Definición de un modelo de estrategia de inteligencia de amenazas cibernéticas en entidades gubernamentales de Colombia como mecanismo de anticipación de riesgos cibernéticos

Cejer Chica Vargas
Diego Fernando Pinto Prada

Universidad Ean

Facultad de ingeniería

Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Bogotá, Colombia

2024

Definición de un modelo de estrategia de inteligencia de amenazas cibernéticas en entidades gubernamentales de Colombia como mecanismo de anticipación de riesgos cibernéticos

Cejer Chica Vargas
Diego Fernando Pinto Prada

Trabajo de grado presentado como requisito para optar al título de:

Magister en Gerencia de Proyectos en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Director:

Emanuel Elberto Ortiz Ruiz

Modalidad:

Monografía

Universidad Ean

Facultad de ingeniería

Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Bogotá, Colombia

2024

Nota de aceptación:

Firma del jurado

Firma del jurado

Firma del director del trabajo de grado

Ciudad, día/mes/año

Dedicatorias

Dedicatoria de Cejer Chica V.:

Mi madre, de quien tengo admiración por la capacidad de salir adelante pese a las dificultades**.** Por la cual estoy orgullosa por su apoyo incondicional en los diferentes proyectos que me he planteado.

Mi padre, a quien siempre dedico de su tiempo para enseñarme que la perseverancia siempre tiene sus frutos. Y el cual ha sido un gran soporte para la familia.

Mis hermanos, por el apoyo ante cualquier situación buena o mala. Y de los cuales admiro la capacidad de ayudar al prójimo.

Mi abuela Mercedes, por todo su amor, dedicación, cariño y comprensión de niña hasta sus últimos momentos.

A Diego Pinto, por todas las noches de desvelos y por la motivación a seguir creciendo cada día.

A John Guevara, por su motivación y dedicación en cada una de las enseñas transmitidas. Y del cual siento admiración por enseñarme que la empatía es fundamental en el ser.

Dedicatoria de Diego F. Pinto P.:

A mi Padre, quien siempre se preocupó por nuestro bienestar y me enseñó que cada logró obtenido es el fruto de nuestros esfuerzos, siendo esto lo que más le llenaba de orgullo.

A mi Madre, que demostró que a pesar de las circunstancias siempre es posible salir adelante, demostrando que no hay imposibles.

A mi hermana y sobrina, a quienes lleno de orgullo con cada logro, motivándome a llegar más lejos.

A mi esposa, quien tuvo la paciencia para acompañarme en esta travesía de casi dos años, dándome su apoyo de seguir y no desfallecer en el camino.

A Cejer Chica, por ser esa compañera de viaje en esta aventura de estudio que en las buenas y en las malas siempre estuvo dispuesta a colaborar.

A John Guevara, gran mentor que durante años me motivó a seguir aprendiendo y cuyo conocimiento y capacidades admiro.

Agradecimientos

Agradecemos a la Universidad EAN, ya que como alma máter nos brindó la oportunidad de formarnos, desarrollarnos y crecer tanto de manera académica, profesional y personal.

Agradecemos enormemente a nuestro mentor, el señor John Albeiro Guevara Pulido, quien, por medio de la generación de esta iniciativa académica, nos forjó, motivó y acompañó antes y durante el proceso de investigación de esta tesis.

Asimismo, agradecemos a nuestro director de trabajo de grado Emanuel Elberto Ortiz Ruiz, por su dedicación y todo el conocimiento transmitido en el proceso de desarrollo de la investigación.

A cada docente de la Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos, de quienes pudimos adquirir e interiorizar todos los conocimientos.

Resumen

El uso exponencial de las tecnologías de la información en el día a día de las actividades del ser humano ha incrementado considerablemente la cantidad de ciberataques en múltiples entornos. Ante esto, se evidencia la necesidad de entender la inteligencia de amenazas cibernéticas como un mecanismo que permita la toma de decisiones a partir de los datos e información obtenidos sobre el contexto de las ciberamenazas, algo que a nivel gubernamental poco se ha explorado.

Para cumplir con lo planteado en la investigación se aplicó el enfoque exploratorio descriptivo y cuantitativo, mediante el desarrollo del objetivo general y los objetivos específicos, orientados a revisar la normatividad de la temática, analizar la materialización de riesgos cibernéticos y proponer una estrategia, aplicado al contexto colombiano, para lo cual se aplicó un instrumento tipo encuesta y entrevista, junto a la obtención de información de fuentes abiertas y diferentes referentes de investigación consultados.

