Buenas prácticas de los marcos de referencias para la creación de un SOC y los controles para tener en cuenta en empresas Mipymes de Bogotá

Laura Yisela Izquierdo Acevedo
Giovanni Mamanché Mamanché
Diego Arley Morales Ballesteros

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ D.C 2021

Tabla de Contenido

Tabla de Ilustraciones

1. INTRODUCCIÓN

En las MiPymes (micro, pequeñas y medianas empresas; que cuenta con un máximo de 200 empleados) [1], [2] la seguridad de la información y los datos deben ser una prioridad ya que hoy en día con el crecimiento en el uso de la tecnología y el acceso a internet, aumenta la posibilidad de enfrentar un mayor volumen de ataques cibernéticos. Esto conlleva a mayores riesgos y amenazas que pueden llegar a afectar la continuidad en la operación de la compañía.

Una de las mayores preocupaciones de las Mipymes al implementar un Centro de Operaciones de Seguridad (SOC), son los altos costos en los que puede incurrir. Sin embargo, la sustracción, modificación, suplantación, el daño en los equipos tecnológicos, la suspensión de la actividad del negocio durante un periodo de tiempo prolongado o el secuestro de la información, entre otras afectaciones que se pueden presentar, puede generar pérdidas económicas a mayores escalas. [3]–[5]

Según el Informe de tendencias del cibercrimen, en Bogotá se reportaron 5308 casos de delitos informáticos en el año 2019, de estos el 42 % corresponden a phishing, 28 % suplantación de identidad, 14 % envío de malware y 16 % fraude en medios de pago. Siendo las MiPymes uno de los principales focos de ataque de los cibercriminales. [6]

Dentro de las diferentes soluciones que hay para fortalecer las Mipymes en Bogotá ante los incidentes de seguridad se ha identificado que la implementación de un SOC genera unos excelentes resultados en este campo, para esto se hace necesario que tengan una herramienta que les permita identificar los controles de los marcos de referencia de ciberseguridad aplicables para la creación de un SOC. En el presente trabajo estaremos analizando los marcos de referencia NIST, normas como la ISO 27002. [7]

Con base en la problemática planteada se pretende el desarrollo de una herramienta en donde a partir de una información inicial suministrada por la empresa se hace la caracterización de esta, brindando una serie de recomendaciones que le permita reducir sus brechas de seguridad en la información.

En el presente trabajo encontraremos un primer capítulo donde se diseñará dos propuestas para la creación de un soc en las Mipymes en Bogotá, en el segundo capítulo se muestra de acuerdo a una selección previa los conocimientos y tareas que desempeñan cada uno de los roles del equipo del SOC, en el capítulo 3 se seleccionaron una serie de controles de la norma Iso 27002 que pueden aplicarse a las Mipymes de acuerdo a los resultados del formulario inicial diligenciado por la empresa, en el capítulo 4 se describe la herramienta diseñada con el fin de generar sugerencias para la creación del SOC, en el capítulo 5 se realizan pruebas de resultados a la herramienta desarrollada.

2. OBJETIVOS

2.1. Objetivo General

Generar una herramienta que permita realizar una propuesta para la creación de un SOC y los controles de seguridad que le aplican de acuerdo con su caracterización, utilizando los marcos de referencia de ciberseguridad NIST, ISO 27002 en las Mipymes en Bogotá.

2.2. Objetivo Específicos

- Proponer dos modelos de implementación del SOC de acuerdo con los tipos de empresas Mipymes en Bogotá.
- selección de tareas, conocimientos del marco de referencia NIST enfocados a un SOC.
- selección de controles de ciberseguridad aplicables para el SOC en las Mipymes de acuerdo con la ISO 27002.
- Desarrollar una herramienta que ayude en la definición del SOC más adecuado, el equipo de expertos y sus funciones al igual que los controles sugeridos para prevenir ataques informáticos dependiendo del tipo de empresa.

3. Capítulo 1.

3.1. Propuesta para la creación de un SOC en las Mipymes

un centro de operación de seguridad es un servicio/equipo de trabajo que funciona 24X7 con el objetivo de monitorear la red, infraestructura y servicios y de estos generar reportes haciendo uso de herramientas tecnológicas para identificar las de vulnerabilidades que se puedan tener ya sea internamente o de un cliente, de igual forma se requiere estar al día con las diferentes nuevas formas de ataques y patrones de ataques. Esta propuesta es muy importante en las Mipymes ya que con la creación de un SOC se previenen los ataques informáticos a los que pueden estar expuestas.

3.2. Beneficios de implementar un SOC en una Mipyme

La implementación de un SOC permite gestionar eficientemente los eventos e incidentes de Seguridad de la Información y Ciberseguridad, con el fin de prevenir y/o mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información, detallando las siguientes actividades.

- Investigar, analizar y monitorear las amenazas, eventos y los móviles de los incidentes de seguridad.
- Clasificar, categorizar, documentar y determinar el impacto de los eventos que se presenten.
- Aplicar de forma correcta los controles de los marcos de referencia de seguridad que se están implementando dentro de la organización.
- Realizar concientización a los usuarios en temas de seguridad.

- Mejorar los tiempos de identificación y gestión de los incidentes y eventos de seguridad.

3.3. Propuestas sugeridas para la creación de un SOC en las Mipymes

Una de las preguntas que las compañías se hacen cuando desean iniciar con un centro de operación en seguridad por primera vez es ¿cómo iniciar?

Teniendo en cuenta que las Mipymes son empresas en las que se cuentan con un rango de empleados que va desde un mínimo de 10 a un máximo de 250 empleados, en el presente trabajo se sugieren dos propuestas las cuales se pueden adaptar a las características propias de cada una de ellas.

Si se está formando un centro de operaciones desde cero en una Mipyme, se presentan los siguientes escenarios:

- Si el personal de la empresa es de máximo 10 personas se sugiere tercerizar las operaciones del SOC o implementar la propuesta de máximo un equipo de tres roles, para una operación 8x5 detallada en el presente trabajo.
- Si el personal de la empresa se encuentra en el rango entre 11 y 50 personas se sugiere implementar la propuesta de máximo un equipo de tres roles detallada en el presente trabajo, para una operación 8x5, si se requiere una operación más extendida se sugiere tercerizar el servicio para el tiempo faltante.
- Si el personal de la empresa se encuentra en el rango entre 51 y 250 personas se sugiere implementar la propuesta de un equipo de diez personas 4 roles detallada en el presente trabajo, para una operación 24x7.

Para el tipo de propuesta sugerida se requieren los siguientes roles:

- **Gerente SOC**: Experticia en planeación estratégica, priorización, contabilidad y trabajo en relación internas.
- **Analista de seguridad:** experticia en procesos operativos, inteligencia de riesgos, respuesta a incidentes, entre otros.

