



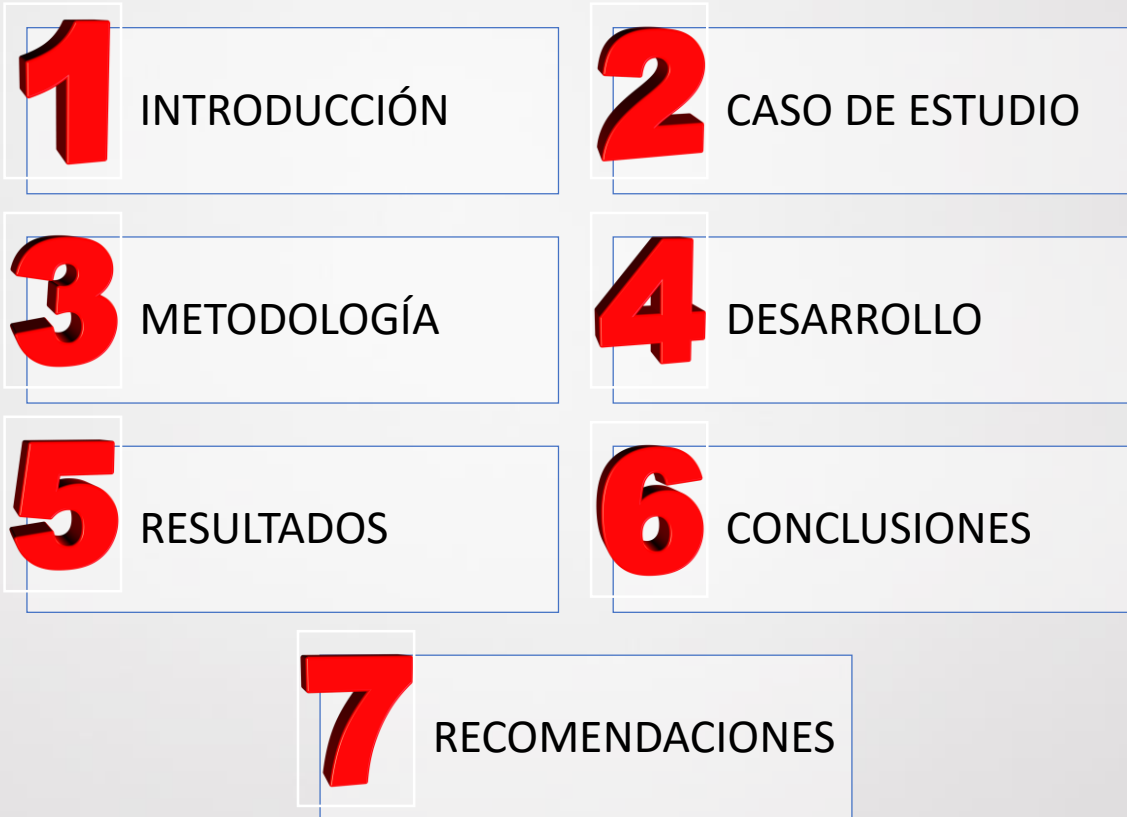
CENTRO DE POSGRADOS
MAESTRÍA EN GERENCIA DE SISTEMAS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE: MAGÍSTER EN GERENCIA
DE SISTEMAS

TEMA: MINERIA DE PROCESOS APLICADOS A LA CYBERSEGURIDAD RELACIONADOS CON
INCIDENTES DE ATAQUES EN UNA EMPRESA QUE OFRECE EL SERVICIO DE ACCESO A INTERNET
UTILIZANDO LA HERRAMIENTA ProM, ENMARcado EN EL ESTANDAR ISO 27000.

Septiembre - 2023

• CONTENIDO



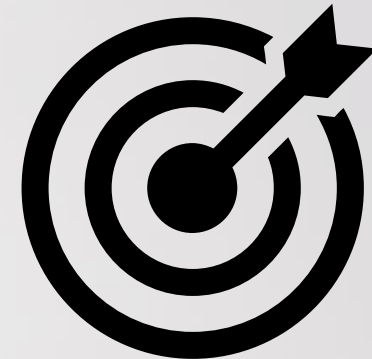
INTRODUCCION: Antecedentes

Crecimiento de inversión en medios digitales es de alrededor de un 22%.