En la investigación participaron 62 funcionarios de las entidades del Estado del orden nacional, lo que representa un 20,8% de la población objetivo. Asimismo, se entrevistaron 10 expertos en ciberseguridad, de los que el 50% pertenece al sector objetivo y el 50% al sector privado. La obtención de estos resultados permitió identificar fortalezas y debilidades del contexto actual, tales como, el entendimiento del CTI en un gran porcentaje, pero que a su vez no se cuenta con personal capacitado en la temática. De igual forma, se evidenció la necesidad de tener capacidades propias, ya que resalta la dependencia de proveedores de servicio, debido a las pocas competencias para producir CTI, al igual que la carencia de herramientas para tal fin.

En cuanto a los expertos entrevistados, los resultados evidenciaron una postura general sobre tener una hoja de ruta a seguir para prevenir afectaciones y minimizar el riesgo de las ciberamenazas sobre las infraestructuras tecnológicas gubernamentales.

A partir de lo anterior, se propuso una estrategia para anticipar y prevenir eventos, incidentes o materialización de riesgos cibernéticos en las entidades gubernamentales en Colombia, para salvaguardar la confidencialidad, integridad y disponibilidad de la información de las diferentes infraestructuras tecnológicas de las organizaciones. Esta se construyó a partir de las necesidades identificadas que derivaron de los instrumentos aplicados y la investigación realizada, lo que conllevo a considerar en primer lugar la definición de un ciclo CTI, seguido de los aspectos importantes para tener en cuenta y finalmente un plan de acción basado en cuatro dimensiones que son: la alineación estratégica, la alineación organizacional, la gestión del talento humano y las capacidades técnicas.

Palabras clave: anticipación, prevención, incidentes, delitos informáticos, ciberataques, inteligencia de amenazas, amenazas, ciberseguridad.

Abstract

The exponential use of information technologies in the day-to-day activities of human beings has considerably increased the number of cyberattacks in multiple environments. Given this, the need to understand cyber threat intelligence as a mechanism that allows decision-making based on the data and information obtained about the context of cyber threats is evident, something that has been little explored at the government level.

To comply with what was proposed in the research, the descriptive and quantitative exploratory approach was applied, through the development of the general objective and the specific objectives, aimed at reviewing the regulations of the subject, analyzing the materialization of cyber risks and proposing a strategy, applied to the Colombian context, for which a survey and interview type instrument was applied, together with obtaining information from open sources and different research references consulted.

62 officials from national State entities participated in the investigation, which represents 20.8% of the target population. Likewise, 10 cybersecurity experts were interviewed, of which 50% belong to the target sector and 50% to the private sector. Obtaining these results made it possible to identify strengths and weaknesses of the current context, such as the understanding of CTI in a large percentage, but at the same time there are no trained personnel on the subject. Likewise, the need to have own capabilities was evident, since the dependence on service providers stands out, due to the few competencies to produce CTI, as well as the lack of tools for this purpose.

Regarding the experts interviewed, the results showed a general position on having a roadmap to follow to prevent impacts and minimize the risk of cyber threats to government technological infrastructures.

Based on the above, a strategy was proposed to anticipate and prevent events, incidents or materialization of cyber risks in government entities in Colombia, to safeguard the confidentiality, integrity and availability of information from the different technological infrastructures of the organizations. This was built from the identified needs that derived from the instruments applied and the research carried out, which led to first considering the definition of a CTI cycle, followed by the important aspects to take into account and finally an action plan. based on four dimensions that are: strategic alignment, organizational alignment, human talent management and technical capabilities.

Keywords*:* anticipation, prevention, incidents, computer crimes, cyberattacks, threat intelligence, threats, cybersecurity.

Contenido

Pág.