3.3.1. Propuesta de un equipo de 3 roles

Con un equipo de 3 personas se podría establecer un centro de operaciones de 8X5, este modelo de centro de operaciones requeriría mucha automatización y métricas de valor. esto también podría significar conseguir la ayuda de un tercero (Híbrido- aumento de personal o una suscripción basada en soluciones)

Ilustración 1 Equipo de 3 personas

Fuente: Elaboración Propia

Los integrantes del equipo serían:

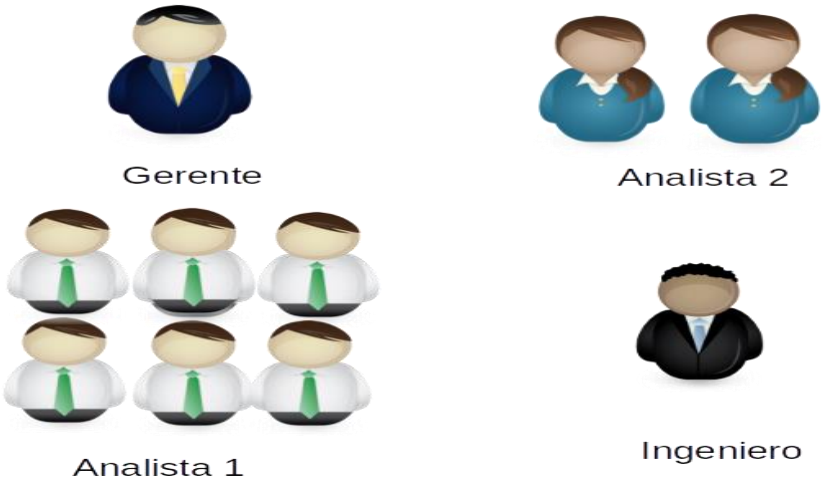
1 gerente, 1 analista nivel 1 y 1 analista nivel 2.

Operación 8X5 con automatización y centro de respuesta híbrido para monitoreo después de horas laborales.

3.3.2. Propuesta de un equipo de 10 personas con cuatro roles

Con un equipo de 10 personas y cuatro roles se podría establecer un centro de operaciones de 24x7, (este modelo de centro de operaciones requeriría menos automatización que el modelo anterior) y la implementación de sus respectivos indicadores de desempeño.

Ilustración 2 Equipo de 10 personas 4 roles



Fuente: Elaboración Propia

Los integrantes del equipo serían:

1 gerente, 6 analistas nivel 1, 2 analistas nivel 2, 1 ingeniero.

Operación 24X7 en instalaciones internas.

4. CAPÍTULO 2

4.1. Selección de roles y responsabilidades

Uno de los problemas más comunes dentro de los equipos del SOC se presenta cuando los miembros del equipo no tienen claro cuál es su rol y atado a este sus funciones, asumiendo de forma errada que una tarea no está bajo su responsabilidad lo cual puede generar una brecha de seguridad.

De acuerdo con las propuestas planteadas en el capítulo 1 respecto al tamaño de un SOC en las Mipymes en Bogotá a continuación se define cada uno de los roles planteados, basado en el marco de referencia NICE asignando las tareas y conocimientos a cada uno. [8]

- **Gerente**

Es el responsable de garantizar que los niveles de acuerdo de servicio, los objetivos del SOC, los indicadores de rendimiento, las políticas y procesos asociados se estén cumpliendo, esto a través del liderazgo eficiente del equipo de trabajo.

- **Analista de seguridad**

Es el encargado de llevar a cabo las tareas y procedimientos que se deben realizar diariamente, dentro de las cuales se encuentra identificar, categorizar, priorizar e investigar eventos rápidamente, así mismo documentar y responder los incidentes de seguridad identificados y velar por que todos los procedimientos relacionados al equipo de trabajo se lleven a cabo cumpliendo los indicadores de rendimiento en busca de la mejora continua.

- **Ingeniero(s) de Seguridad**

Un ingeniero de seguridad principalmente es responsable de llevar a cabo las tareas de configuración relacionados con la infraestructura de seguridad, tales

como firewall, antivirus, detección o prevención de intrusos y otras tecnologías, buscando la aplicación de las políticas de seguridad de la organización.

4.2. Marcos de referencia base para seleccionar los controles de seguridad aplicables en las Mipymes

Para el presente trabajo se analizarán como base los marcos de referencia NIST y la Iso 27002 de donde se seleccionan las tareas y conocimientos que se requieren para un equipo del SOC adicionalmente los controles aplicables de seguridad en las Mipymes de Bogotá.

Del marco de referencia NIST se seleccionaron las tareas y conocimientos que pueden ser aplicables al SOC en las dos propuestas planteadas para el presente trabajo de igual manera de este mismo marco y de la Iso 27000 se identificaron los controles de seguridad que se sugieren para este tipo de organizaciones.

4.3. Selección de Conocimientos, Tareas y habilidades bajo la NICE

Teniendo en cuenta los roles anteriormente especificados para los equipos de trabajo sugeridos para las Mipymes, tomamos como base de referencia el marco de la NICE para determinar cuáles son los conocimientos, tareas y habilidades que deben tener cada uno de ellos.

Realizamos un análisis a la lista Maestra de conocimientos, tareas para cada uno de los roles e identificamos cuáles de ellos son los que deberían tener para poder ejecutar sus actividades diarias y apoyar al equipo a continuación relacionamos los códigos que se encuentra en la tabla Maestra de la NICE[1]:

---

1. Anexo Tabla

Gerente

- Lista de códigos de Conocimiento asociados a este rol

CONOCIMIENTOS
K0001
K0002
K0003
K0004
K0005
K0006
K0066
K0612
K0613
K0614

- Lista de Tareas asociadas a este rol

TAREAS
T0003
T0029
T0930
T0032
T0066
T0188
T0384
T0865
T0866
T0869
T0870
T0871
T0872
T0873
T0875
T0876
T0880
T0881
T0882
T0885
T0888
T0895
T0897
T0898
T0902
T0905
T0911
T0912
T0915
T0916
T0917

Analista de seguridad

- Lista de códigos de Conocimiento asociados a este rol

CONOCIMIENTOS
K0001
K0003
K0004
K0005

K0006
K0016
K0020
K0025
K0031
K0056
K0060
K0065
K0083
K0129
K0229
K0049
K0093
K0179
K0203

K0260
K0261
K0262
K0266
K0275
K0276
K0281
K0284
K0002
K0018
K0040
K0044
K0075
K0263

- Lista de Tareas asociadas a este rol

TAREAS
T0068
T0195
T0342
T0347
T0349
T0351
T0366
T0381
T0382
T0385
T0403
T0404
T0023
T0043
T0088
T0155
T0164
T0166
T0178
T0187
T0198
T0214

T0258
T0259
T0260
T0290
T0291
T0292
T0293
T0294
T0295
T0296
T0297
T0298
T0299
T0310
T0332
T0469
T0470
T0475
T0503
T0504
T0526
T0545
T0548

Ingeniero de Seguridad

- Lista de códigos de Conocimiento asociados a este rol

Conocimientos
K0001
K0002
K0003
K0004
K0005
K0006
K0009
K0011
K0013
K0015
K0016
K0018
K0019
K0025
K0026
K0027
K0033
K0034
K0036
K0038
K0040
K0041
K0044
K0045
K0046
K0047
K0048
K0054
K0057
K0058
K0059
K0060
K0061
K0062
K0070
K0074
K0075
K0104
K0105
K0106
K0107
K0110
K0111
K0112
K0115
K0129
K0130
K0131
K0137
K0138
K0145
K0147
K0161
K0191
K0192
K0233
K0234
K0259
K0261
K0263
K0264
K0276
K0290
K0295
K0297
K0298
K0308
K0320
K0324
K0342
K0351
K0362
K0363
K0367
K0375
K0392
K0395
K0397
K0408
K0415
K0416
K0432
K0449
K0452
K0481
K0487
K0493
K0499
K0502
K0507
K0620
K0621
K0630
K0632