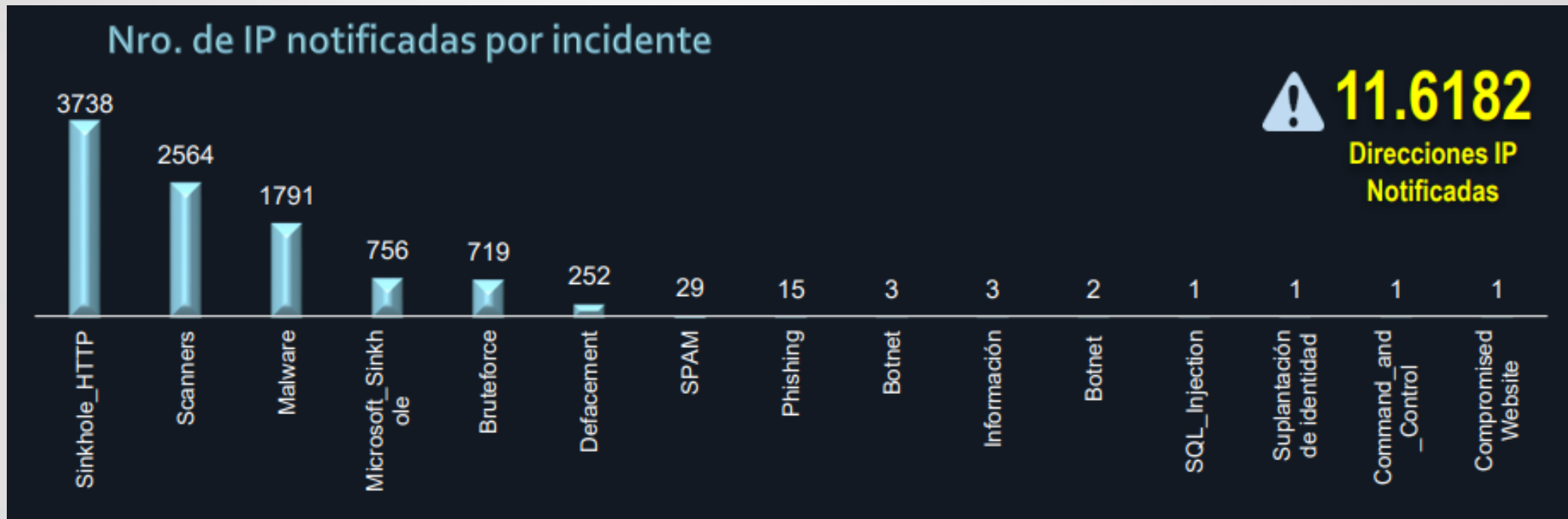
•Fuente: Informe Estado Digital 2021

Población con Acceso a Internet de casi el 80% de la población.

•Fuente: Informe Estado Digital 2021



INTRODUCCION: Antecedentes



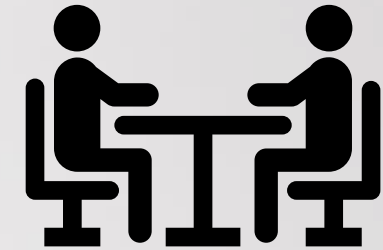
FUENTE: ECUCert 2022

- **INTRODUCCION: Objetivo General**
- Realizar una Minería de Procesos aplicados a la ciberseguridad relacionados con incidentes de ataques en una empresa que ofrece el Servicio de Acceso a Internet utilizando la herramienta ProM, enmarcado en el estándar ISO-27001.



INTRODUCCION: Objetivos específicos

- Analizar la calidad de servicio de internet brindada a los usuarios, con el fin de determinar la necesidad de implementar una adecuada ciberseguridad dentro de la empresa.
- Desarrollar un modelo basado en Minería de Procesos, con la finalidad de analizar el nivel de riesgo en los procesos operacionales en cuanto a la seguridad cibernética.
- Determinar el cumplimiento de normas legales en el control y seguridad de los procesos basándose en la norma ISO 27001.



