ESQUEMA DE ASEGURAMIENTO PROACTIVO A TRAVÉS DEL USO DE INTELIGENCIA DE AMENAZAS PARA UNA EMPRESA DE CONTACT CENTER

Leidy Bayona, Edward J. Sarmiento, Sandra Milena Huerfano
Estudiantes Maestría en Seguridad de la Información
Departamento de Ingeniería de Sistemas y Computación
Universidad de los Andes, Bogotá, Colombia
Diciembre 2020

---

1. Introducción

Los ataques cibernéticos a nivel mundial han aumentado con el paso del tiempo, ocasionando significativas pérdidas económicas, de reputación y tecnológicas en industrias de todos los sectores y tamaños. De acuerdo con el reporte publicado por el equipo de X-Force IRIS de IBM - 2020 (IBM, 2020) "más de 8.500 millones de registros se vieron comprometidos en 2019, una cifra que es más del 200 por ciento mayor que la cantidad de registros perdidos en 2018, debido a servidores mal configurados (incluido el almacenamiento en la nube de acceso público, las bases de datos en la nube sin asegurar y las copias de seguridad de rsync protegidas incorrectamente o los dispositivos de almacenamiento de área de red conectados a Internet abiertos) lo que representó el 86 por ciento de los registros comprometidos en 2019".

A través del reporte de Mandiant – Fireye 2020 (Report, Deep Dive Into Cyber Reality Security Effectiveness Report, 2020), se identificó que:

- El 53% de los ataques no fueron prevenidos o detectados.
- Únicamente se generaron alertas del 9% de los ataques.
- En el 68% del tiempo de operación de las compañías, los controles desplegados no lograron prevenir o detectar ataques de Ransomware.
- En el 48% de los eventos, los controles desplegados no pudieron prevenir o detectar los ataques en algunas de sus etapas.
- En el 67% de los incidentes, las técnicas y tácticas de exfiltración fueron exitosas.

En cuanto a las cifras de ataques para las cadenas de suministros registrados en Colombia según la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) para el 2019 (Colombia, 2019 - 2020), se registraron las siguientes estadísticas:

- 54% de incremento en el número de incidentes, con respecto al 2018
- 80% de correos fraudulentos personalizados (spear phishing)
- 7994 casos reportados por acceso abusivo a sistema informático
- 2387 casos reportados como uso de software malicioso
- 37% en infección de sitios
- 30% de los ataques de Ransomware han sido dirigidos a Colombia a nivel Latinoamérica
- 612% crecimiento en los ataques de Malware
- 170 empresas reportaron ataques DDoS que consiguieron interrumpir sus servicios de cara a sus clientes

Debido al aumento de los ataques anteriormente mencionados, se ve la necesidad de reforzar los esfuerzos de los equipos de seguridad de la información en una defensa proactiva por medio del uso de inteligencia de amenazas, lo que según los estudios realizados por la firma IDC (Future, 2018) permitirá:

- Que los equipos de seguridad de TI sean 32% más eficientes
- Recuperación del retorno de inversión en un corto periodo de tiempo
- Identificación de amenazas 10 veces más rápido
- Detección del 22% de las amenazas antes de que impacten al negocio
- 86% menos de indisponibilidad
- Una significativa disminución en sanciones o multas por incumplimiento.

La inteligencia de amenazas ayuda a las empresas a detectar y analizar ciberamenazas de manera oportuna, permitiendo la gestión proactiva para la mitigación de estas, lo que la convierte en una "parte fundamental de cualquier ecosistema de defensa" (amenazas, 2020), brindando un contexto que ayuda a las empresas a tomar decisiones sobre el estado de su seguridad a través de la identificación de tácticas y técnicas usadas por los atacantes.

Por otro lado, los atacantes han detectado que comprometer a compañías de Contact Center que centralizan información de otros sectores como: financiero, aseguradoras, retail, telecomunicaciones, entre otros, puede llegar a resultar más lucrativo que el ataque directo a las empresas de alto valor por la relación de confianza establecida entre ellas, generando un nuevo vector de ataque. La ilustración 1, muestra los sectores afectados mediante un informe de reporte de costos de brechas (IBM, 2020).