- Lista de Tareas asociadas a este rol

tareas
T0013
T0028
T0029
T0036
T0085
T0091
T0095
T0105
T0140
T0151
T0170
T0177
T0181
T0235
T0284
T0325

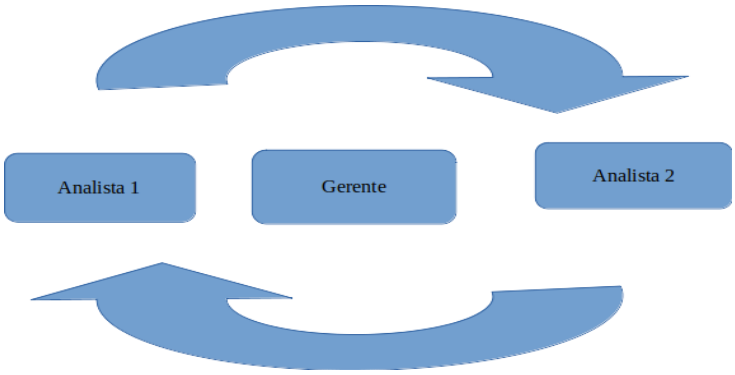
T0348	T0532	T0748
T0365	T0538	T0786
T0371	T0539	T0873
T0417	T0612	T0892
T0420	T0641	T0904
T0461	T0687	T0936
T0485	T0691	T0938
T0498	T0708	T0954
T0499	T0724	T0964
T0501	T0731	T0967

4.4. Modelo de Operación

De acuerdo con los modelos del SOC que se proponen en el capítulo 1 del presente trabajo en las Mipymes en Bogotá se realiza el analisis del modelo de operación de cada una de las propuestas y sus interacciones:

- **Equipo de SOC 3 personas:** el gerente es el líder del equipo el analista 2 tiene conocimientos más técnicos en comparación al analista 1 en donde el analista 2 dará apoyo al analista 1 en actividades que estén fuera de su experticia, se apoyan mutuamente en sus actividades diarias.

Ilustración 3 Interacción equipo de 3

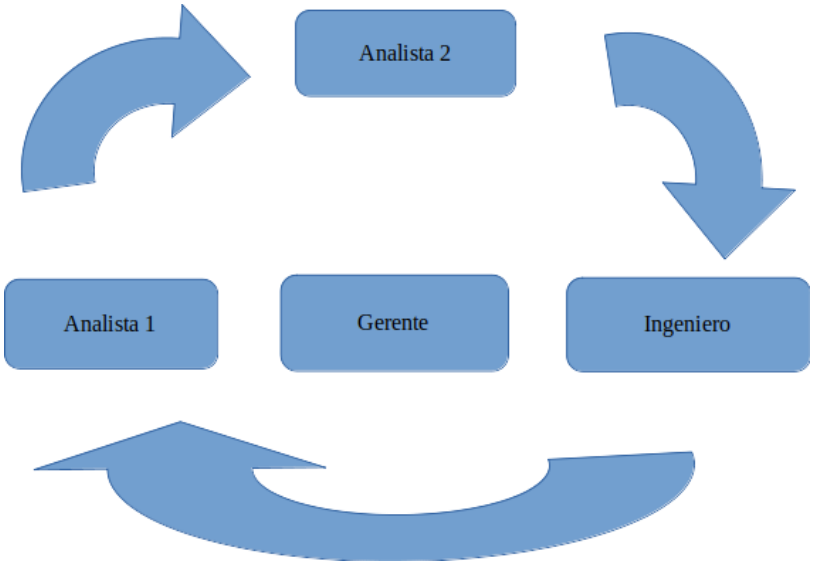


Fuente: Elaboración Propia

- **Para el equipo del SOC de 10 personas**: se sugiere el siguiente modelo de operación con sus interacciones:

Entre el analista 1 y el 2 y gerente aplica el mismo concepto del modelo anterior con la diferencia que entra un nuevo rol de ingeniero de seguridad en donde este apoyara a los analistas con nuevas definiciones en reglas de seguridad y solución de incidentes de alta complejidad.

Ilustración 4 Interacción equipo de 10 personas 4 roles



Fuente: Elaboración Propia

4.5. Indicadores de Desempeño

Los indicadores de desempeño permiten al equipo del SOC verificar y medir la capacidad de respuesta que se tiene frente a los incidentes o eventos de seguridad que se están presentado, cuáles son los tipos de incidentes más frecuentes y usuarios que más reportes hacen

En donde se definen las siguientes variables y estados para cada una de ellas

- Cantidad de casos: Corresponde a todos los incidentes reportados por los usuarios en un periodo de tiempo determinado.
- Estado: Corresponde en que parte del proceso se encuentra un incidente para dar solución (Radicado, Asignado, En curso, Pendiente, Resuelto, Solucionado, Cancelado, Rechazado)
- Severidad: Corresponde al nivel que se ve comprometido el sistema, o el reporte de incidente (Critica, Alto, Medio, Bajo)
- categoría de eventos: Corresponde a la tipología del evento que se está reportando (Correo Malicioso, IP maliciosas, Ip Publicas, Url sospechosas entre otras)
- Cierre de casos: Corresponde al número de casos que se les brindó atención.
- Tiempo de Solución: Corresponde a cuánto tiempo transcurrió entre la apertura y el cierre.

A continuación, se sugieren algunos indicadores que se pueden manejar y queda a definición de la compañía los rangos de cumplimiento para cada uno:

- Cantidad de casos por estado
- casos mensuales por severidad

- casos mensuales por categoría de eventos
- Números de casos cerrados por mes
- tiempo de solución por severidad mensual

5. CAPÍTULO 3

5.1. Selección de controles aplicables para las Mipymes según los marcos de referencia

Para la selección de los controles aplicables para los procesos del SOC se verificaron los marcos de referencia de la Nist y la Iso 27002, se procede a escoger los controles de acuerdo con las preguntas formuladas inicialmente en el formulario de ingreso para conocer sobre la información de la empresa, la identificación de sus activos y los niveles de seguridad de las Mipymes

En la siguiente tabla relacionamos los controles seleccionados de acuerdo con el análisis realizado de los marcos de referencia que aplican para el SOC en las Mipymes:

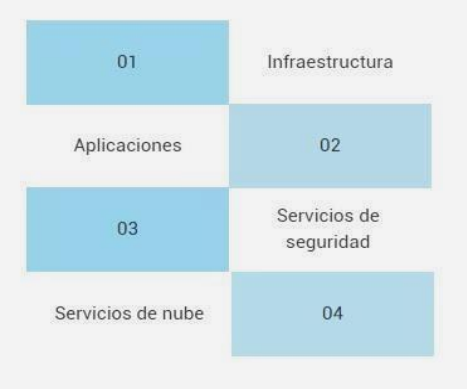
Controles seleccionados	
13.2.3	6.1.4
12.2.1	7.2.2
14.1.1	12.6.1 16.2.1
6.2.1	11.2
6.2.2	13.1

5.2. Infraestructura tecnológica de seguridad

La infraestructura tecnológica hace referencia a los equipos, aplicaciones y servicios de seguridad que sirven como fuentes de información para el análisis de los eventos que se presenten dentro de la compañía de forma externa o interna, con estas herramientas que se detallaran en este capítulo les permitirá mitigar o contener los ataques informáticos.