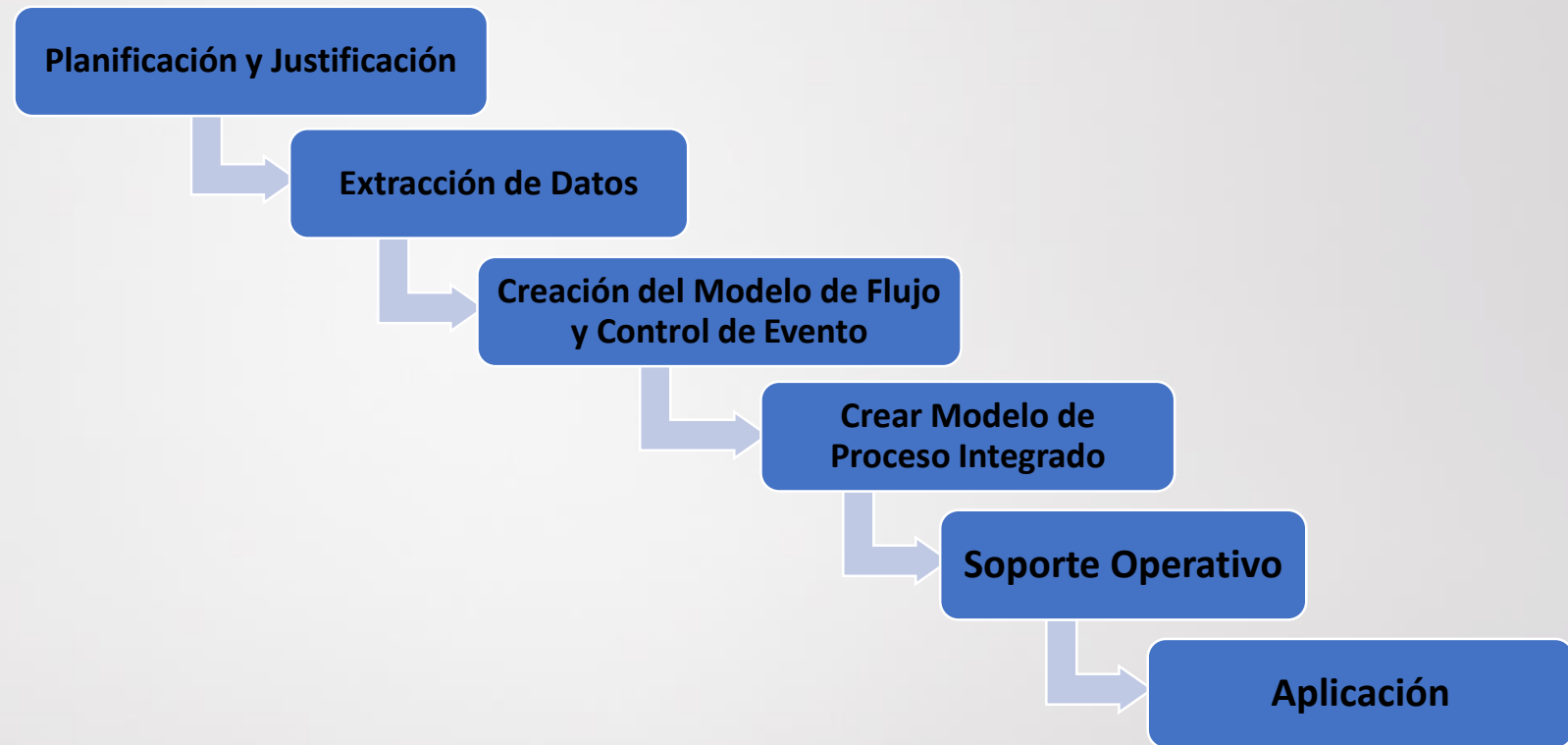
CASO DE ESTUDIO



-  Modelado a Partir de Datos
-  Modelado basado en Minería de Procesos
-  Minería de Datos no es Minería de Procesos
-  Minería de Procesos en ISPs

Metodología de la Investigación

Lifecycle model for process Mining.