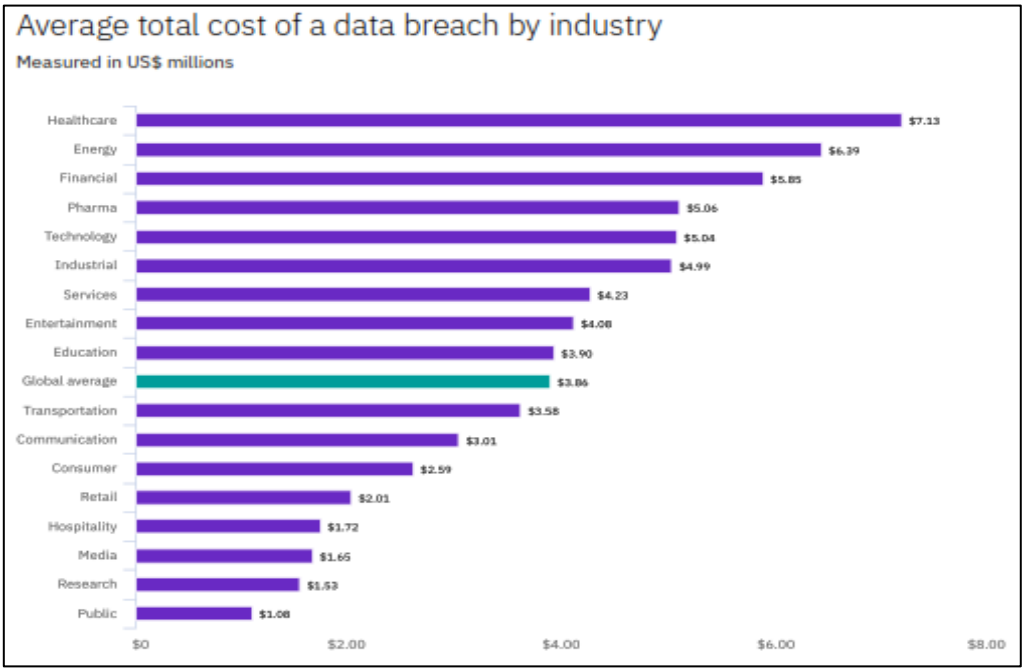

Ilustración 1 Costo promedio por brecha de datos por industria (IBM, 2020)

De acuerdo con el informe de TRUSID (TRUSID, 2019) "los Contact Center son los enlaces más débiles en la cadena de autenticación", por lo que los ciberdelincuentes están dirigiendo sus ataques a este tipo de compañías ya que cuentan con información confidencial de clientes. TRUSID indica que "Los centros de llamadas son ahora el vector de elección para ataques criminales. Este año, el 51% de los encuestados de la industria de servicios financieros y el 32% de todos los encuestados reconocieron el canal telefónico como la fuente principal de ataques".

La CISA (CISA, 2020) publicó un artículo alertando sobre las posibles amenazas a las que se exponen los centros de comunicaciones, como por ejemplo los ataques de denegación de servicio de telefonía (TDoS). Tal como lo menciona la empresa SecureLogix (Securelogix, 2020), “el objetivo de este tipo de ataques es realizar una cantidad significativa de llamadas y mantener esas llamadas activas durante el mayor tiempo posible, para abrumar o al menos "obstruir" todo o una parte del sistema de voz de la víctima. Esto puede incluir circuitos troncales, teléfonos de emergencia, asistentes / agentes, un sistema de respuesta de voz interactiva (IVR), números de teléfono específicos o algún otro punto de estrangulamiento”.

1.1 Identificación del Problema

Se ha identificado que el sector de Contact Center enfoque de este estudio, aborda la toma de acciones frente a las nuevas amenazas y vulnerabilidades de forma reactiva, aplicando las medidas y controles tradicionales sin tomar en cuenta la evolución de las nuevas amenazas y vectores de ataque, que pueden impactar a su propio sector y a los clientes a los que presta sus servicios.

El proceso habitual inicia con la búsqueda manual de información de inteligencia de amenazas en diferentes fuentes, verificando indicadores de compromiso (IoC) de fuentes públicas abiertas que no siempre son confiables y precisas, lo que consume un alto tiempo de las áreas de seguridad de la información en realizar este tipo de búsqueda, análisis, toma de decisión y gestión interna con las demás áreas.