Las principales fuentes de información para análisis son:

Ilustración 5 Fuentes de información



Fuente: Elaboración Propia

A continuación, se da a conocer algunas de las características de software que se debe adquirir ya sea opensource o licenciado para el análisis de eventos.

Antivirus: aplicación para proteger los computadores de software malicioso como virus, troyanos, gusanos entre otros. Este se instala de forma local en los equipos de cómputo, la identificación de las amenazas se realiza mediante firmas en el código (Bloques de código ya identificados como malicioso) para así poder contenerlo.

EDR: endpoint detection response, es un tipo de antivirus más avanzado, integra la funcionalidad de detección de amenazas, pero adiciona un componente de inteligencia artificial que permite determinar si un archivo puede ser potencialmente malicioso con el fin de contenerlo o eliminarlo. Los ERD a diferencia de los antivirus, pueden hacer análisis de los equipos dentro de la red, dando mayor alcance a la protección dentro de una organización.

Monitores de archivos: Aplicaciones que validan los cambios que se han hecho sobre archivos, esto se realiza mediante las verificaciones de

hashes con el fin de evaluar si el archivo ha tenido algún cambio; de igual forma llevar control de quien lo ha modificado y cuando fue su última modificación.

sistema de detección de intrusos: Los sistemas de detección de intrusos o IPS, son herramientas que validan los activos de información y la red con el fin de identificar tráfico anómalo dentro de esta y alertar sobre estas anomalías cuando se presenten.

Monitores de Red y Hardware: Aplicación que se encargue de monitorear si hay problemas dentro de la red tanto de dispositivos de hardware (espacio en disco, uso de memoria, uso de procesador, etc.) como software, al igual que monitoreo de servicios de protocolos. El sistema dará alerta cuando alguno de ellos no tenga el funcionamiento correcto según la parametrización que se le haya dado.

Sistema de gestión de eventos (SIEM): Una herramienta que recopila los logs de sistemas externos, como logs de sistema operativo, del monitor de red, IDS, IPS, etc., y otorga información sobre posibles amenazas dentro de la organización.

6. Capítulo 4

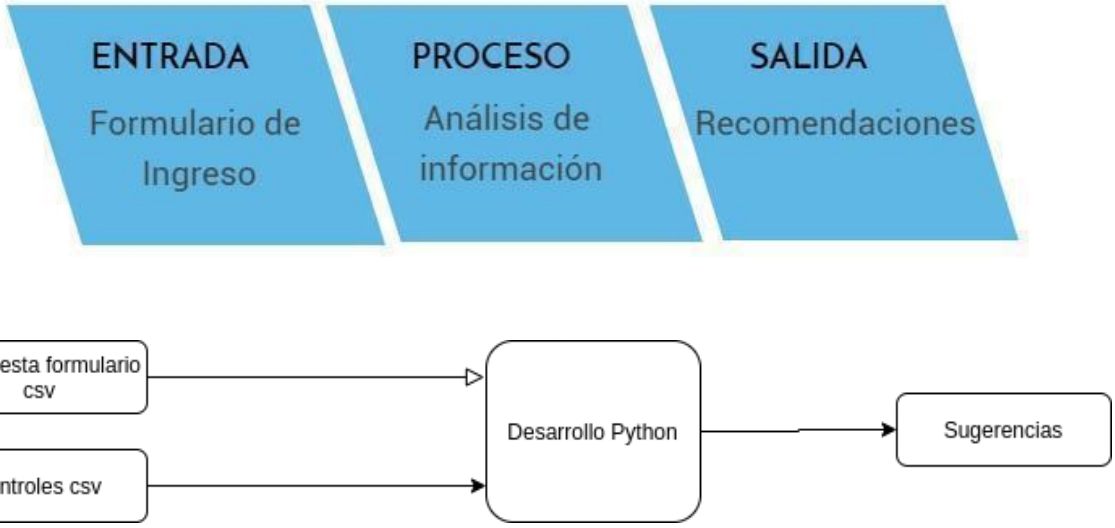
6.1. Nombre de la herramienta

Consideraciones generales para la creación de un SOC en una Mipyme

6.2. Descripción de la Herramienta

A través de la herramienta se busca proveer un apoyo a las empresas en la creación de un SOC y de los controles de seguridad que se pueden aplicar en la organización mediante una aplicación desarrollada en Python, las cual carga un archivo csv con las respuestas suministradas por el usuario y otro con los controles.

