.
- La predicción realizada por el filtro se muestra en un dashboard que podrá observar el equipo de gestión de incidentes o quien haga las veces de receptor de los reportes automáticos del sistema.

A continuación, se muestra una representación gráfica del flujo propuesto (figura 3-30)

Figura 3-30: Flujo de detección, análisis y reporte. Fuente autores.



Los principales elementos que componen esta fase son detección, identificación, registro, acción predictiva y reporte, todos estos relacionados con los equipos o hardware que interviene en el proyecto y hacen parte del inicio del ciclo de vida de la gestión de incidentes de seguridad, de ahí la importancia de contar con una adecuada preparación para la fase 2 y también de tener claridad en la fase 3 de lecciones aprendidas y mejoramiento lo equivalente a las características que se pueden tener en cuenta para contribuir al constante fortalecimiento de la presente fase, ya que es fundamental para la objetividad de los reportes y su predicción. Entre mejor sea el proceso de preparación y entre más armonía exista en relación con la última fase de este modelo (lecciones aprendidas y mejoramiento) mejor comportamiento y mayor eficiencia tendrán los reportes y sus predicciones, contribuyendo así a un mejoramiento continuo del modelo en general.

Los demás elementos del ciclo de vida de la gestión de incidentes de seguridad con el alcance del presente proyecto como lo son la tipificación, categorización y priorización de incidentes se abordan en la siguiente fase (gestión de reportes) del modelo.

Fase 3: Gestión de reportes

La fase de gestión de reportes es la fase en la que inicia la interacción con el equipo de gestión de incidentes o el equipo de respuesta a incidentes. Corresponderá a un equipo único de contacto inicial, al grupo de respuesta a incidentes o a quien haga sus veces recibir y estar atentos a los reportes que arroja el dashboard del sistema de la fase anterior.

Los reportes que se generan de la fase de detección, análisis y reporte deberán ser gestionados por el equipo de gestión de incidentes correspondiente y deberán tener en cuenta los siguientes elementos principales para relacionar el reporte presentado con el impacto o afectación que este pueda generar a la organización en orden de operación y continuidad de negocio. Estos elementos son la categorización, clasificación y priorización del incidente.

Categorización: Los incidentes de seguridad pueden ser generados por diferentes factores como acciones humanas intencionadas o accidentales, acontecimientos técnicos como fallas o medios físicos externos. A continuación, se presenta una lista de categorías que se pueden contemplar en el modelo de gestión de incidentes de seguridad, considerando que puede ser modificado según la necesidad de la organización con énfasis al entorno económico o nicho de negocio que maneje. Las siguientes categorías se presentan como las más relevantes y relacionadas con el objetivo del modelo (tabla 3-7).

Tabla 3-7 Incidentes por categoría

Categoría	Descripción	Ejemplo
Malware e inspección	Eventos causados por programas maliciosos que puedan afectar la confidencialidad, integridad o disponibilidad de la información y los sistemas SCADA afectando la operación.	Virus, gusanos, troyanos, botnet, ramsomware, ataques persistentes de fuerza bruta, denegación de servicios, escaneo de redes, intentos de acceso, inundación de paquetes, entre otros.
Daño físico	Eventos que causen afectación por acciones malintencionadas o accidentales sobre los sistemas de red industrial.	Incendio, contaminación, corrosión, destrucción de equipos, vandalismo, robo o alteración de componentes, entre otros.
Falla técnica	Eventos causados por fallas sobre los sistemas o elementos base que soportan los sistemas de red industrial SCADA	Interrupción eléctrica, sobrecarga, falla de comunicación, intermitencias, malfuncionamiento de software o hardware, entre otros.
Desorden social	Eventos causados por inestabilidad político social	Disturbios, guerra, terrorismo, entre otros.

	que afecten la seguridad o estabilidad de los sistemas SCADA.	
Desastre natural	Eventos causados por desastres naturales que puedan afectar a los sistemas SCADA en diferentes geografías.	Derrumbes, tormentas eléctricas, inundaciones, temblores, entre otros.

Priorización: La prioridad que tendrá un incidente de seguridad informática en el modelo de gestión de incidentes será determinado por el impacto y la urgencia que pueda generar el incidente en la operación del sistema industrial y también en la continuidad del negocio.

Para realizar una estimación del impacto que puede generar un incidente de seguridad en el sistema de redes industriales SCADA se determina una clasificación según los siguientes criterios para determinar una escala o niveles de impacto:

Se considera inicialmente un criterio que no se incluye en la escala o niveles de impacto por considerarse inicialmente crítico para el negocio, se trata de la importancia del sistema afectado, que para el caso de este modelo es el sistema de redes industriales SCADA que soportan la operación y producción del negocio, por ende, se considera una infraestructura crítica para los criterios de pérdida de operación e impacto social y cualquier incidente que se reporte en relación al sistema SCADA, deberá tener prioridad con relación a otros incidentes reportados por otras fuentes, medios o canales ajenos a este modelo (tabla 3-8).

Tabla 3-8 Niveles de impacto

Criterio \ Niveles	Severo	Grave	Considerable	Menor
Pérdida de operación y continuidad	-Parálisis total de la operación.	-Parálisis temporal o	-Intermitencias frecuentes de la operación.	-Intermitencias leves o poco

	-Pérdida de capacidad productiva. -Pérdida de la confidencialidad, integridad y disponibilidad de datos clave. -Otros que la organización no pueda soportar el nivel de pérdida.	parcial de la operación. -Reducción o limitación prolongada de la capacidad productiva. -Compromiso de la confidencialidad, integridad y disponibilidad de datos clave. -Otros que para la organización represente costo enorme la recuperación y normalidad de la operación.	-Reducción o limitación temporal de la capacidad productiva. -Afectación de algún componente de confidencialidad, integridad o disponibilidad de los datos clave. -Otros que para la organización represente un costo alto la recuperación y normalidad de la operación.	frecuentes de la operación. -Reducción momentánea de la capacidad productiva. -Afectación leve de algún componente de confidencialidad, integridad o disponibilidad de los datos clave. -Otros que para la organización representen un costo aceptable la recuperación y normalidad de la operación.
Impacto social	-Afectación en la mayoría de los departamentos con presencia del servicio.	-Afectación en una o más ciudades principales con presencia del servicio.	-Afectación en una o más ciudades secundarias o municipios con presencia del servicio.	-Afectación de un área o sector de una ciudad con presencia del servicio.