1.2 Propuesta de Solución

Este trabajo propone un esquema proactivo basado en el modelamiento de procesos de seguridad en inteligencia de amenazas, apoyado en el uso de herramientas de código abierto que permiten la gestión de nuevos vectores de ataque en ciberseguridad, en conjunto con el análisis realizado por los integrantes del equipo de seguridad, para una adecuada implementación tecnológica como se muestra en la Ilustración 2.

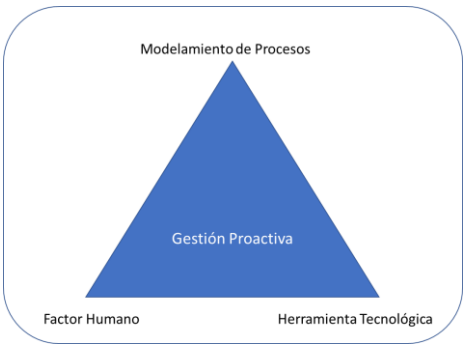

Ilustración 2 Propuesta de solución

2. Diseño del esquema de gestión proactiva

2.1 Modelamiento del proceso y herramientas tecnológicas

El ciclo de inteligencia de amenazas es un proceso continuo de cinco pasos llevado a cabo por equipos de seguridad de la información, para proporcionar a las áreas interesadas, información relevante y oportuna de amenazas, vulnerabilidades y actores maliciosos, buscando la reducción del riesgo de materialización de un ataque. Los cinco pasos son: dirección y planeación, recolección y procesamiento, análisis y producción, difusión y retroalimentación.

- *Planificación y dirección*: En este paso, los equipos definen el propósito y los objetivos de una operación de inteligencia, conocidos como requisitos prioritarios de inteligencia (de sus siglas

en inglés (*Priority Intelligence Requirements - PIR*). Los PIR reflejan lo que un equipo de inteligencia necesita identificar para satisfacer el propósito de la operación.

Para el objetivo de este proyecto, se definieron los siguientes PIR:

Requisitos prioritarios de inteligencia (PIR)	**Condiciones por cumplir**	**Actividades relacionadas**	**Proceso de Inteligencia**
Investigar y notificar sobre vulnerabilidades que puedan afectar a los activos críticos de la compañía.	Que las vulnerabilidades identificadas tengan un puntaje CVSS superior a 9 o esté relacionado con un *exploit* público.	1. Investigar y notificar a las áreas interesadas sobre las vulnerabilidades con severidad mayor o igual al puntaje CVSS 9 que afecten a los activos críticos. 2. Investigar si existen *exploit*, pruebas de concepto o posibles campañas en las que se estén explotando vulnerabilidades que puedan afectar a los activos críticos. 3. - Investigar si existen *exploit*, pruebas de concepto o posibles campañas en las que se estén explotando vulnerabilidades que puedan afectar a los activos críticos.	Gestión proactiva de vulnerabilidades
Realizar el monitoreo de amenazas que puedan afectar los activos críticos de la compañía.	Relacionado con: 1. Ransomware. 2. Malware que exfiltre información. 3. Ataques que afecten la disponibilidad del servicio.	1. Investigar y notificar a las áreas interesadas sobre las amenazas que puedan afectar los activos críticos de la organización. 2. Verificación de los indicadores de compromiso asociados a las amenazas. 3. Realizar el bloqueo de los indicadores de compromiso relacionados en los controles de seguridad para las amenazas reportadas.	Gestión proactiva de amenazas
Monitorear a posibles actores maliciosos que podrían atacar a la compañía.	Se deben tomar en cuenta los siguiente Actores: 1. Que afecten al sector del Contact Center y sus principales socios de negocio. 2. Que afecten a la región.	1. Identificar actores maliciosos que podrían afectar a la compañía. 2. Realizar seguimiento a la actividad de los actores maliciosos identificados. 3. Notificar campañas realizadas por estos actores.	Perfilamiento de actores malicios

Tabla 1. PIR – inteligencia de amenazas

- <u>*Recolección y Procesamiento*</u>: Los equipos de inteligencia determinan el tipo de información y las fuentes donde se obtendrán los datos necesarios. En este paso los equipos usan las plataformas de inteligencia de amenazas (de sus siglas en inglés *Threat Intelligence Platform - TIP*).

  Este trabajo propone la automatización del proceso de gestión de inteligencia de amenazas por medio del uso de una herramienta para TIP y una para gestión de flujo de procesos, las cuales al integrarse proporcionan beneficios como: realizar consultas de indicadores de compromiso a través de una API hacia diferentes motores de base de datos de malware, lo que permite obtener más información para los casos internos de incidentes de seguridad; además, la integración y visualización de alertas generadas desde la TIP hacia la herramienta de flujo de procesos.