Fuente: Process Mining de Van der Aalst, 1998, pág. 284

Metodología de la Investigación: Planificación y Justificación

- Este escenario corresponde al conocimiento total del negocio.



Fuente: Process Mining
de Van der Aalst, 1998,
pág. 284

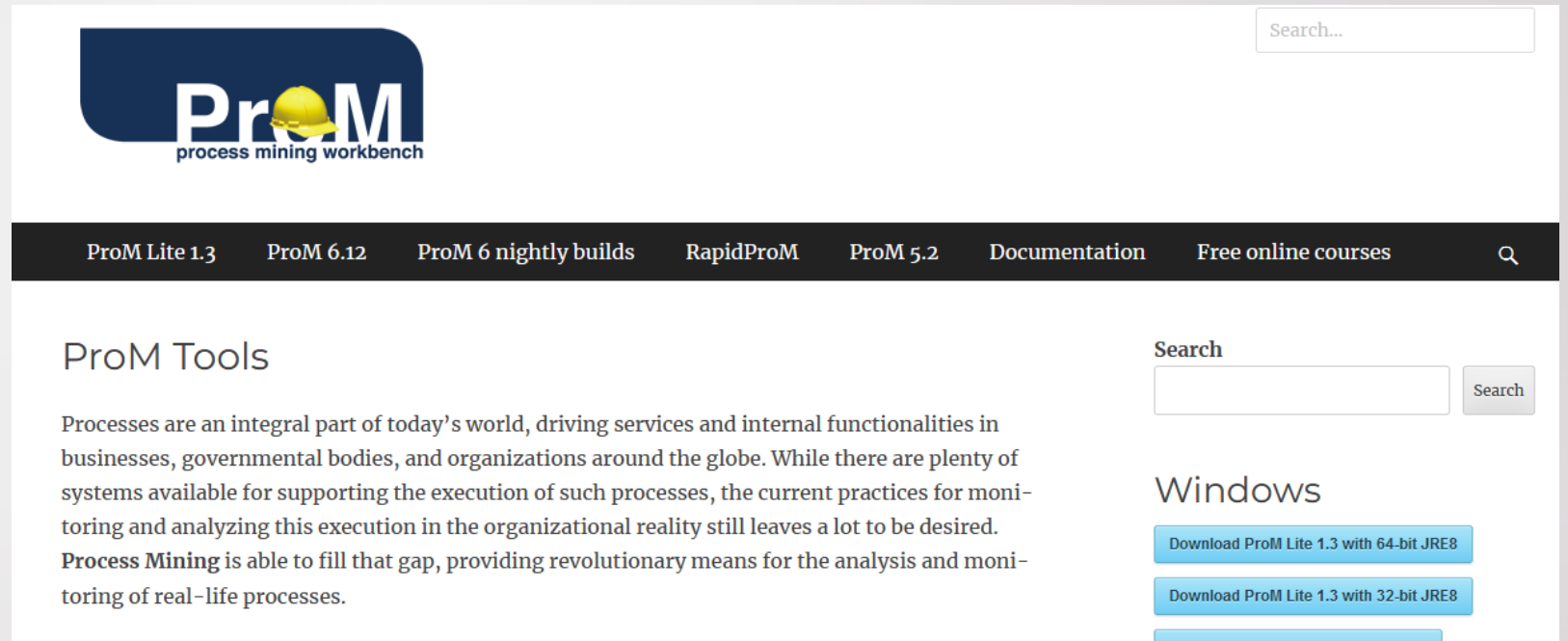
Metodología de la Investigación: Extracción de Datos



Item	Tipo de Incidentes	Numeros de Ips Notificadas
1	Sinkhole	3738
2	Scanners	2564
3	Malware	1791
4	Microsoft_Sinkhole	756
5	Bruteforce	719
6	Defacement	252
7	Spam	29
8	Phishing	15
9	Botnet	3
10	Información	3
11	SQL_Injection	1
12	Suplantación de Identidad	1
13	Comand_and_Control	1
14	Compromise Webside	1

FUENTE: ECUCert 2022

Metodología de la Investigación: Creación del Modelo de Flujo y Control de Evento