Lista de Figuras **10**

Lista de Tablas **11**

1. Introducción **12**

2. Objetivos **16**

2.1. Objetivo general *16*

2.2. Objetivos específicos *16*

3. Justificación **17**

4. Marco Teórico **20**

4.1. Inteligencia de amenazas cibernéticas *21*

4.2. Ciclo de inteligencia de amenazas *22*

4.3. Fases del ciclo de inteligencia de amenazas *35*

4.4. Tipos de inteligencia de amenazas *37*

4.5. Indicadores de compromiso *40*

4.6. Beneficios de la inteligencia de amenazas *42*

4.7. Retos de la inteligencia de amenazas *42*

4.8. Panorama actual de la inteligencia de amenazas *45*

4.9. Contexto de inteligencia de amenazas cibernéticas en Colombia *46*

5. Análisis PESTEL **48**

5.1. Político *48*

5.2. Económico *48*

5.3. Social *49*

5.4. Tecnológico *50*

5.5. Ambiental *50*

5.6. Legal *51*

6. Hipótesis **52**

7. Variables **53**

7.1. Conocimiento de CTI *54*

7.2. Recursos asociados a inteligencia de amenazas *54*

7.3. Capacidad de anticipación y respuesta incidentes *54*

7.4. Sector/roles y aplicabilidad del CTI *55*

7.5. Implementación y uso de CTI *55*

7.6. Entidad líder de la estrategia *55*

8. Metodología 56

8.1. Enfoque y alcance de la investigación *56*

8.2. Enfoque de la investigación *56*

8.3. Tipo de la investigación *56*

8.4. Diseño de la investigación *57*

8.5. Población *58*

8.6. Muestra *59*

8.7. Diseño del instrumento *60*

8.8. Técnicas para el análisis de la información *61*

9. Trabajo de Campo 62

9.1. Revisión frente a la normatividad, medidas y controles existentes en Colombia sobre la prevención en la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos, enfocado en la inteligencia de amenazas (CTI). *64*

9.2. Afectación causada por la materialización de riesgos cibernéticos en las entidades gubernamentales de Colombia. *72*

9.3. Propuesta de una estrategia orientada a la anticipación y prevención por medio de la inteligencia de amenazas cibernéticas que complemente las capacidades existentes de seguridad informática y ciberseguridad en las entidades gubernamentales de Colombia. *80*

10. Discusión 107

11. Conclusiones y trabajos futuros 110

1.1. Conclusiones *110*

1.2. Trabajo futuro *110*

12. Referencias 113

A. Anexo. Encuesta 121

B. Anexo. Entrevista 127

Lista de Figuras

Figura 1. Adaptado del Modelo de 16 fases CTI. 23
Figura 2. Adaptado del Modelo de 8 fases de CTI. 24
Figura 3. Adaptado del Ciclo de 6 fases CTI. 25
Figura 4. Adaptado del Ciclo CTI NCSC. 26
Figura 5. Adaptado al Ciclo CTI CPNI. 27
Figura 6. Adaptado del Ciclo de inteligencia FAS. 28
Figura 7. Adaptado del Ciclo de inteligencia OTAN. 29
Figura 8. Adaptado del Ciclo de inteligencia FBI. 30
Figura 9. Adaptado del Ciclo de inteligencia CIA. 31
Figura 10. Adaptado del Ciclo de inteligencia ACIC. 32
Figura 11. Adaptado del Ciclo de Inteligencia FIRST. 33
Figura 12. Adaptado del Ciclo de Inteligencia CNI. 34
Figura 13. Adaptado del Ciclo de inteligencia Colombia. 35
Figura 14. Análogo de la Pirámide del Dolor. 41
Figura 15. Resultado 1 encuesta nivel de apropiación del CTI. 62
Figura 16. Resultado 1 encuesta nivel de apropiación del CTI - expertos. 63
Figura 17. Resultado 21 encuesta nivel de apropiación del CTI. 72
Figura 18. Tipo de incidentes ocurridos. 72
Figura 19. Comparativo conductas delictivas en el ciberespacio 73
Figura 20. Cirfras URL en Colombia. 74
Figura 21. Cifras archivos en Colombia. 75
Figura 22. Resultado 2 encuesta nivel de apropiación del CTI. 80
Figura 23. Resultado 3 encuesta nivel de apropiación del CTI. 81
Figura 24. Resultado 4 encuesta nivel de apropiación del CTI. 81
Figura 25. Resultado 6 encuesta nivel de apropiación del CTI. 82
Figura 26. Resultado 7 encuesta nivel de apropiación del CTI. 83
Figura 27. Resultado 9 encuesta nivel de apropiación del CTI. 83
Figura 28. Resultado 10 encuesta nivel de apropiación del CTI. 84
Figura 29. Resultado 11 encuesta nivel de apropiación del CTI. 85
Figura 30. Resultado 13 encuesta nivel de apropiación del CTI. 86
Figura 31. Resultado 14 encuesta nivel de apropiación del CTI. 86
Figura 32. Resultado 16 encuesta nivel de apropiación del CTI. 87
Figura 33. Resultado 17 encuesta nivel de apropiación del CTI. 87
Figura 34. Resultado 18 encuesta nivel de apropiación del CTI. 88
Figura 35. Resultado 19 encuesta nivel de apropiación del CTI. 89
Figura 36. Resultado 20 encuesta nivel de apropiación del CTI. 90
Figura 37. Cronograma estrategia Inteligencia de amenazas. 106
Figura 38. Modelo herramienta para la fase de recolección CTI. 112