- **Plataforma de inteligencia de amenazas TIP**: tiene la capacidad de consolidar, correlacionar, y clasificar la información de una manera estructurada para que sea fácilmente consumible por el equipo de seguridad. Estas herramientas se usan para recolectar y utilizar de manera efectiva información sobre amenazas, vulnerabilidades, ataques y *exploits*.

  En el mercado existen diferentes tipos de herramientas TIP, cada una con diferentes capacidades y bajo diferentes modelos de licencia, algunas de las evaluados en este proyecto son: **OpenCTI, MISP, CRITS y CIF.**

  Para el desarrollo del proyecto, se seleccionó la herramienta **OpenCTI**, la cual cuenta con características como:

  - Cuenta con plantillas predefinidas para correlacionar información de interés
  - Creación de perfiles de las amenazas y actores de acuerdo con los intereses del Contact Center.
  - Cuenta con panel de recomendaciones para aplicación de reglas y firmas para los dispositivos de control.
  - Proporciona documentación muy extensa y completa, entre otras características.

- **Herramienta Flujo de Procesos:** permite la creación de flujos de procesos a través de plantillas personalizadas, la selección y uso de analizadores de indicadores de compromiso de forma automatizada y la generación de reportes estadísticos en tiempo real.

  Se evaluaron herramientas para este proyecto que cumplieran lo requerido, tales como: **Cyphon y TheHive;** la herramienta seleccionada es **TheHive,** teniendo en cuenta que también puede integrarse con OPENCTI.

- **Orquestación de herramientas:** el despliegue de las herramientas se realizó por medio del uso de dockers (TheHive-Project, 2020) (OpenCTI-Platform, 2020), mostrando la arquitectura en la ilustración 3. Las características de los dockers se describen a continuación:

  Arquitectura Plataforma TheHive
  La plataforma de gestión de Flujos, de acuerdo con su arquitectura hace uso de tres componentes:

  • *TheHive:* a nivel de frontend hace uso de AngularJS y de Bootstrap y en el backend hace uso de REST API mediante Scala, akka y play.

  • *Cortex:* a nivel de frontend hace uso de AngularJS y de Bootstrap y en cuanto al backend hace uso de REST API mediante Scala, akka y play; para los módulos de analizadores y responder utiliza Python, de igual forma, Cortex se integra con TheHive para automatizar las tareas de analizar indicadores de compromiso y a través de una API integrarse con OpenCTI.

  • *Elasticsearch:* como plataforma de almacenamiento de información y de indexación para TheHive y Cortex.

Arquitectura Plataforma OpenCTI

La plataforma de gestión de inteligencia de amenazas, de acuerdo con su arquitectura hace uso de los siguientes componentes:

• *Grakn:* como plataforma de base de datos relacional para datos altamente interconectados y que proporciona un esquema a nivel de concepto que implementa completamente el modelo Entidad-Relación (ER), es una base de conocimiento para la inteligencia artificial y los sistemas de computación cognitiva.

• *Elasticsearch:* como plataforma de indexación.

• *Redis:* como almacén de estructura de datos en memoria que se utiliza como base de datos caché y agente de mensajes.

• *MinIO:* como almacenamiento de objetos de alto rendimiento, para cargas de trabajo de datos de aplicaciones, análisis y aprendizaje automático.

• *RabbitMQ:* como plataforma de agente de mensajes que implementa el protocolo avanzado de cola de mensajes (AMQP).

• *GraphQL:* como lenguaje de consulta para API en tiempo de ejecución para completar esas consultas con sus datos existentes.

• *React:* como plataforma de frontend.

• *Python:* para los workers y conectores de la plataforma.