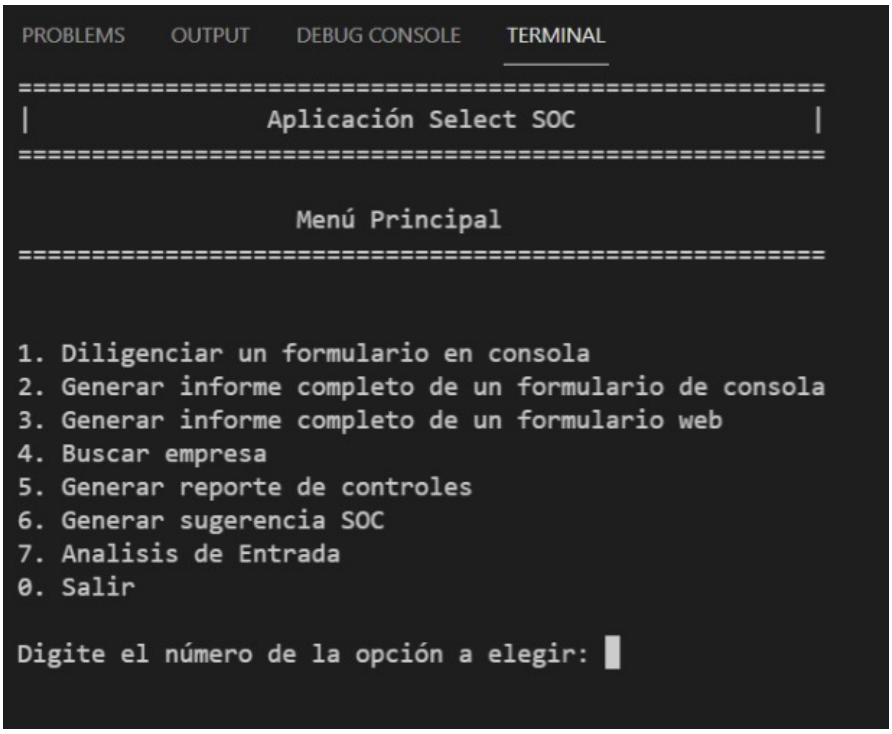
Ilustración 6 Flujo de Herramienta

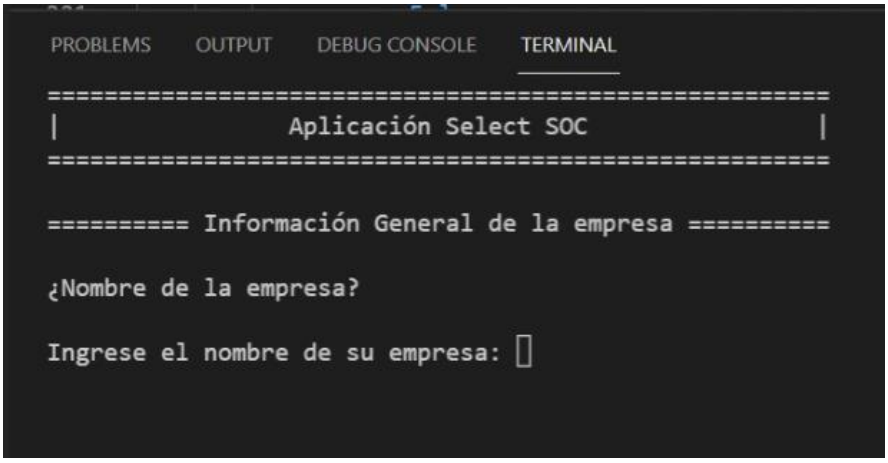


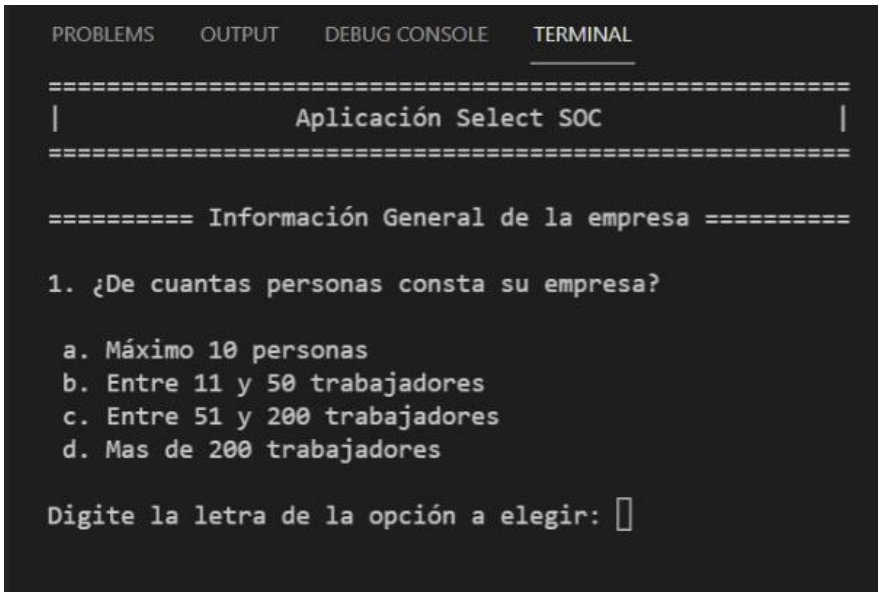
Fuente: Elaboración Propia

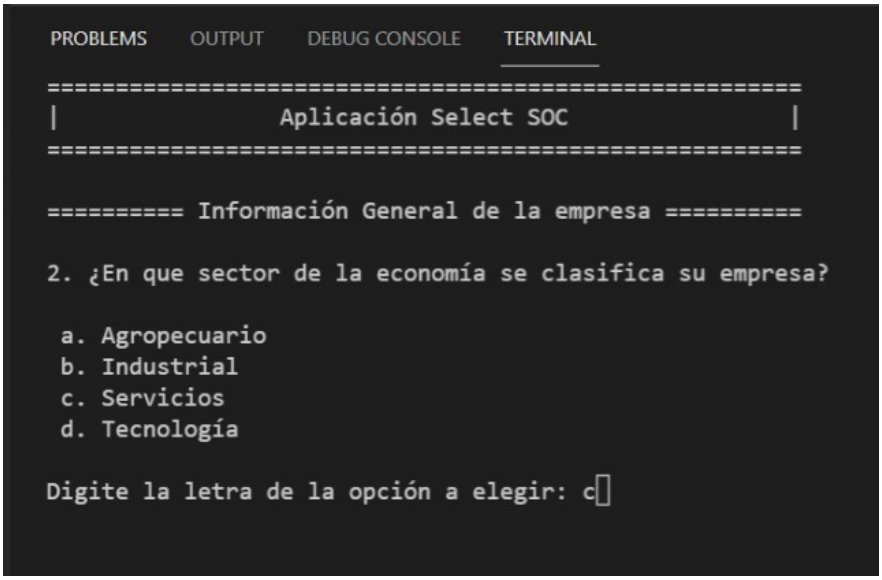
Se realiza una encuesta a el empleado(s) de la empresa en donde se realizan preguntas referentes a la organización y del diario actuar de estos en relación con las tecnologías (cantidad de personas que laboran dentro de la empresa, partes involucradas, en qué sector de la economía está, cuáles son los servicios que tiene o presta y que canales de comunicación maneja con los clientes)