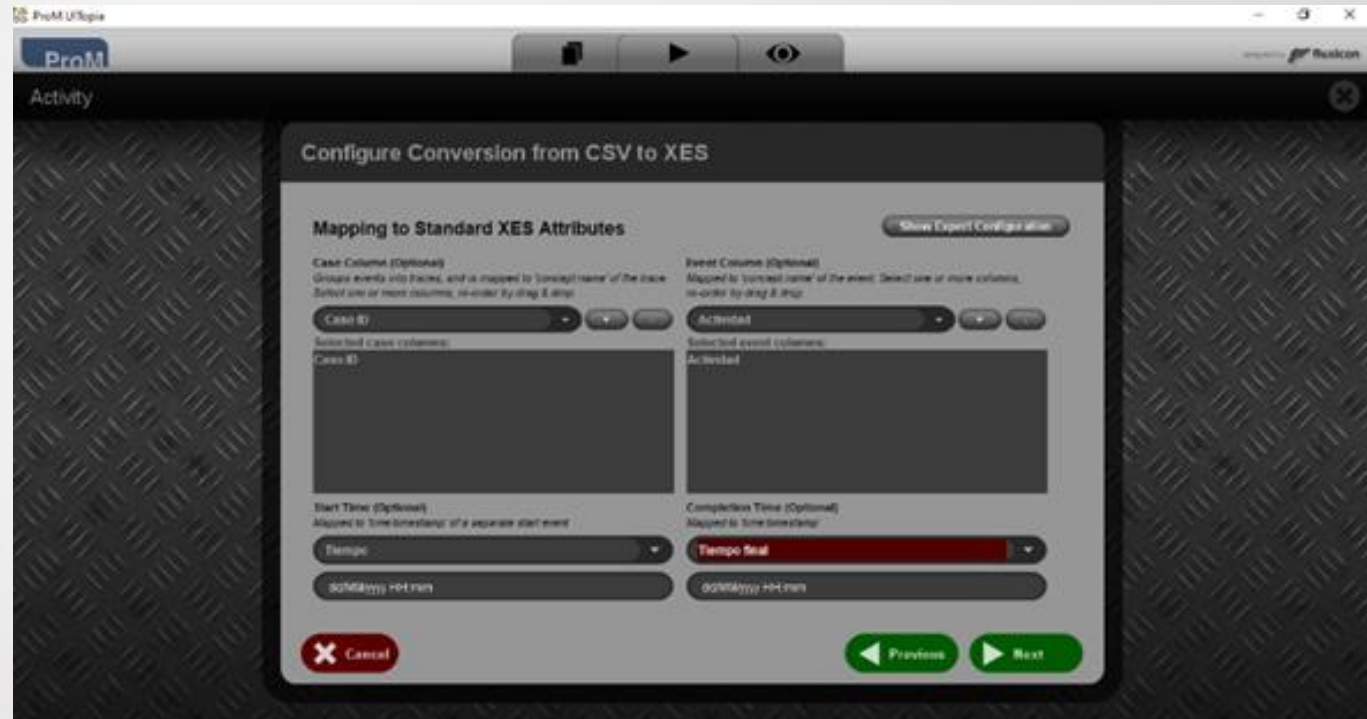


The screenshot shows the ProM Tools website. At the top, there is a search bar with the text "Search...". Below the search bar is the ProM logo, which consists of a blue rectangle with the word "ProM" in white and a yellow hard hat icon. Underneath the logo is the text "process mining workbench". A dark navigation bar contains the following links: "ProM Lite 1.3", "ProM 6.12", "ProM 6 nightly builds", "RapidProM", "ProM 5.2", "Documentation", and "Free online courses". Below the navigation bar, the main content area is titled "ProM Tools". It contains a paragraph of text: "Processes are an integral part of today's world, driving services and internal functionalities in businesses, governmental bodies, and organizations around the globe. While there are plenty of systems available for supporting the execution of such processes, the current practices for monitoring and analyzing this execution in the organizational reality still leaves a lot to be desired. **Process Mining** is able to fill that gap, providing revolutionary means for the analysis and monitoring of real-life processes." To the right of this text is another search bar with the text "Search" and a "Search" button. Below the search bar, there is a section titled "Windows" with two download buttons: "Download ProM Lite 1.3 with 64-bit JRE8" and "Download ProM Lite 1.3 with 32-bit JRE8".