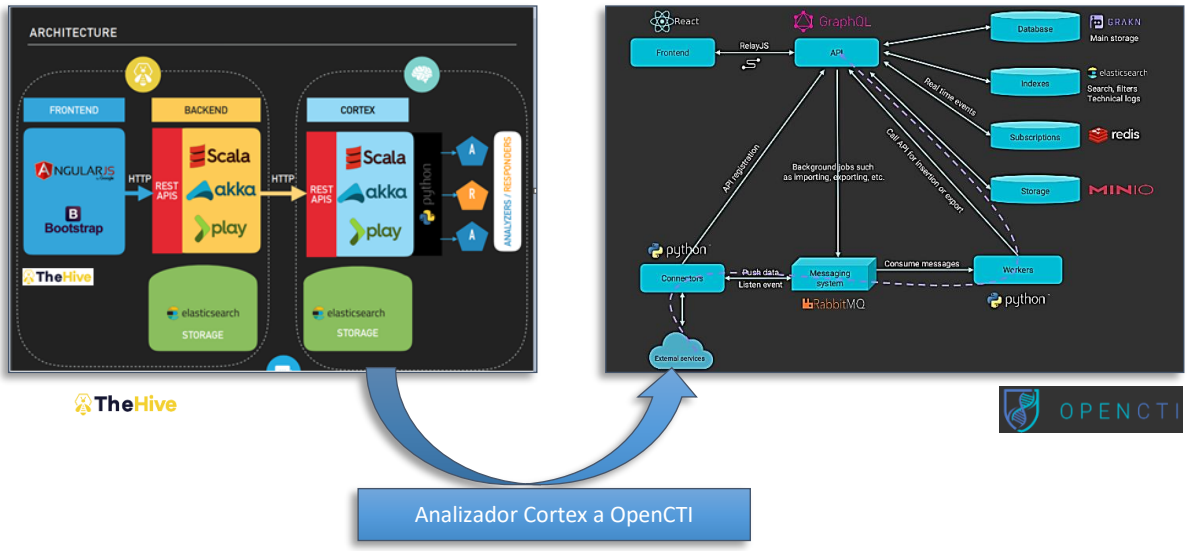

Ilustración 3 Arquitectura Gestión de flujos e Inteligencia de Amenazas

- *Análisis y producción*: Los equipos deben analizar la información correlacionada de la TIP de manera efectiva con el fin de extraer información de interés para el negocio y producir entregables de valor para la organización.
  La ilustración 4 presenta el flujo general del proceso de inteligencia de amenazas, el cual inicia cuando el equipo de seguridad busca la información de interés en OpenCTI, luego valida la información con los PIR para determinar si cumple con la condición y así proceder a crear el caso y ejecutar el flujo en TheHive y de acuerdo con el resultado realizar la difusión a las áreas

interesadas. Finalmente, los equipos de tecnología entregaran una retroalimentación de las acciones ejecutadas.

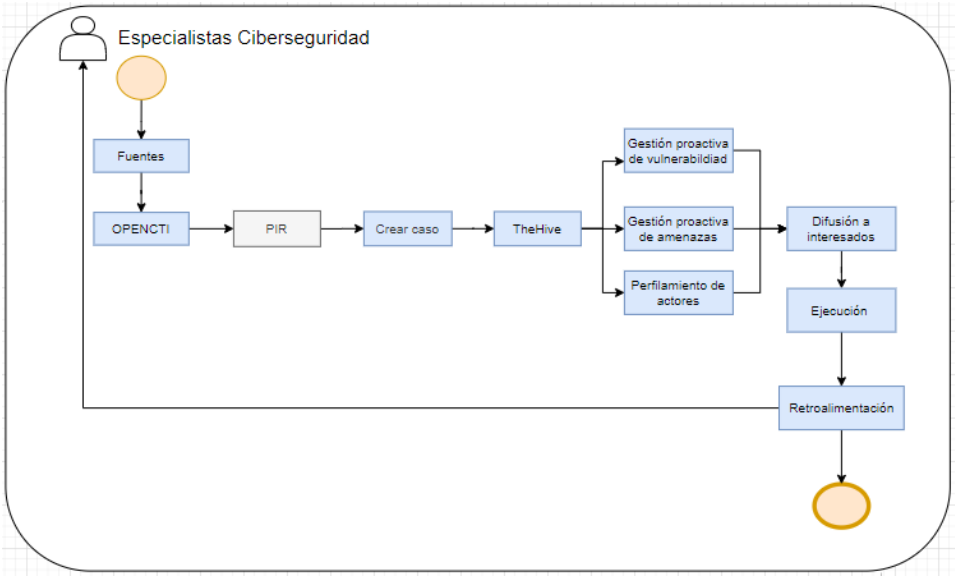

Ilustración 4 Esquema general de aseguramiento proactivo

- *Difusión*: Como se muestra en la ilustración 5, los equipos de seguridad de la información deben distribuir los informes de inteligencia a las partes interesadas para su respectiva ejecución que van desde el nivel técnico, pasando por niveles operativos, tácticos y estratégicos; siendo el nivel estratégico, el responsable de la asignación de recursos y establecimiento de prioridades.