Lista de Tablas

Tabla 1. Comparativa de ciclos de inteligencia aplicables al CTI. 43
Tabla 2. Cuantitativo: Apropiación del conocimiento de CTI. 53
Tabla 3. Cualitativo: Impacto del CTI en la anticipación de eventos, incidentes o materialización de riesgos cibernéticos..... 54
Tabla 4. Identificador de nivel implementación del control 5.7. 96
Tabla 5. Personal capacitado en Inteligencia de Amenazas. 99
Tabla 6. Nivel de implementación de Sandbox en las entidades. 102
Tabla 7. Interconexión de plataforma MISP. 104
Tabla 8. Efectividad en la recolección de Inteligencia de Amenazas. 105

1. Introducción

El aumento del uso de las tecnologías de la información en las actividades diarias del ser humano ha traído consigo ciberataques asociados a ello, que a su vez crecen de forma exponencial. Históricamente, Estonia es conocido como el primer país que sufrió el mayor ciberataque de la historia en el 2007, afectando la infraestructura tecnológica del sector gobierno y las finanzas. Esto conllevó a la creación de los Centros de Excelencia de la Organización del Tratado del Atlántico Norte (OTAN) enfocados en la cooperación en ciberdefensa, con el objetivo principal de proteger y salvaguardar a los países miembros de ciberataques por medio del entrenamiento, desarrollo de investigaciones en técnicas defensivas y establecimiento de marcos legales que permitieran el desarrollo de las estrategias planteadas (Departamento Nacional de Planeación, 2011).

Adicionalmente, lo anterior dio paso a la creación de la Liga de Ciberdefensa de Estonia con la misión de garantizar la protección del “estilo de vida de alta tecnología” de dicho país, siendo un referente en el despliegue de estrategias de ciberdefensa a nivel mundial (Cardash, Cilluffo, & Ottis, 2013).

Sin embargo, a pesar de dichas iniciativas, se han observado gran cantidad de ciberataques en múltiples sectores a nivel mundial desde el 2007 hasta la fecha, tales como: la afectación a la central nuclear de Irán en 2010, el acceso no autorizado a PlayStation de Sony en 2011, el ataque a Spamhaus en 2013 que ralentizó el internet en todo el mundo y el ataque del virus Petya que afectó el gobierno de Ucrania en 2017 (Loishyn, y otros, 2021).

Otro caso relevante en 2017 fue lo ocurrido con WannaCry, cuando en febrero de ese año se descubrió la primera versión de este *software malicioso* que cifraba los archivos sin tener el típico comportamiento de gusanos informáticos. Posteriormente, el 28 de marzo de 2017, se descubrió la versión 1.0 que accedía por medio del protocolo SMB (*Server Message Block*) a carpetas compartidas y descargaba el navegador TOR

(*The Onion Router*) para completar la secuencia del ataque y cifrar la información. Finalmente, con la evolución a la versión 2.0 se mejoró considerablemente el método de propagación, al implementar un gusano y un módulo de *exploit* llamado EternalBlue, que explotaba la vulnerabilidad CVE-2017-0144 del servicio SMB (NIST, 2017), lo que permitió la infección de un aproximado de 300.000 equipos distribuidos en más de 150 países durante mayo de ese mismo año. Lo relevante de este caso es que Microsoft había desarrollado el parche de seguridad MS17-010 dos meses antes de que se llevara a cabo el ciberataque (Akbanov, Vassilakis, & Logothetis, 2019).

Colombia no ha sido la excepción en cuanto a ataques cibernéticos. Durante los últimos tres años se han presentado gran cantidad de ataques informáticos de alto impacto, donde instituciones como el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (INVIMA), el Departamento Administrativo Nacional de Estadística (DANE), KERALTY, las Fuerzas Militares, FISCALÍA, entidades de salud, universidades, entre otras, fueron víctimas de ciberdelincuentes con casos asociados a software maliciosos, robo de información y daño a infraestructuras.