	-Grave amenaza para la seguridad nacional. -Causal de alteración social inminente. -Consecuencias severas para el desarrollo económico e interés público.	-Alta amenaza para la seguridad nacional. -Causal de pánico social inminente. -Consecuencias significativas para el desarrollo económico e interés público.	-Amenaza limitada para la seguridad nacional. -Causal de alguna alteración social focalizada. -Consecuencias ligeras para el desarrollo económico e interés público	-Pequeña posibilidad de amenaza para la seguridad nacional. -Baja posibilidad de alteración social. -Daño a los intereses de individuos, organizaciones y comercios.

Luego de los criterios y niveles de impacto que se indican en la tabla anterior, se realiza a continuación una tabla de prioridad que se recomienda en el modelo de gestión de incidentes de seguridad y que servirá al equipo de gestión de incidentes o quien haga sus veces para orientarse en las decisiones que se deben tomar para lograr un escalamiento asertivo al equipo de respuesta a incidentes. Así tendrá criterios para identificar el nivel de impacto por escala y cruzarla con la prioridad en relación con el incidente y tener elementos suficientes para tomar una decisión. Esta parte del modelo se relaciona con los elementos de observación y orientación del método OODA en la tabla 3-9.

Tabla 3-9 Nivel de prioridad

Prioridad	Descripción
Crítica	-Incidente que no se puede manejar o controlar utilizando recursos propios disponibles.

	-Incidente que inevitablemente generar interrupción o falla en los sistemas críticos del negocio (SCADA) y requieren planes adicionales -Incidente que implique o relacione sanciones y regulaciones gubernamentales o legales por incumplimientos en el servicio. -Errores procedimentales que puedan generar pérdida financiera o reputacional aceleradamente. -Cualquier incidente que afecte la reputación de la organización y amenace la continuidad del negocio.
Alta	-El incidente puede generar pérdida total del control de uno o más sistemas de la red SCADA. -El incidente puede contemplar fuga de información clave del negocio. -El incidente puede requerir unidades de apoyo externas o adicionales como trabajo forense, judicial o gubernamental. -El incidente compromete la imagen o reputación organizacional ante medios de comunicación.
Media	-El incidente puede afectar el control de algún componente del sistema de la red SCADA. -El incidente puede contemplar fuga de información no crítica del negocio, de procesos o datos personales. -Puede comprometer otros sistemas y/o estaciones de trabajo de los colaboradores con funciones clave para la operación de la red industrial.

	-El incidente puede comprometer levemente la imagen o reputación de la organización.
Baja	-Cuando el impacto financiero es bajo para la organización. -El incidente puede afectar sistemas o estaciones de trabajo no críticos para la operación de la red industrial. -El incidente no compromete fuga de información clave del negocio, de procesos u otros datos propios de la operación del negocio. -El incidente no afecta la imagen o la reputación de la organización.

Una vez se tienen las tablas de criticidad e impacto, se puede realizar un cruce entre ellas para observar y orientarse, y determinar qué decisión tomar en relación y que puedan reducir, evitar o minimizar los impactos que pueda llegar a generar el incidente si se llega a materializar.

Dado lo anterior, se resalta la importancia de la observación y orientación en el método OODA para obtener la mayor información posible relacionada con el impacto y criticidad que pueda tener el incidente, para así poder darle la prioridad que requiere y dar un diagnóstico inicial más preciso y óptimo con el que se pueda realizar un escalamiento seguro. Posterior a la priorización del incidente, es necesario determinar a quién se deberá informar según la prioridad definida y por los medios establecidos como telefónico, Mensaje Instantáneo (MI) como WhatsApp, Telegram, entre otros autorizados por la organización o correo electrónico como se muestra en la tabla 3-10.

Tabla 3-10 Roles y contactos que se deben informar

Prioridad	Contacto	Momento	Medio
Crítica	Equipo técnico de respuesta a incidentes	Inmediato	Telefónico
	Gestor de seguridad informática	Inmediato	Telefónico
	Gestor de operaciones del sistema SCADA	Inmediato	Telefónico
	Jefe de seguridad informática	Inmediato	Telefónico

	Gerente de TI	Inmediato	Telefónico
Alta	Equipo técnico de respuesta a incidentes	Inmediato	Telefónico
	Gestor de seguridad informática	Inmediato	Telefónico
	Gestor de operaciones del sistema SCADA	< 15 min	Telefónico
	Jefe de seguridad informática	Inmediato	Telefónico
	Gerente de TI	< 15 min	MI y correo
Media	Equipo técnico de respuesta a incidentes	Inmediato	Telefónico
	Gestor de seguridad informática	< 15 min	MI y correo
	Gestor de operaciones del sistema SCADA	< 30 min	Correo
Baja	Equipo técnico de respuesta a incidentes	Inmediato	Telefónico
	Gestor de Seguridad informática	< 1 hora	Correo

Para los casos críticos lo ideal es que exista un comité o equipo de crisis al que se pueda notificar directamente y que se encargue de liderar un Puesto de Mando Unificado (PMU) para la gestión de crisis y que se apoye en las unidades técnicas y operativas correspondientes para afrontar y superar la etapa de crisis. Los lineamientos, planes y recomendaciones para la gestión de crisis exceden los ámbitos de este proyecto.