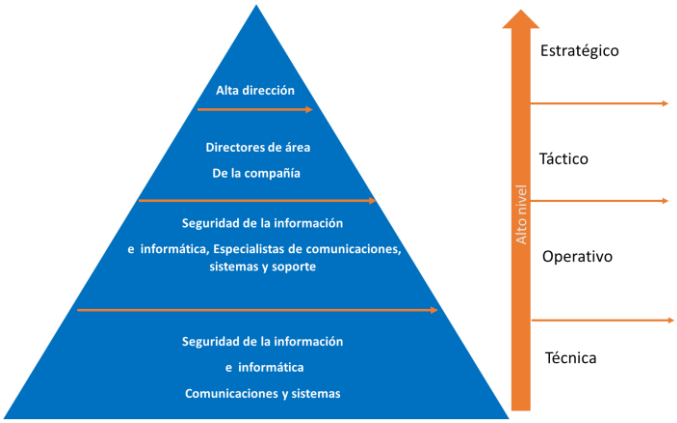

Ilustración 5 Niveles de Gestión

- *Retroalimentación*: Las partes interesadas deben proporcionar retroalimentación del proceso aplicado al equipo de inteligencia para ayudar a afinar las iteraciones futuras del paso de análisis y producción.

2.2 Factor Humano

Esta sección identifica las competencias (Alles, 2009), que deben tener los integrantes del equipo de seguridad encargados del proceso descritos anteriormente:

- Flexibilidad y adaptación (nivel experto- nivel 2): Capacidad para trabajar con eficacia en situaciones variadas y/o inusuales, con personas o grupos diversos. Implica comprender y valorar posturas distintas a las propias, incluso puntos de vista encontrados, modificar su propio enfoque a medida que la situación cambiante lo requiera, y promover dichos cambios en su ámbito de actuación.

- Orientación al cliente interno y externo (nivel líder nivel 1): Capacidad para actuar con sensibilidad ante las necesidades de un cliente y/o conjunto de clientes, actuales o potenciales, externos o internos, que se pueda/n presentar en la actualidad o en el futuro. Implica una vocación permanente de servicio al cliente interno y externo, comprender adecuadamente sus demandas y generar soluciones efectivas a sus necesidades.

- Calidad y mejora continua (nivel líder nivel 1): Capacidad para optimizar los recursos disponibles –personas, materiales, etc.– y agregar valor a través de ideas, enfoques o soluciones originales o diferentes en relación con la tarea asignada, las funciones de las personas a cargo, y/o los procesos y métodos de la organización. Implica la actitud permanente de brindar aportes que signifiquen una solución a situaciones inusuales y/o aportes que permitan perfeccionar, modernizar u optimizar el uso de los recursos a cargo.

- Conocimientos técnicos (nivel experto nivel 2): Capacidad para poseer, mantener actualizados y demostrar todos aquellos conocimientos y/o experiencias específicas que se requieran para el ejercicio de la función a cargo, y avivar de manera constante el interés por aprender y compartir con otros los conocimientos y experiencias propios.

3. Resultados

- En cuanto al modelamiento del esquema de gestión proactiva, se logra generar un proceso estandarizado con etapas claramente definidas y medibles, que, al estar enfocado en el objeto de negocio específico, generan valor para el Contact Center.

- En las pruebas realizadas, se observó la importancia de tener definidos los PIR específicos ya que permite enfocarse en las necesidades del Contact Center, teniendo en cuenta los grandes volúmenes de información de inteligencia de amenazas que se generan en un marco de tiempo determinado.

- Al hacer uso de una herramienta TIP con información centralizada en amenazas, vulnerabilidades y actores maliciosos, se evidencia la disminución de tiempos para la búsqueda, correlación y análisis de información recibida.

- Mediante la herramienta de flujo de procesos se generaron plantillas estandarizadas que indican las actividades a realizar para gestionar las alertas identificadas por el equipo de seguridad.

- A través de la herramienta de flujo de procesos, se automatizó el análisis de los indicadores de compromiso, por medio del uso de múltiples bases de datos de malware, evidenciando la disminución de tiempos en este proceso.