Fuente: <https://promtools.org/>

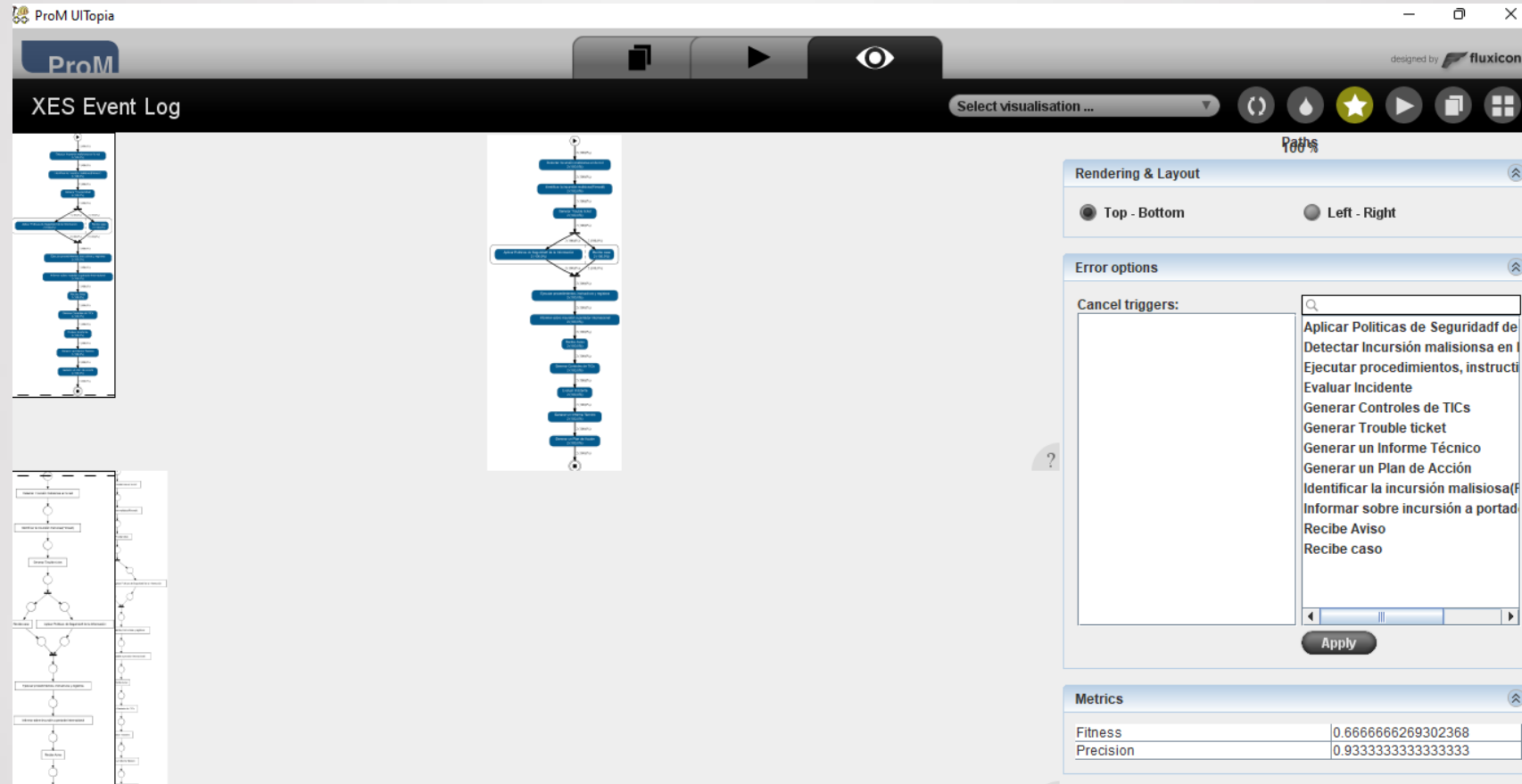
Metodología de la Investigación: Crear de Modelo Integrado