Un caso relevante es el ciberataque ocurrido a IFX Networks en septiembre del 2023 que afectó múltiples servicios de entidades colombianas y otros países, teniendo como vector de ataque el secuestro de información (Rasomware) (Brodersen, 2023). Estos hechos son conocidos como Amenazas Avanzadas Persistentes *(APT - Advanced Persistent Threat)*, cuyo objetivo es el de afectar la confidencialidad, integridad y disponibilidad de la información (Tatam, Shanmugam, Azam, & Kannoorpatti, 2021), comúnmente conocida como la triada de seguridad.

De acuerdo con cifras de cibercrimen publicadas por el tanque de análisis y creatividad del sector las Tecnologías de la Información y las Comunicaciones (TIC) en

Colombia, TicTac, en lo corrido de enero y octubre de 2022 se presentaron 54.121 denuncias por eventos, incidentes o materialización de riesgos cibernéticos, para el 2021 fueron reportadas 42.998 denuncias, lo que representó un 25 % de incremento (TicTac, 2022). A partir de estos datos, se evidencia un aumento considerable de actividades fraudulentas que hacen uso del ciberespacio como un medio y que en ocasiones repercuten en el contexto físico. Por ejemplo, el ciberataque ocurrido a Empresas Públicas de Medellín (EPM), que afectó a miles de usuarios al no poder efectuar los pagos de servicios prepagados de energía. De igual forma, cabe destacar el ataque de *software malicioso* realizado a Keralty por el actor *Ransomhouse,* ocasionando que cientos de ciudadanos no tuvieran la atención en el agendamiento de citas médicas y entrega de medicamentos. En ambos casos se afectó la calidad de vida de los usuarios.

A partir de lo anterior, la inteligencia de amenazas cibernéticas (CTI - *Cyber Threat Intelligence*) surge como una necesidad que permita afrontar los ciberataques, permitiendo que las instituciones puedan pasar de ser reactivas a proactivas (Wagner, Mahbub, Palomar, & Abdallah, 2019).

Sin embargo, en Colombia no se observan estrategias de anticipación de amenazas, puesto que los documentos del Consejo Nacional de Política Económica y Social (CONPES) creados para el fortalecimiento de la ciberseguridad del país se enfocan en la prevención y atención de incidentes desde el punto de vista reactivo. Asimismo, la Política Nacional de Seguridad Digital (Departamento Nacional de Planeación, CONPES 3854, 2016), en el capítulo 4 relaciona el diagnóstico en su numeral 4.4. correspondiente a "*reforzar las capacidades de ciberdefensa con un enfoque de gestión de riesgos*" (2016, p. 44), en el que se manifestó la dificultad de llevar a cabo la acción de anticipar debido al uso de técnicas sofisticadas y complejas empleadas por los atacantes. De igual forma, la Política Nacional de Confianza y Seguridad Digital (Departamento Nacional de Planeación, CONPES 3995, 2020) se

enfoca en generar confianza digital por medio de la implementación de medidas contra las amenazas digitales, donde se menciona “una adecuada anticipación” sin tener en cuenta el potencial que puede alcanzar la proactividad con propósitos defensivos. Por tal motivo, Colombia, al no contar con una estrategia CTI, pierde la oportunidad de llevar a cabo la “detección temprana” (Oosthoek & Doerr, 2020) que disminuya las intrusiones sobre las infraestructuras tecnológicas y la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos.

Conforme a lo anterior, el presente documento se desglosa en tres capítulos principales, mediante los cuales se desarrolla el objetivo general, así: “Revisión frente a la normatividad, medidas y controles existentes en Colombia sobre la prevención en la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos, enfocado en la inteligencia de amenazas (CTI)”, “Afectación causada por la materialización de riesgos cibernéticos en las entidades gubernamentales de Colombia” y “Propuesta de una estrategia orientada a la anticipación y prevención por medio de la inteligencia de amenazas cibernéticas que complemente las capacidades existentes de seguridad informática y ciberseguridad en las entidades gubernamentales de Colombia”.

Pregunta de investigación

¿De qué manera una estrategia CTI fortalecerá la anticipación y prevención en la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos en las entidades gubernamentales en Colombia?

2. Objetivos

2.1. Objetivo general

Definir una estrategia CTI orientada a anticipación y prevención en la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos en las entidades gubernamentales en Colombia.