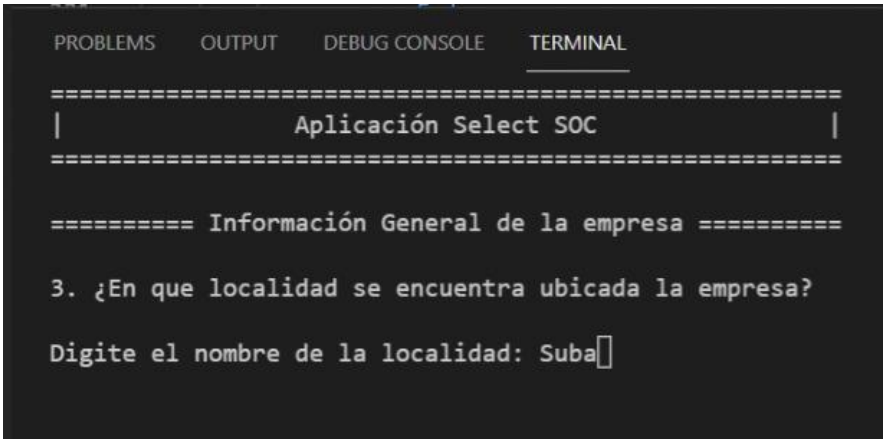
Ilustración 7 Formulario de ingreso

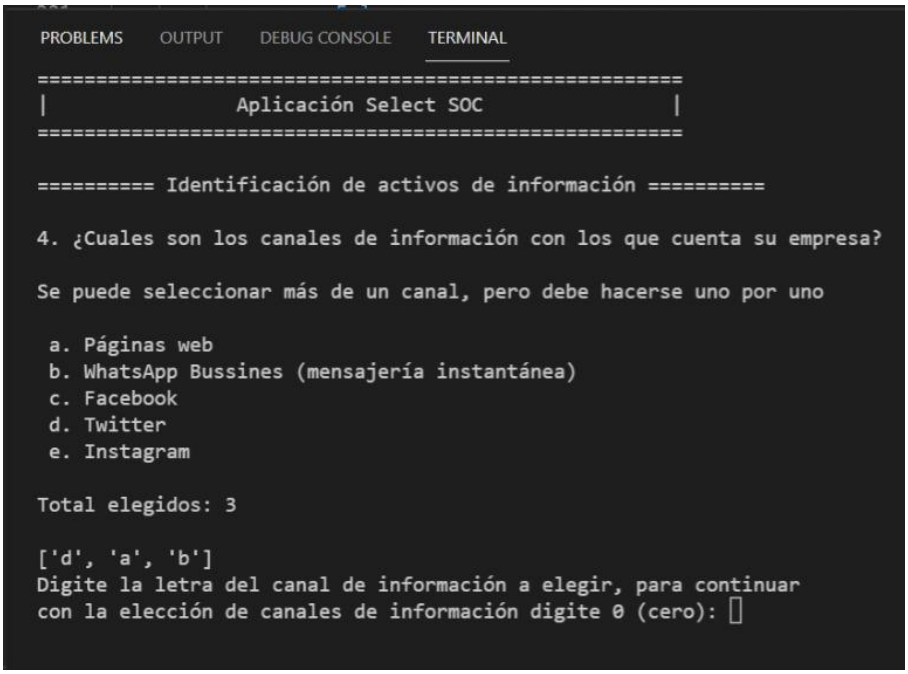


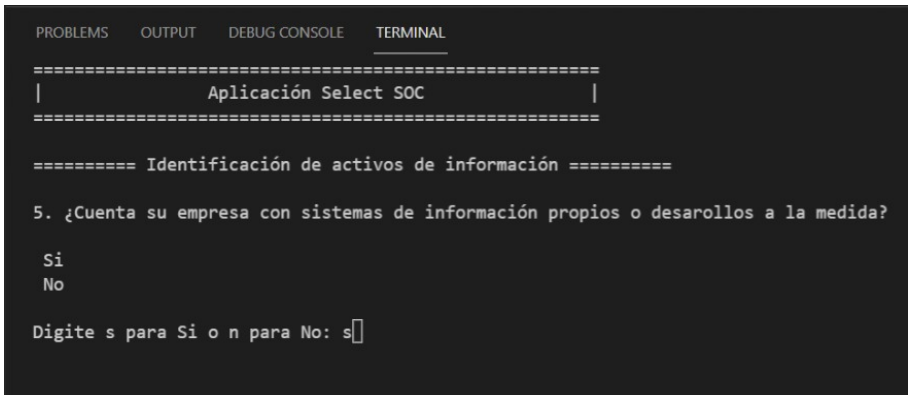


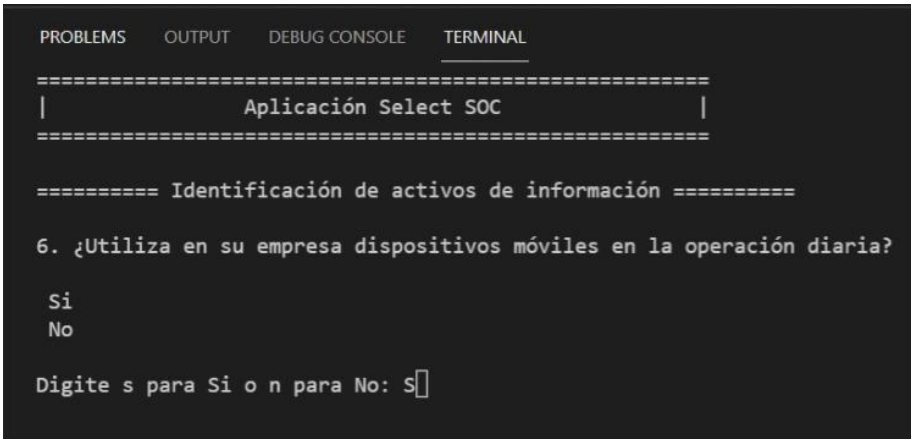

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Aplicación Select SOC
Información General de la empresa
1. ¿De cuantas personas consta su empresa?
a. Máximo 10 personas
b. Entre 11 y 50 trabajadores
c. Entre 51 y 200 trabajadores
d. Mas de 200 trabajadores
Digite la letra de la opción a elegir:

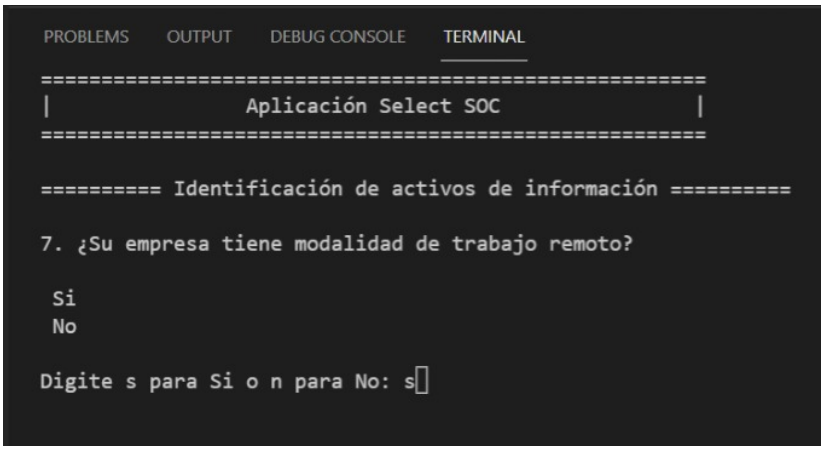

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Aplicación Select SOC
Información General de la empresa
2. ¿En que sector de la economía se clasifica su empresa?
a. Agropecuario
b. Industrial
c. Servicios
d. Tecnología
Digite la letra de la opción a elegir: c

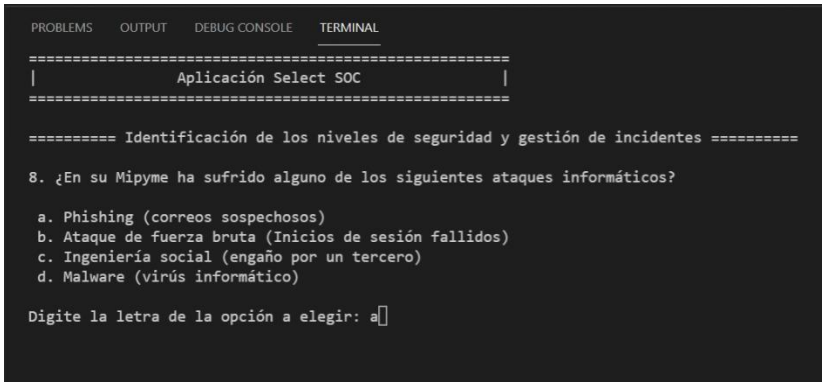

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Aplicación Select SOC
Información General de la empresa
3. ¿En que localidad se encuentra ubicada la empresa?
Digite el nombre de la localidad: Suba