**Lifecycle model
for process
Mining.**

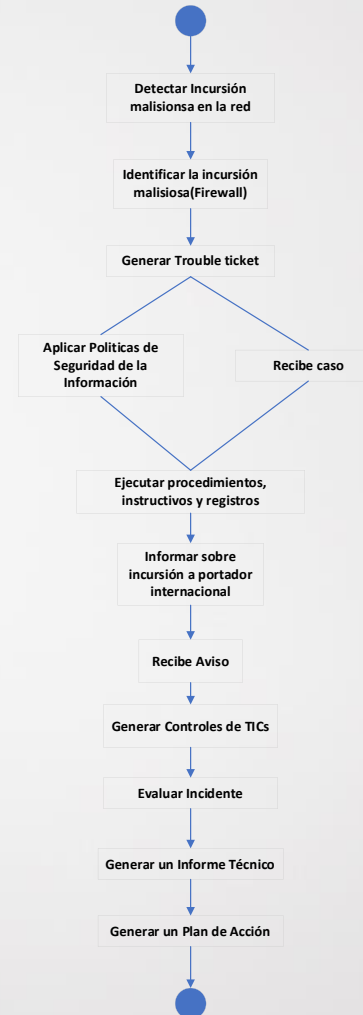


Fuente: Process Mining
de Van der Aalst, 1998,
pág. 284

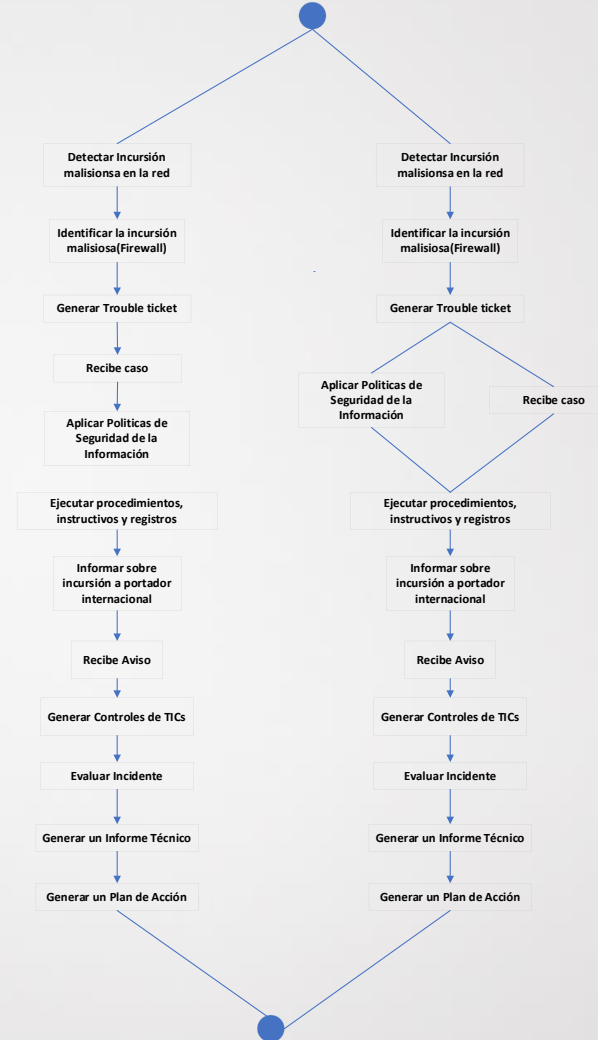
Metodología de la Investigación: Soporte Operativo y Desarrollo