Diagnóstico inicial: El equipo de gestión de incidentes deberá estar lo suficientemente preparado, familiarizado y enfocado para referenciarse en el método OODA y así poder realizar un diagnóstico inicial preciso que permitirá al equipo de respuesta a incidentes continuar con el proceso de contención, erradicación y respuesta que le corresponde, pero es de vital importancia que quien notifique lo realice de la forma adecuada y con la mayor cantidad de información posible, y lo más importante, que sea acertada y óptima al incidente de seguridad.

La observación y orientación son claves en el personal del equipo de gestión de incidentes y dependerá de las habilidades que puedan desarrollar, la astucia y agilidad para realizar una buena conjetura del incidente que están gestionando y así tomar una decisión acertada.
Las tablas anteriores permitirán orientarse dependiendo del tipo de incidente que reporte el filtro Kalman y así poder llevar a tomar una decisión respecto a cómo continuar la gestión del incidente.

Lo anterior corresponde en el método OODA a la Decisión, que se presenta cuando se tiene la información suficiente y se toma la determinación de continuar con la gestión que corresponda según se haya determinado en la observación y orientación como lo más objetivo para reducir los impactos que pueda generar el incidente si llega a materializarse.

Escalamiento: Una vez se tiene la información suficiente respecto al incidente reportado, el relacionamiento de la criticidad y la orientación sobre lo que está sucediendo y haber tomado una decisión, se deberá pasar a tomar las acciones correspondientes al escalamiento. Si el equipo de gestión de incidentes es el mismo equipo de respuesta a incidentes, el escalamiento que se realiza es casi transparente entre los procesos, ya que pertenece al mismo equipo de trabajo y proceso, por lo que solamente se considera necesario el proceso de documentación correspondiente y notificación al resto del equipo al que interesa o corresponde colaboración en la respuesta al incidente. Si el equipo de gestión de incidentes es distinto al equipo de respuesta a incidentes, deberá realizarse un proceso de escalamiento siguiendo lo indicado en la tabla 3-10, para así poder garantizar una entrega óptima de la información correspondiente al incidente reportado.

El escalamiento debe realizarse por medio de un formato ligero, el cual permite relacionar la información completa y más relevante que le permitirá al equipo de respuesta a incidentes continuar con la gestión correspondiente. El formato de registro y escalamiento se presenta más adelante en los anexos del presente documento.

Fase 4: Lecciones aprendidas y mejoramiento

Las lecciones aprendidas son capaces de determinar el valor y el crecimiento del modelo, a partir del desarrollo, la implementación de la herramienta OODA y este a su vez, aumenta el nivel de conocimiento y madurez de cómo debe actuar el equipo de respuesta en cada iteración, por tal razón, se minimiza el riesgo y se optimizan los procesos de seguridad. Por lo anterior, se propone que al finalizar cada una de las etapas se recolecte la siguiente información:

Ajuste al proceso de observación: Primero se debe recolectar y analizar los datos para iniciar con el diagnóstico temprano del incidente, analizar si afecta directamente al negocio. Permanecer atento, alerta, vigilante y bien enterado de lo que ocurre en los grupos de interés (directivos del negocio).

Actualización de las reglas: Se debe ajustar las reglas personalizadas que se crearon en el IDS SNORT para minimizar las posibles vulnerabilidades del sistema SCADA, adicionalmente actualizar las reglas por defecto de la comunidad o de pago que se hayan configurado en el sistema.

Ajustar los grados de criticidad del modelo: Cuando las reglas hayan sido actualizadas, deben ser monitoreadas constantemente respecto a los principales vectores de ataques de los sistemas SCADA y ajustar la criticidad para que no pierdan vigencia en el tiempo y si es el caso, configurar nuevas reglas que contemplen dichos vectores de ataque.

Gestión a los reportes: Los reportes que se muestran en el filtro Kalman deben de ser priorizados por el nivel de criticidad y el volumen de los ataques, para que el equipo pueda gestionar los eventos más críticos haciendo más eficiente el proceso.

Capacitación del equipo de gestión de incidentes: Los miembros deben ser capacitados y entrenados sobre cada evento que se haya materializado, garantizando la transferencia de conocimiento y contribuya en el aseguramiento del sistema. Así mismo énfasis fundamental en la utilización del método OODA como herramienta clave en su labor.

Actualización de la base de conocimiento: La base debe actualizarse con los aciertos y desaciertos, ajustar los procesos, las decisiones que mejor funcionaron como las que no fueron tan asertivas para permitir recolectar la experiencia y mejorar el proceso de gestión de reportes.

3.4. Evaluación del modelo de incidentes

A continuación, se muestran los resultados de los ataques que se desarrollaron anteriormente, donde se analizan cada uno de sus componentes de salida en el dashboard de la herramienta de predicción basada en el filtro Kalman.

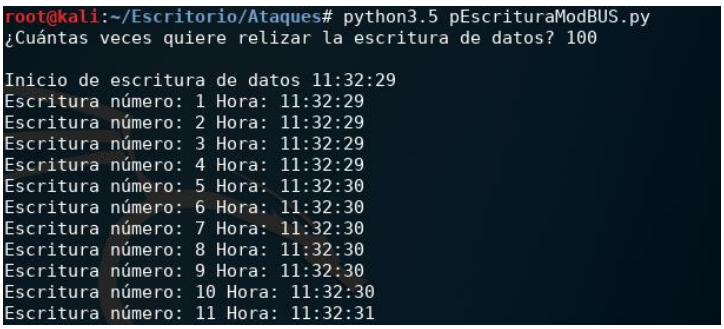
3.4.1. Generación de diferentes tipos de eventos simulados de intrusión al sistema SCADA

Para un mejor entendimiento de la generación de los diferentes eventos simulados, el proceso se divide en simulación de ataques, registro del evento y visualización.