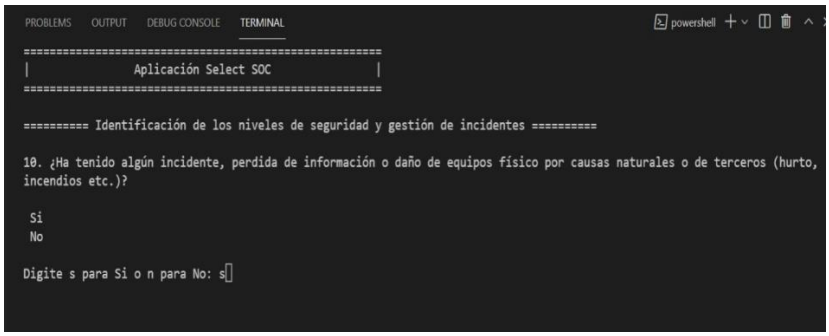

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
| Aplicación Select SOC |
========== Identificación de activos de información ==========
4. ¿Cuales son los canales de información con los que cuenta su empresa?
Se puede seleccionar más de un canal, pero debe hacerse uno por uno
a. Páginas web
b. WhatsApp Bussines (mensajería instantánea)
c. Facebook
d. Twitter
e. Instagram
Total elegidos: 3
['d', 'a', 'b']
Digite la letra del canal de información a elegir, para continuar
con la elección de canales de información digite 0 (cero):

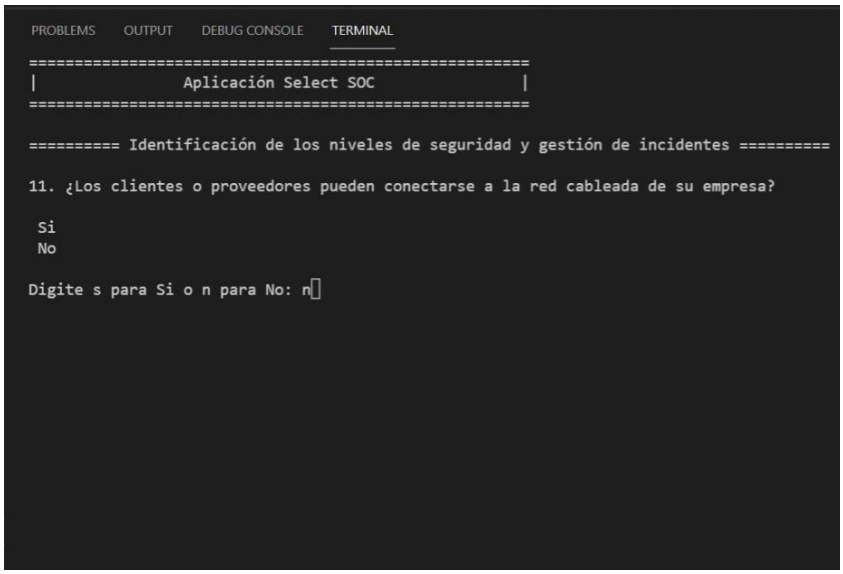

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
| Aplicación Select SOC |
========== Identificación de activos de información ==========
5. ¿Cuenta su empresa con sistemas de información propios o desarollos a la medida?
Si
No
Digite s para Si o n para No: s


PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
| Aplicación Select SOC |
========== Identificación de activos de información ==========
6. ¿Utiliza en su empresa dispositivos móviles en la operación diaria?
Si
No
Digite s para Si o n para No: S


PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
Aplicación Select SOC
========== Identificación de activos de información ==========
7. ¿Su empresa tiene modalidad de trabajo remoto?
Si
No
Digite s para Si o n para No: s


PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
Aplicación Select SOC
========== Identificación de los niveles de seguridad y gestión de incidentes ==========
8. ¿En su Mipyme ha sufrido alguno de los siguientes ataques informáticos?
a. Phishing (correos sospechosos)
b. Ataque de fuerza bruta (Inicios de sesión fallidos)
c. Ingeniería social (engaño por un tercero)
d. Malware (virús informático)
Digite la letra de la opción a elegir: a


PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
powershell
Aplicación Select SOC
========== Identificación de los niveles de seguridad y gestión de incidentes ==========
10. ¿Ha tenido algún incidente, perdida de información o daño de equipos físico por causas naturales o de terceros (hurto, incendios etc.)?
Si
No
Digite s para Si o n para No: s



Fuente: Elaboración Propia

El proceso de análisis y caracterización se toma como fuente de información la encuesta, donde las respuestas son cargadas automáticamente a una hoja de cálculo tras finalizar la encuesta.
La hoja de cálculo con las respuestas se exporta como un archivo plano delimitado por comas (CSV) que será una de las entradas de información para el programa.

Otra fuente de información será los controles seleccionados de la norma iso 27002 y NIST

La herramienta se desarrolla en el lenguaje de programación Python, en donde se usa la librería panda para cargar los archivos CSV, la librería sklearn la cual es una herramienta de aprendizaje automático (Machine Learning) que nos permite hacer análisis predictivo con los datos cargados y graficar dicha información.

Posterior al cargue de la información la aplicación sugiere el mínimo requerido en personal para el soc y controles de seguridad, el análisis de

la información se realiza comparando palabras del archivo CSV de la encuesta y dependiendo de esta, tomamos los controles aplicables del archivo CSV que contiene los controles.

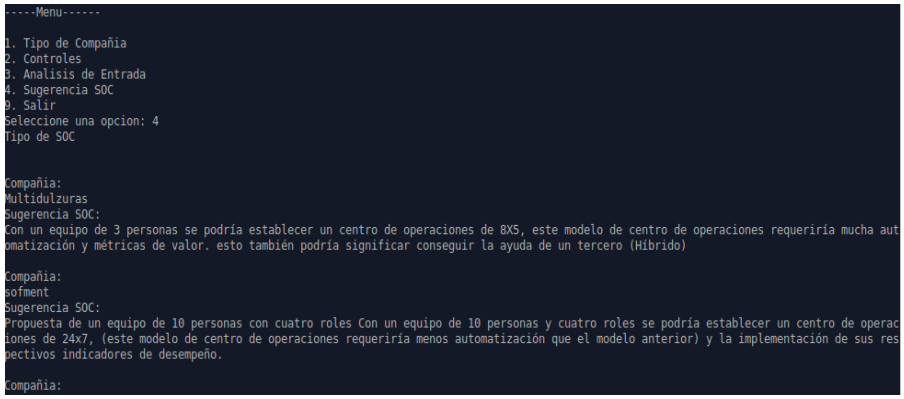
El desarrollo de esta herramienta les permitirá a las Mipymes tener en consideración aspectos relevantes para la creación de un SOC y así mismo poder establecer los controles de seguridad específicos de acuerdo con las características de la empresa, cabe aclarar que son sugerencias y no se está obligado a su implementación, sin embargo, poner en práctica estos controles ayuda a reducir los impactos en fallas de seguridad y ataques informáticos.