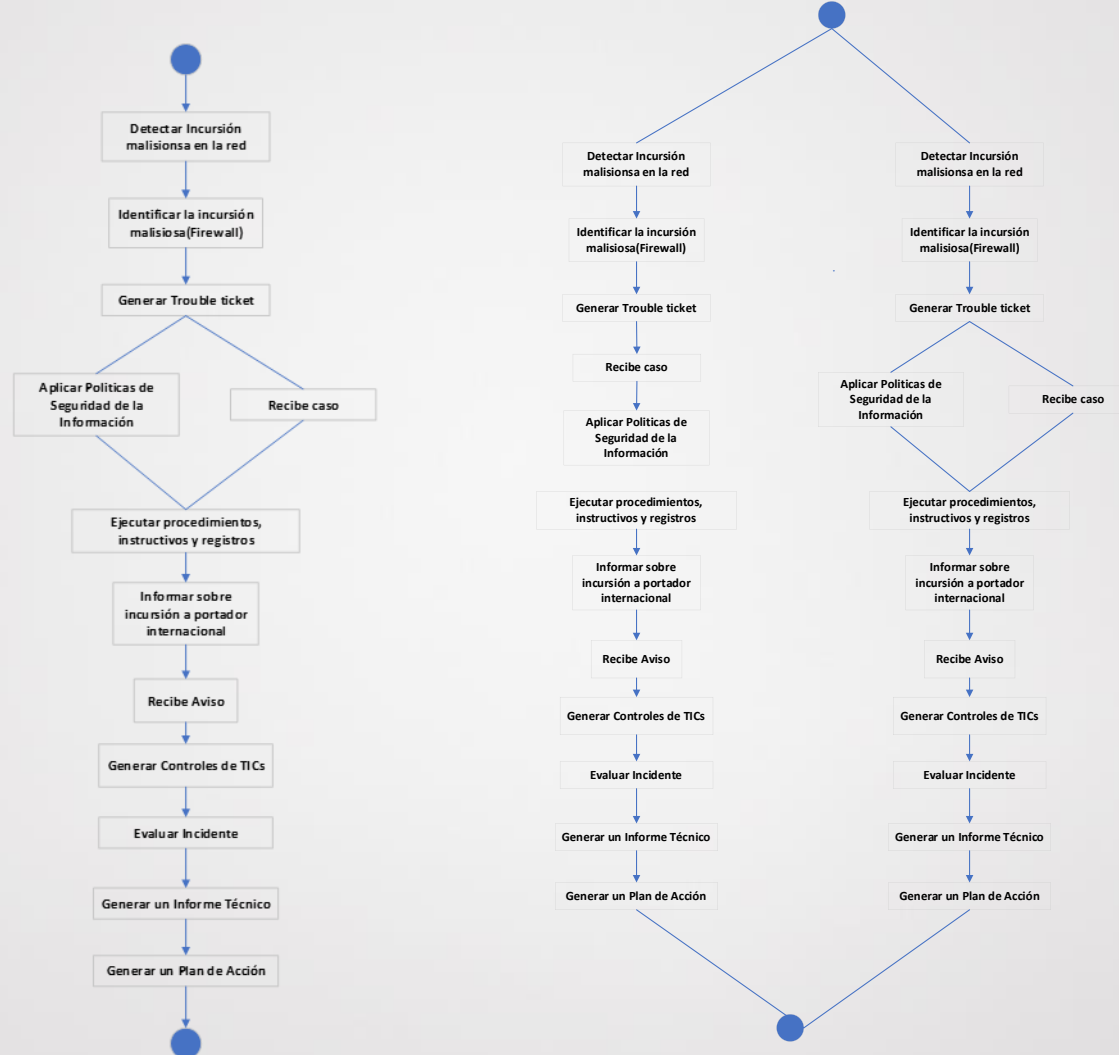
Metodología de la Investigación: Soporte Operativo



Metodología de la Investigación: Soporte Operativo



Resultados



ISO-27001

La Minería de
Procesos
esta
basada en
controles
de la
norma:

Política de seguridad de la información

**Organización de la seguridad de la
información**

**Gestión de incidentes de seguridad de
la información**

Operaciones de seguridad



Conclusiones



Mejora las condiciones para Decisiones gerenciales

ProM de libre acceso

Mejor relación Costo Beneficio

Objetivos claros con el Process Mining

Modelado de procesos en todas las áreas de la industria

Validación de la calidad de los procesos

ProM en constante actualización de plugings

Recomendaciones

- Ampliar el periodo de registro de eventos.
- Futuras investigaciones con otras fuentes de registros