Simulación de ataques

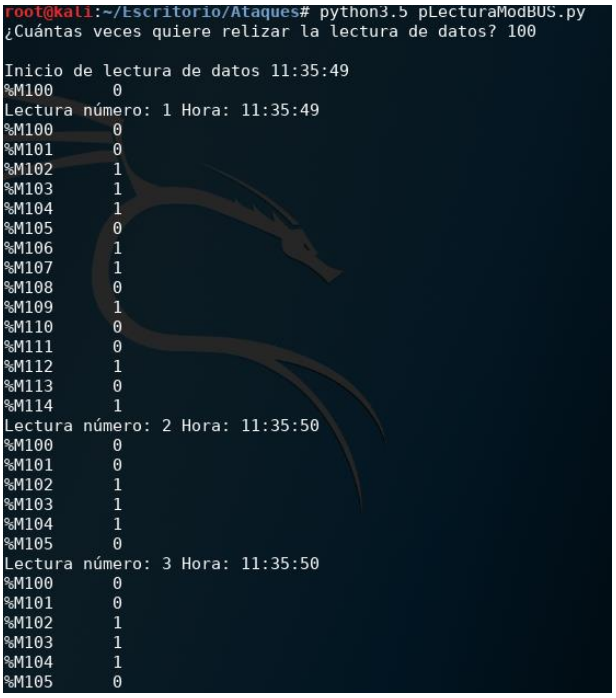
Inicialmente se ejecutan los ataques que se explicaron anteriormente desde un sistema operativo Kali Linux que servirá como "atacante". Se ejecuta el evento de escritura donde se realiza una modificación en los datos del PLC con datos aleatorios y este proceso se repite por **100 veces**, como se observa, este evento tiene una tasa de 5 incidentes por segundo que comprometen la integridad de la información como se muestra en la figura 3-31.

Figura 3-31: Ataque 1. Sobrescribir datos al PLC Siemens 2700 con protocolo modbus. Fuente autores.



Luego la máquina "atacante" realiza un segundo ataque, el cual consiste en leer toda la información que se aloja en el PLC comprometiendo los datos alojados en este. Este evento lee la información del PLC de forma aleatoria, desde la posición %M100 hasta la %M114 y puede volcar los datos de los bloques de información donde el atacante puede realizar una copia completa de los datos del dispositivo. Este evento también se ejecuta **100 veces** con una velocidad de 4 lecturas por segundo como se muestra en la figura 3-32

Figura 3-32: Ataque 2. Lectura de datos al PLC Siemens 2700 con protocolo modbus. Fuente autores.



Registro del evento

Desde el lado del sistema SCADA, se evidencia como se captura cada intento del "atacante" por leer y sobrescribir la información que se encuentra alojada en el PLC Siemens 2700 a través del LOG, donde se destaca la captura de la dirección IP y la ID de la máquina que se conecta al PLC del sistema SCADA, puerto, hora de conexión, hora de desconexión, entre otras opciones (ver figura 3-33), la generación de esta información se da uno a uno por cada evento que ocurra con el sistema SCADA (de 20 a 30 por segundo aproximadamente) y no puede ser analizada por el personal técnico dada su velocidad de entrega, por tal razón los datos son capturados por el IDS SNORT para ser almacenando en la base de datos MySQL que se configuró anteriormente y ser analizada por el visualizador.

Figura 3-33: Comportamiento del sistema SCADA Laboratorio CONPOT. Fuente autores.

```
2019-06-08 11:53:23,166 Modbus response sent to 10.1.1.12
2019-06-08 11:53:23,169 Modbus client disconnected. (74a637d8-1bd7-4686-9747-ed8499e2bf30)
2019-06-08 11:53:23,279 New Modbus connection from 10.1.1.12:58828. (74a637d8-1bd7-4686-9747-ed8499e
2bf30)
2019-06-08 11:53:23,293 Modbus traffic from 10.1.1.12: {'function_code': 15, 'slave_id': 1, 'request
': '000100000009010f0064000a02d400', 'response': '0f0064000a'} (74a637d8-1bd7-4686-9747-ed8499e2bf30
)
2019-06-08 11:53:23,298 Modbus response sent to 10.1.1.12
2019-06-08 11:53:23,300 Modbus client disconnected. (74a637d8-1bd7-4686-9747-ed8499e2bf30)
2019-06-08 11:53:23,364 New Modbus connection from 10.1.1.12:58830. (74a637d8-1bd7-4686-9747-ed8499e
2bf30)
2019-06-08 11:53:23,376 Modbus traffic from 10.1.1.12: {'function_code': 1, 'slave_id': 1, 'request'
: '000100000006010100640014', 'response': '0103d45003'} (74a637d8-1bd7-4686-9747-ed8499e2bf30)
2019-06-08 11:53:23,381 Modbus response sent to 10.1.1.12
2019-06-08 11:53:23,385 Modbus client disconnected. (74a637d8-1bd7-4686-9747-ed8499e2bf30)
2019-06-08 11:53:23,498 New Modbus connection from 10.1.1.12:58832. (74a637d8-1bd7-4686-9747-ed8499e
2bf30)
```