- La herramienta de gestión de flujos de procesos permite generar estadísticas en tiempo real de los casos gestionados para obtener métricas de rendimiento.

- La integración de la herramienta TIP con la herramienta de flujo de procesos se realizó a través de una API para la consulta de indicadores de compromiso.
- La integración de la herramienta TIP con la herramienta de flujo de procesos para la generación de alertas de inteligencia de amenazas, requerirá de un desarrollo de código en una fase posterior a este proyecto.
- El esquema de aseguramiento proactivo permite una reducción de tiempo al pasar de un proceso manual y reactivo a un proceso automatizado y proactivo como se muestra en las siguientes tablas:

Tarea	Fuentes	Tiempo (minutos)	Total (minutos)	Frecuencia de las búsquedas	Tiempo Total (horas)
Búsqueda de vulnerabilidades en las páginas del fabricante	15	5	75	2 veces por semana	**2,3**
Búsqueda de amenazas	10	10	100	1 vez al día	**8,33**
Carga y, revisión del indicador	50	1,5	75	1 vez por semana	**1,25**
				Total	**11,88**

Tabla 2. Proceso manual y reactivo

Tarea	Fuentes	Tiempo (minutos)	Tiempo total (minutos)	Frecuencia de las búsquedas	Tiempo total (horas)
Búsqueda de vulnerabilidades en las páginas del fabricante	15	0,58	8,7	2 veces por semana	**0,29**
Búsqueda de amenazas	10	0,58	5,8	1 vez al día	**0,48**
Carga y, revisión del indicador	50	0,25	12,5	1 vez por semana	**0,21**
				Total	**1,38**

Tabla 3. Proceso automatizado y proactivo

Tarea	Tiempo Ahorrado (horas) contra proceso manual
Búsqueda de vulnerabilidades en las páginas del fabricante	2,01
Búsqueda de amenazas	7,85
Carga y, revisión del indicador	1,04
Total	**10,9**

Tabla 4. Resultado ahorro total de tiempo

4. Conclusiones

La implementación del esquema de gestión proactiva se enfocó en tres áreas definidas como los pilares que permiten agregar valor y mejoras al proceso actual iniciando con el modelamiento, configuración e implementación de las herramientas tecnológicas para finalmente ser gestionadas a través de las habilidades definidas en recurso humano.

4.1 **Modelamiento de procesos**

- La definición adecuada de los requisitos prioritarios de inteligencia (de sus siglas en ingles *Priority Intelligence Requirements - PIR*) es clave para que el proceso se diseñe e implemente de acuerdo con las capacidades de la compañía y con ello genere un valor real para el negocio.

- El establecimiento de los diferentes tipos de inteligencia, aseguran que las áreas interesadas de la compañía reciban la información en el lenguaje preciso para su adecuada gestión.

- La identificación de los procesos internos y su integración con el esquema de aseguramiento garantizará los resultados adecuados para su ejecución a través de las diferentes áreas.

- La ejecución del modelo propuesto lleva a una disminución en los tiempos de tareas operativas, permitiendo la mejora de la capacidad para el análisis por parte de los especialistas.

4.2 **Herramientas tecnológicas**

- En el mercado se encuentra una gran variedad de herramientas código abierto que brindan la posibilidad de implementación para este tipo de iniciativas, sin embargo, la definición del uso de alguna en específico dependerá de la necesidad de la compañía.

- Debido a que el despliegue de herramientas tecnológicas se realiza mediante el uso de Docker, la configuración e implementación puede ser realizada con los conocimientos y la experiencia del personal que actualmente cuenta la empresa.

4.3 **Factor Humano**

- Adoptar estos modelos dentro de la gestión de los equipos de Seguridad de la Información, aumenta la capacidad de análisis para la investigación de vulnerabilidades, amenazas y actores maliciosos, a través del aprovechamiento de la tecnología dentro de la compañía.

- El perfilamiento realizado de las personas que componen el equipo actualmente para el esquema de aseguramiento cumple las expectativas para alcanzar los objetivos de la gestión proactiva; sin embargo, para la maduración del proceso, será necesaria la ampliación de la capacidad humana para la ejecución del proyecto.