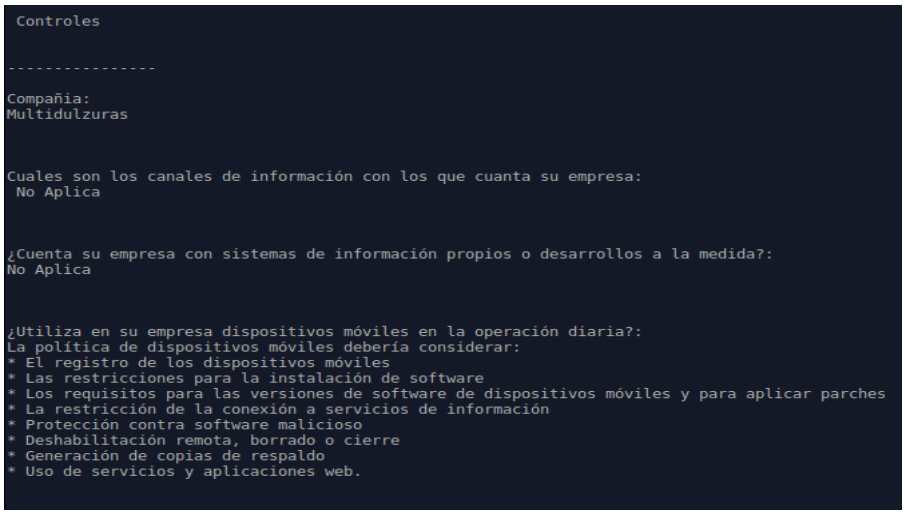
7. CAPÍTULO 5

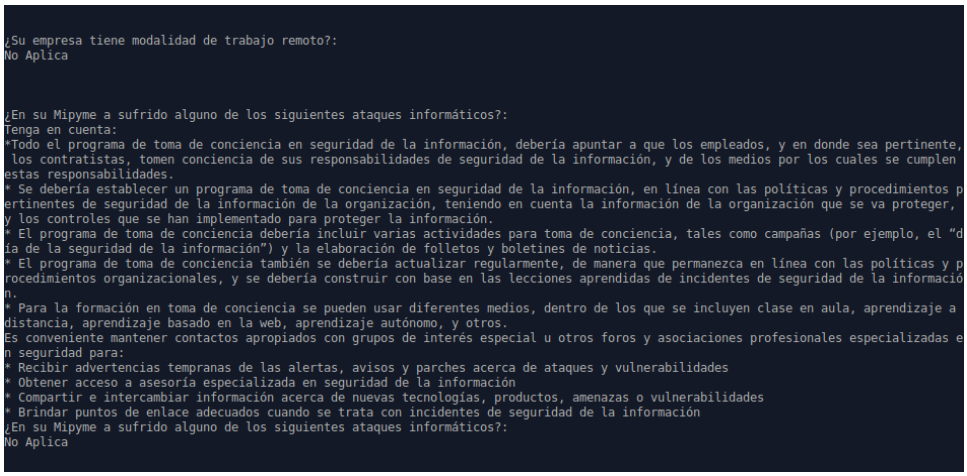
7.1. Análisis de resultados

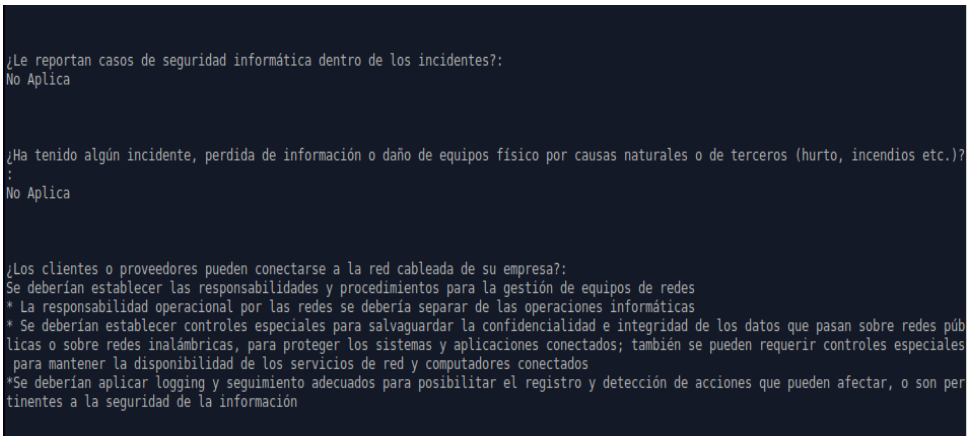
De acuerdo con la herramienta propuesta se realiza un ejercicio donde se diligencia el formulario de ingreso a través de la consola de la aplicación, finalizado el diligenciamiento de la información se procede a hacer la determinación del SOC y dependiendo las respuestas ingresadas en el formulario se indica cuáles son los controles que aplican para la organización.

Ilustración 8 Prueba de resultados









Fuente: Elaboración Propia

8. Conclusiones

- Se diseñaron dos propuestas del SOC para las Mipymes de Bogotá de acuerdo con la cantidad de empleados que manejan, cada una de estas propuestas nos muestran los roles y el número de personas que pueden aplicar para un SOC de acuerdo con la organización.
- Se realiza el análisis del marco de referencia NICE para extraer los conocimientos que debe tener el especialista y las tareas a desempeñar de cada uno de los roles dentro del equipo SOC.
- Se realiza el análisis de la norma Iso 27002 para identificar los controles que pueden aplicarse al SOC de una Mipyme en Bogotá.
- Con base en el análisis realizado en el presente trabajo se diseñó una herramienta que permite a una empresa Mipyme ingresar información por medio de un formulario la cual posteriormente analizara e indicara el tamaño de SOC más adecuado para la organización, las tareas y conocimientos que deben tener los diferentes roles que hacen parte de este y se sugiere los controles a implementar.

9. Anexos

- Supplement_nice_specialty_areas_and_work_role_ksas_and_task (hoja Master KSA List, Master Task List)

10. Referencias Bibliográficas

[1] "Dinámica empresarial - Observatorio - Cámara de Comercio de Bogotá." https://www.ccb.org.co/observatorio/Dinamica-Empresarial/Dinamica-empresarial (accessed Sep. 13, 2021).

[2] "LEY 590 DE 2000." http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1663080 (accessed Sep. 20, 2021).

[3] "Aumenta en 30% la inversión de las Pymes en ciberseguridad | ACIS." https://acis.org.co/portal/content/NoticiaDelSector/aumenta-en-30-la-inversi%C3%B3n-de-las-pymes-en-ciberseguridad (accessed Sep. 27, 2021).

[4] "Costos asociados a la pérdida de información en las empresas." https://destinonegocio.com/co/economia-co/costos-asociados-perdida-informacion-en-las-empresas/ (accessed Sep. 27, 2021).

[5] "¿Cuánto le cuesta a su empresa un ataque de ciberseguridad?" https://www.netec.com/post/cu%C3%A1nto-le-cuesta-a-su-empresa-un-ataque-de-ciberseguridad (accessed Sep. 27, 2021).

[6] "Tendencias." https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf (accessed Oct. 29, 2021).

[7] "¿Por qué incorporar un SOC a tu empresa? Los nuevos desafíos de una vida en la nube." https://www.nordsterntech.com/post/incorporar-un-soc-a-tu-empresa (accessed Sep. 27, 2021).

[8] "supplement_nice_specialty_areas_and_work_role_ksas_and_tasks - Buscar con Google." https://www.google.com/search?q=supplement_nice_specialty_areas_and_work_role_ksas_and_tasks&oq=supplement_nice_specialty_areas_and_work_role_ksas_and_tasks&aqs=chrome..69i57j69i61.3459j0j15&sourceid=chrome&ie=UTF-8 (accessed Nov. 07, 2021).