Visualización del evento

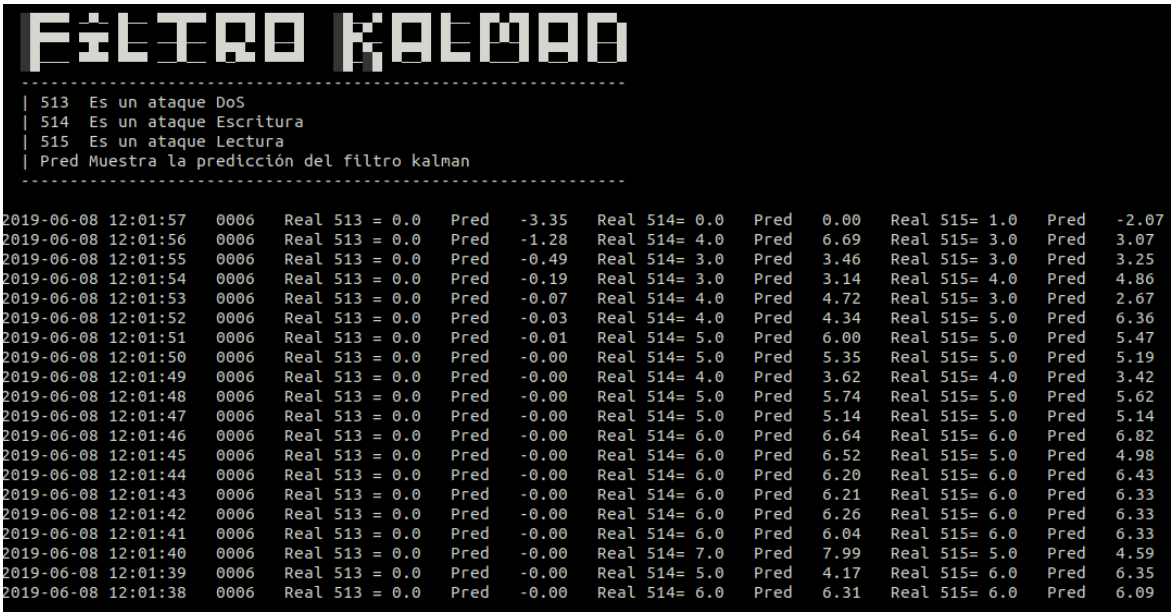
Ahora que el sistema SCADA se encuentra bajo ataque, el IDS está capturando y almacenando toda la información generada por el atacante, estos datos son agrupados y seleccionados para que se inicie el proceso de predicción con el filtro Kalman, el cual se alimenta de toda la información que se encuentra en la base de datos y se muestra en pantalla en un lenguaje simple para que sea analizado por el personal técnico.

En este tablero se muestra la cantidad de eventos que se están materializando en tiempo real, la información es actualizada segundo a segundo para que se obtenga toda la trazabilidad de los sucesos que ocurren dentro del sistema SCADA, dentro de este se muestran las siguientes variables:

- Fecha: En este campo se muestra el momento exacto que ocurre el evento.
- 513 ataque DoS: Muestra la cantidad de eventos sucedidos por el escaneo de IP y puertos que se realizan dentro del sistema SCADA.
- 514 ataque de escritura: Es la cantidad de veces que un atacante sobrescribe los datos dentro del PLC a través del puerto 502 de comunicación Modbus
- 515 ataque de lectura: Es la cantidad de veces que los datos del PLC han sido leídos y accedidos.
- Predicción del filtro Kalman: de acuerdo con la información histórica generada por los eventos de seguridad, el filtro actúa y muestra cual sería el estado futuro por cada uno de los eventos que se encuentren configurados.

A continuación, se muestra cómo es el tablero de control (figura 3-34).

Figura 3-34: Dashboard de visualización. Fuente autores.



Como se mencionó anteriormente, el dashboard imprime los eventos que están sucediendo segundo a segundo dentro del sistema SCADA registrando todos los posibles eventos de seguridad. Para interpretar la información, ésta debe ser analizada de forma vertical por cada evento que muestra el tablero, por ejemplo:

En el caso del ataque 513 (que es un ataque de DoS), se identifica la palabra “Real”, esto hace referencia a la cantidad de eventos que se están registrando dentro del IDS SNORT, la columna “Pred” es la predicción que realiza el filtro Kalman de acuerdo al historial que se va generando a la columna “Real” que se encuentran almacenados en la base de datos del sistema SCADA, dado que en los 19 segundos que muestra en la figura 3-34 el IDS no detectó ningún evento relacionado a este tipo de ataque, el resultado o valor del predicción es negativo porque el dato de entrada al filtro Kalman es cero, vale recordar que el filtro Kalman recibe tres variables de entrada para realizar la predicción, los cuales son: dato real, predicción anterior y la varianza para afinar la predicción en cada iteración.

En los ataques 514 y 515, se observa como el IDS SNORT va registrando los posibles eventos de seguridad, donde se identifica que éstos van incrementando a medida que trascurre el tiempo y a su vez, el filtro Kalman recibe estos datos para calcular la predicción, la tendencia y la intensidad de los ataques que ayudan al personal de seguridad a interpretar de forma más asertiva dicho comportamiento de forma más rápida y eficaz.

3.4.2. Validación de las salidas del Filtro Kalman respecto a criticidad e impacto

De acuerdo con la salida del filtro Kalman, para el alcance de este proyecto se podrán tener tres tipos de reportes, DoS, Lectura y Escritura. Al realizar una validación de estas salidas respecto a la criticidad e impacto de un incidente como se ha definido anteriormente, el orden de criticidad e impacto de menor a mayor es DoS, Lectura y Escritura.

DoS: Será la salida del filtro Kalman para aquellos ataques de identificación u observación de posibles objetivos, que en sí pueden no considerarse un incidente, pero sí un precursor importante para prestar atención de que algo o alguien está observando la red. De acuerdo con lo anterior, su criticidad e impacto se consideran bajos.

Lectura: Para un reporte de lectura, se relacionan aquellos ataques que han logrado identificar uno o varios PLCs de la red SCADA y están capturando o leyendo los datos generados por éstos, para lo cual se considera una criticidad e impacto medio ya que puede estar en curso un incidente o a punto de presentarse.