Bibliografía

Alles, M. A. (2009). *Diccionario de competencias, la trilogía.* Buenos Aires, Mexico, Santiago, Montevideo: GRANICA.

amenazas, D. d. (2020). *Definición de inteligencia de amenazas.* Obtenido de https://latam.kaspersky.com/resource-center/definitions/threat-intelligence

CISA. (2020). *CISA.* Obtenido de https://www.cisa.gov/blog/2020/06/09/cisa-releases-cyber-risks-911-tdos-fact-sheet

Colombia, T. c. (2019 - 2020). *www.ccit.org.co.* Obtenido de https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf

Dabbas, E. (s.f.). *DataCamp*. Recuperado el 19 de 04 de 2020, de DataCamp: https://www.datacamp.com/community/tutorials/absolute-weighted-word-frequency

Future, I. O. (2018). *IDC Organizations React to Security Threats More Efficiently and Cost Effectively with Recorded Future.* Obtenido de https://go.recordedfuture.com/hubfs/white-papers/idc-executive-summary.pdf

IBM. (14 de 11 de 2020). *IBM Security*. Obtenido de Cost of a Data Breach Report: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/es

Index, I. X.-F. (2020). *IBM X-Force Threat Intelligence Index.* Obtenido de https://www.ibm.com/security/data-breach/threat-intelligence

Industrial-Strength Natural Language Processing. (s.f.). Recuperado el 25 de 04 de 2020, de https://spacy.io/

Johan, R. (2016). Topic Modelling. En *Detecting Twitter topics using Latent Dirichlet Allocation. Uppsala Universitet* (pág. 45). Uppsala Universitet.

Kapadia, S. (19 de 08 de 2019). *Evaluate Topic Models: Latent Dirichlet Allocation (LDA)*. (Towards Science) Recuperado el 26 de 05 de 2020, de https://towardsdatascience.com/evaluate-topic-model-in-python-latent-dirichlet-allocation-lda-7d57484bb5d0

Loria, S. (s.f.). *TextBlob: Simplified Text Processing*. Recuperado el 26 de 04 de 2020, de https://textblob.readthedocs.io/en/dev/

O4IT, A. –r. (2019). *www.acis.org.co.* Obtenido de https://www.acis.org.co/portal/content/NoticiaDelSector/circular-externa-circular-externa-007-de-2018-cuenta-regresiva-para-su-entrada-en-vigencia#_ftn1

Python, R. (s.f.). *Real Python*. Recuperado el 21 de 04 de 2020, de https://realpython.com/beautiful-soup-web-scraper-python/

Řehůřek, R. (01 de 2019). *LDA Model*. (gensim - Topic Modelling for humans) Recuperado el 18 de 05 de 2020, de https://radimrehurek.com/gensim/auto_examples/tutorials/run_lda.html#sphx-glr-auto-examples-tutorials-run-lda-py

Report, D. D. (2020). *content.fireeye.com.* Obtenido de https://content.fireeye.com/security-effectiveness/rpt-security-effectiveness-2020-deep-dive-into-cyber-reality

Report, D. D. (2020). *Deep Dive Into Cyber Reality Security Effectiveness Report.* Obtenido de https://content.fireeye.com/security-effectiveness/rpt-security-effectiveness-2020-deep-dive-into-cyber-reality

Securelogix. (2020). *Securelogix.* Obtenido de https://securelogix.com/threats/stop-tdos-attacks/

SFC, C. 0. (2018). *www.superfinanciera.gov.co.* Obtenido de https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00

Steven Bird, E. K. (2009). *Natural Language Processing with Python.* Sebastopol, California: O'Reilly.

Subrahmannian, S. (16 de Abril de 2018). *Learn to Find Topics in a Text Corpus*. (Medium Data Science) Recuperado el 03 de Abril de 2020, de https://medium.com/@soorajsubrahmannian/extracting-hidden-topics-in-a-corpus-55b2214fc17d

Taspinar, A. (s.f.). *Scrape Twitter for Tweets*. Recuperado el 21 de 04 de 2020, de MIT License Copyright (c): https://github.com/taspinar/twitterscraper

Tripathi, M. (s.f.). *freeCodeCamp*. Recuperado el 21 de 04 de 2020, de https://www.freecodecamp.org/news/how-to-process-textual-data-using-tf-idf-in-python-cd2bbc0a94a3/

TRUSID. (2019). *TRUSID* . Obtenido de https://www.securitymagazine.com/articles/90028-how-call-centers-are-the-weakest-links-in-authentication-chain