Escritura: El reporte de escritura que genera el filtro Kalman, corresponde a un ataque en el cual los datos generados por uno o varios PLC están siendo sobrescritos o reemplazados por los verdaderos datos del PLC, lo que ocasiona mediciones erradas sobre la red SCADA, considerándose esto de un impacto y criticidad altos por alterar la información del sistema y comprometiendo su confidencialidad, disponibilidad e integridad. Para lo cual se deberá considerar de alta prioridad ya que el incidente puede ser inminente.

En cualquier tipo de salida o reporte que se presente desde el dashboard del filto Kalman, el equipo de gestión de incidentes deberá relacionar los datos necesarios en el formato de registro y escalamiento de incidentes [Anexo 2] según el tipo de incidente, su criticidad e impacto. Se recomienda llevar el formato en un sistema de información digital que permita agilizar su diligenciamiento y tener control de la base de datos de los registros de incidentes que se presentan. El formato para diligenciar será básico y llevará la información fundamental que permita describir el incidente y relacionar lo que el equipo de gestión haya obtenido del método OODA para así brindar los elementos básicos para que el equipo de respuesta a incidentes pueda seguir con la respectiva gestión y de ser el caso, su contención y erradicación.

El diligenciamiento del formato de registro y escalamiento, deberá ser realizado con la información que el personal técnico de gestión de incidentes haya logrado obtener poniendo en práctica el OODA y con la información que arroja el dashboard del filtro Kalman, es así como esta parte del modelo es de criterio propio de quien gestiona el reporte, permitiendo así la experiencia del personal y su buena preparación y capacitación, mejorar los tiempos de respuesta, objetividad de los incidentes escalados.

4. Conclusiones

Como se pudo apreciar en los resultados, se propone un modelo para el manejo de incidentes de seguridad una vez detectado de manera predictiva con el filtro Kalman posibles intrusiones en los SCADA, con ello, es posible evitar posibles riesgos que afecten la disponibilidad, integridad y/o confidencialidad de la información (acorde a la naturaleza del ataque), en consecuencia, el objetivo general del proyecto se ha cumplido. Dicho modelo puede ser replicado a sistemas similares que tengan la capacidad de implementar un filtro Kalman para la predicción.

Poder predecir posibles eventos de seguridad les permitirá a las organizaciones gestionar de manera más proactiva la seguridad en sus sistemas industriales, de igual forma, es fundamental que el manejo de incidentes de seguridad esté relacionado y/o integrado con los procesos de continuidad de negocio y gestión de crisis, con ello, logra gestionar adecuadamente cualquier evento.

El primer objetivo “Identificar los diferentes sistemas de detección de intrusos que puedan integrarse a las redes industriales – SCADA” se logró de manera exitosa como se muestra en el numeral 2.1, además como resultado, se obtiene una tabla comparativa con diferentes aspectos considerados para los sistemas IDS y con sus diferentes funcionalidades. Adicionalmente, en el punto 3.1 se muestra una tabla que compara cada uno de los IDS considerados, y como resultado, arroja que el IDS SNORT es el más apropiado para este proyecto.

En el punto 3.3 se muestra la construcción, implementación y configuración del filtro Kalman, el cual es desarrollado en el lenguaje de programación Python que facilita la integración de la solución propuesta. Adicionalmente, se realizaron tres eventos simulando diferentes ataques (DoS, Escritura y Lectura) a sistemas SCADA en sus PLC’s a través del protocolo de comunicación Modbus. También se realizó la creación y configuración de las reglas personalizadas en el IDS SNORT, que sirven de insumo al filtro Kalman en la predicción de los eventos que se están materializando. Con la combinación de los elementos anteriores se construye la herramienta de predicción, la cual muestra por medio de un tablero de líneas de comando el estado de los ataques y la predicción de

cada uno de ellos y da como solución al segundo objetivo específico “Desarrollar el filtro Kalman para la detección de intrusos, así lograr predecir posibles eventos de seguridad”.

Para dar solución al tercer objetivo específico “Establecer la estrategia para de identificación, manejo y respuesta de los incidentes de seguridad” en el punto 3.4 se creó un modelo de identificación y reacción ante los diferentes tipos de eventos de seguridad que apliquen a los sistemas SCADA. Este procedimiento se construyó a partir de documentación disponible en diferentes bases de datos de información sobre manejo de incidentes de seguridad y apalancándose en las normas SP800-61 de la NIST e ISO 27035 y teniendo en cuenta que este desarrollo es de naturaleza predictiva. Adicionalmente, se desarrolló un modelo de escalamiento del evento de acuerdo con su nivel de categoría, criticidad e impacto para generar un marco de actuación dentro de la organización cuando se materialice un evento.

Finalmente, el cuarto objetivo específico “Evaluar el modelo para el manejo de incidentes de seguridad una vez realizada la predicción de posibles ataques en el sistema de detección de intrusos en un ambiente controlado” se logra alcanzar realizando inicialmente una descripción lógica y argumentativa de cómo funciona la fase 2 de detección, análisis y reporte de los incidentes detectados desde la figura 3-31 hasta la figura 3-34, así como de la validación de las salidas del filtro Kalman en relación con la criticidad e impacto. También se enuncia cómo es el procedimiento que se lleva a cabo con el método OODA para lograr un escalamiento asertivo y el diligenciamiento del formato correspondiente lo más completo y claro posible para el equipo técnico de respuesta a incidentes que continuará con la gestión correspondiente al incidente, tenga la mayor información posible, pero en un formato simple que brinde agilidad.

5. Recomendaciones, lecciones aprendidas y trabajo futuro.

De acuerdo al desarrollo del laboratorio que se implementó en este trabajo, se recomienda que las reglas del sistema de detección de intrusos IDS SNORT, cuente con un mecanismo de actualización que vienen por defecto, esto se puede realizar con una configuración adicional en IDS con la herramienta PulledPork [45].

En La configuración e implementación del laboratorio del sistema SCADA con el proyecto CONPOT, se presentaron dificultades al momento de la instalación del componente Barnyard2, dado que éste tiene una cantidad de elementos como prerrequisitos para su funcionamiento y no se encontró información que ayudara a solucionarlo. Para resolver este inconveniente, se implementaron las librerías **autoreconf** y **automake --add-missing** que ayudaron a recopilar de forma automática todas las dependencias necesarias para la ejecución de Barnyard2.

Tener en cuenta que se debe actualizar las reglas personalizadas de acuerdo con la evolución de los vectores de ataques que vayan surgiendo en el tiempo y así certificar la vigencia de estas, ayudando a blindar y minimizar al sistema SCADA de vulnerabilidades explotadas anteriormente.

Es de vital importancia que todos los eventos sean registrados con los aciertos y desaciertos dentro de una base de conocimiento cuando el incidente haya terminado y luego de esto, todo el personal sea capacitado e instruido sobre las medidas tomadas para minimizar riesgos futuros.

Para un trabajo futuro de este proyecto, se recomienda desarrollar las fases de contención, erradicación y recuperación de incidentes de seguridad, desde la óptica de ISO 27035 y NIST SP800-61, esto ayudaría a mejorar la capacidad de respuesta del equipo de seguridad informática de la organización.

También es importante considerar como alcance futuro la sincronización del sistema de detección de intrusos con la base de la comunidad SNORT, porque no siempre se conocerá la totalidad de las vulnerabilidades del sistema, lo que hace necesario contar con una actualización automática de la línea base de las reglas del sistema de detección para aumentar la protección.

A. Anexo 1: Lista de chequeo para la validación de la arquitectura del modelo.

Lista de chequeo para validación elementos tecnológicos de la arquitectura del modelo.		
Elemento o flujo en conjunto de elementos	Resultado	Observación
Solución CONPOT	Positivo	
Componentes PLC CONPOT	Positivo	
IDS SNORT y reglas base	Positivo	
Base de datos MySQL	Positivo	
Conexión IDS - MySQL	Positivo	
Almacenado MySQL	Positivo	
Switch conexión espejo	Positivo	
Conexión CONPOT - IDS	Positivo	
Automatización de ataques	Positivo	
Almacenado en MySQL con los ataques automatizados. Flujo atacante – CONTPOT – IDS – MySQL.	Positivo	
Filtro Kalman con variables ficticias	Positivo	
Conexión filtro Kalman - MySQL	Positivo	
Reportes filtro Kalman con datos de MySQL	Positivo	
Estructuración de Dashboard	Positivo	

B. Anexo 2: Formato de registro y escalamiento de incidentes

ORMATO DE REGISTRO Y ESCALAMIENTO DE INCIDENTES DE SEGURIDAD	
Fecha y hora del reporte	DD/MM/AA hh:mm:ss
Tipo de reporte	__DoS __Lectura __Escritura
Observación del reporte	
Categoría del incidente	
Nivel de impacto	
Nivel de prioridad	
Detalle del posible incidente y consecuencias	
Observaciones generales para la respuesta al incidente	
Nombres y apellidos de quien escala	
Fecha y hora del escalamiento	DD/MM/AA hh:mm:ss

6. Bibliografía

[1] K. Coffey, R. Smith, L. Maglaras, and H. Janicke, “Vulnerability Analysis of Network Scanning on SCADA Systems,” *Secur. Commun. Networks*, vol. 2018, pp. 1–21, Mar. 2018.

[2] D. J. Kalbfleisch, “SCADA Technologies and Vulnerabilities,” no. May 2014, 2013.

[3] J. J. Cano, G. María, and S. Meza, “IX Informe de encuesta lationamericana de seguridad de la informacion 2017,” no. c, pp. 1–10, 2017.

[4] A. A. Al Jahil and D. Giarratano, “Improvement of cyber-security measures in National Grid SA substation process control,” in *2016 Saudi Arabia Smart Grid Conference, SASG 2016*, 2017, pp. 1–6.

[5] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology,” 2012.

[6] A. S. Gallego and J. V. Salcedo, “Proyecto de automatización de planta multiproceso con horno mediante autómata siemens s7-1214c y scada en wincc,” 2016.

[7] E. Carozo Blumsztein and L. Vidal, “Sistemas SCADA, algunas recomendaciones de seguridad – Parte II,” Sep. 2013.

[8] H. Amini, M. R. Razeghinejad, and B. Esfandiarpour, “Primary single-plate molteno implant for pediatric glaucoma associated with sturge-weber syndrome,” *J. Ophthalmic Vis. Res.*, vol. 2, no. 1, pp. 40–45, 2007.

[9] A. Warzynski and G. Kolaczek, “Intrusion detection systems vulnerability on adversarial examples,” in *2018 Innovations in Intelligent Systems and Applications (INISTA)*, 2018, pp. 1–4.

[10] Martin Roesch, “Snort - Network Intrusion Detection & Prevention System,” 1998. [Online]. Available: https://www.snort.org/. [Accessed: 30-Apr-2019].

[11] M. O’Leary, “Snort,” in *Cyber Operations*, Berkeley, CA: Apress, 2015, pp. 605–641.

[12] Suricata, “Suricata Open Source IDS / IPS / NSM engine,” *https://suricata-ids.org*, 2017. [Online]. Available: https://suricata-ids.org/. [Accessed: 04-Jun-2019].

[13] J. Amann, J. Azoff, T. Fleury, and V. Grigorescu, “The Zeek Network Security Monitor,” 2019. [Online]. Available: https://www.zeek.org/. [Accessed: 04-Jun-2019].

[14] “Kismet Wireless.” [Online]. Available: https://www.kismetwireless.net/. [Accessed: 10-Nov-2018].

[15] OSSEC PROJECT TEAM, “OSSEC.” [Online]. Available: https://www.ossec.net/. [Accessed: 10-Nov-2018].

[16] Tripwire, "Cybersecurity and Compliance Solutions | Tripwire." [Online]. Available: https://www.tripwire.com/. [Accessed: 13-Jun-2019].

[17] "Samhain Labs | Samhain." [Online]. Available: https://la-samhna.de/samhain/. [Accessed: 20-Nov-2018].

[18] "Fortinet | Enhancing the Security Fabric." [Online]. Available: https://www.fortinet.com/. [Accessed: 13-Nov-2018].

[19] "DDoS Services: Cloud Security Products and Solutions | Radware." [Online]. Available: https://www.radware.com/. [Accessed: 20-Nov-2018].

[20] Palo Alto, "Threat Prevention - Palo Alto Networks." [Online]. Available: https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/threat-prevention.html. [Accessed: 11-Feb-2019].

[21] D. Stiawan, A. H. Abdullah, and M. Y. Idris, "The trends of Intrusion Prevention System network," *ICETC 2010 - 2010 2nd Int. Conf. Educ. Technol. Comput.*, vol. 4, pp. V4-217-V4-221, Jun. 2010.

[22] Siemens, "Operator Control and Monitoring Systems - Industrial Automation - Siemens Global Website." [Online]. Available: https://www.siemens.com/global/en/home/products/automation/simatic-hmi.html. [Accessed: 31-Oct-2018].

[23] R. E. Kalman, "A New Approach to Linear Filtering and Prediction Problems," *J. Basic Eng.*, vol. 82, no. 1, p. 35, 1960.

[24] N. Goldenberg and A. Wool, "Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 6, no. 2, pp. 63–75, Jun. 2013.

[25] H. M. N. Al Hamadi, C. Y. Yeun, and M. J. Zemerly, "A novel security scheme for the smart grid and SCADA networks," *Wirel. Pers. Commun.*, vol. 73, no. 4, pp. 1547–1559, 2013.

[26] Y. Yang *et al.*, "Multiattribute SCADA-specific intrusion detection system for power networks," *Power Deliv. IEEE Trans.*, vol. 29, no. 3, pp. 1092–1102, 2014.

[27] V. L. Do, L. Fillatre, and I. Nikiforov, "Sensitivity analysis of the sequential test for detecting cyber-physical attacks," in *2015 23rd European Signal Processing Conference, EUSIPCO 2015*, 2015, pp. 2261–2265.

[28] F. A. Ruslan, A. M. Samad, and R. Adnan, “Modelling of flood prediction system using hybrid NNARX and Extended Kalman Filter,” in *2017 IEEE 13th International Colloquium on Signal Processing & its Applications (CSPA)*, 2017, pp. 149–152.

[29] M. Nicola, C.-I. Nicola, M. Dutta, D. Sacerdotianu, and I. Hurezeanu, “System for monitoring of hot spot temperature of power transformer windings using fiber optic sensors, Kalman Filter and SCADA integration,” in *2018 International Conference on Development and Application Systems (DAS)*, 2018, pp. 99–104.

[30] P. Liu and T. Liu, “Physical Intrusion Detection for Industrial Control System,” in *2018 IEEE Conference on Communications and Network Security (CNS)*, 2018, pp. 1–2.

[31] S. Kumar, N. Gaur, and A. Kumar, “Developing a Secure Cyber Ecosystem for SCADA Architecture,” in *2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*, 2018, pp. 559–562.

[32] P. Valladares, W. Fuertes, F. Tapia, T. Toulkeridis, and E. Perez, “Dimensional data model for early alerts of malicious activities in a CSIRT,” in *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, 2017, pp. 1–8.

[33] C. De, Estudio sobre el estado de la Ciberseguridad Industrial en Euskadi. 2018.

[34] P. T. C., K. G. Boroojeni, M. Hadi Amini, N. R. Sunitha, and S. S. Iyengar, “Key Pre-distribution Scheme with Join Leave Support for SCADA Systems,” *Int. J. Crit. Infrastruct. Prot.*, 2018.

[35] “Conpot.” [Online]. Available: http://conpot.org/. [Accessed: 13-Nov-2018].

[36] “Welcome to Conpot’s documentation! — Conpot 0.6.0 documentation.” [Online]. Available: https://conpot.readthedocs.io/en/latest/index.html. [Accessed: 13-Nov-2018].

[37] “CommunityHelpWiki.” [Online]. Available: https://help.ubuntu.com/community/CommunityHelpWiki. [Accessed: 13-Nov-2018].

[38] Open CV Dev. Team, “OpenCV Introduction,” *OpenCV Online Doc.*, pp. 5–6, 2013.

[39] Python Software Foundation, “Welcome to Python.org.” [Online]. Available: https://www.python.org/. [Accessed: 09-Feb-2019].

[40] Numpy, “NumPy - NumPy.” [Online]. Available: http://www.numpy.org/. [Accessed: 09-Feb-2019].

[41] S. Rodriguez, “GUÍA TÉCNICA GTC-ISO/IEC COLOMBIANA 27035 TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.” .

[42] G. L. Rogova and R. Ilin, “Reasoning and Decision Making under Uncertainty and Risk for Situation Management,” in *2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, 2019, pp. 34–42.

[43] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, “Cyber-attack modeling analysis techniques: An overview,” in *Proceedings - 2016 4th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2016*, 2016, pp. 69–76.

[44] PulledPork, “GitHub - shirkdog/pulledpork: Pulled Pork for Snort and Suricata rule management (from Google code).” [Online]. Available: https://github.com/shirkdog/pulledpork. [Accessed: 23-Jun-2019].