2.2. Objetivos específicos

- Realizar una revisión frente a la normatividad, medidas y controles existentes en Colombia sobre la prevención en la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos, enfocado en la inteligencia de amenazas (CTI).
- Describir la afectación causada por la materialización de riesgos cibernéticos en las entidades gubernamentales de Colombia.
- Proponer una estrategia orientada a la anticipación y prevención por medio de la inteligencia de amenazas cibernéticas que complemente las capacidades existentes de seguridad informática y ciberseguridad en las entidades gubernamentales de Colombia.

3. Justificación

El uso del internet es una variable de crecimiento exponencial, llegando al punto que hoy en día no es posible concebir la idea de un mundo sin acceso a este recurso. Por tal razón, múltiples organizaciones de carácter público y privado han optado por ofrecer servicios a través del ciberespacio como medio para brindar capacidad y dar mayor alcance de cobertura a los usuarios. Sin embargo, debido al internet también han surgido una serie de actores maliciosos que realizan secuestro, daño, modificación o robo de información a las infraestructuras tecnológicas, con el propósito de obtener beneficios económicos y que permiten que la amenaza, pueda lograr la efectividad en sus acciones de realizar usos no autorizados sobre los datos obtenidos de forma fraudulenta si no consiguen lo que quieren.

La información como activo principal de las organizaciones tiene un gran valor para los ciberdelincuentes que, con el objetivo de extorsionar pueden causar cierta presión sobre las entidades afectadas. Este tipo de situaciones se han venido incrementando con el tiempo, puesto que abundan casos de fuga de información a nivel mundial por no cumplir con las exigencias de los extorsionistas (International Business Machines, 2023), y otros que a pesar de haberlas cumplido igual fueron víctimas de la exposición de la información. Lo anterior, sin tener en cuenta el daño a las infraestructuras tecnológicas causado por los atacantes una vez han robado los datos, lo que genera afectaciones en la prestación de los servicios, pérdidas económicas, afectación social y el daño reputacional de las organizaciones, aspectos en los que Colombia no han sido la excepción.

Con base en lo anterior, se hace necesario entender que existe un ciclo de inteligencia en el que se sugiere como planteamiento del flujo del proceso de inteligencia

cibernética las fases que incluye planear, recolectar, procesar, analizar, difundir y retroalimentar, con el propósito de ayudar a la toma de decisiones gerenciales en temáticas de seguridad digital y disminuir así el campo de acción de los ciberdelincuentes. Al tratarse de un tema escasamente explorado en el país, no existen investigaciones similares sobre CTI, salvo lo planteado por (Almanza, 2022) Almanza (2022) en la XXIII Encuesta Nacional de Seguridad Informática aplicada en Colombia, en la que se hace referencia sobre los temas emergentes en los que se enfocan los profesionales de seguridad, destacando en el noveno puesto la inteligencia de amenazas con un 33 %. Por lo tanto, resulta pertinente desarrollar una investigación asociada con el propósito de plantear un modelo que pueda ser aplicado por las instituciones estatales de Colombia y sacar provecho de sus beneficios.

Lo anterior, se encuentra enmarcado dentro de las competencias y habilidades que busca desarrollar el programa de maestría, desde la gestión estratégica y la aplicación de la tecnología para desarrollar proyectos innovadores que generen procesos de mejora, que en este proyecto estarían enfocados en la ciberseguridad de las entidades gubernamentales y de los usuarios de internet en general.

Un aspecto de importancia tiene que ver con la información existente, que de manera argumentativa ha generado elementos de estudio y de análisis que permiten determinar que los estudios son escasos en esta materia; esto se debe a las limitantes que inhabilitan de manera constante la creación de nuevas estrategias que logren anticipar o focalizar la amenaza como parte de la orientación de los actores de la amenaza (Sun, y otros, 2023). Asimismo, la composición del ciberespacio trae consigo estos nuevos retos que no han sido resueltos por lo antes expuesto, y se hace cada vez más complejo reducir la brecha entre la comisión de la conducta y la afectación a los activos sensibles o críticos del país.

Finalmente, es importante definir un modelo estándar de CTI para que las organizaciones gubernamentales puedan alinearse a una estrategia, para minimizar la materialización de riesgos cibernéticos en las entidades gubernamentales. Así mismo, un modelo permite definir procesos y procedimientos genéricos que pueden aplicarse y ajustarse según los requerimientos y capacidades puntuales de cada organización, permitiendo la integración de múltiples organizaciones.

4. Marco Teórico

El mundo cada vez es más digital y ha sido impactado por el incremento de la migración de las organizaciones de un contexto físico al ejercicio del ciberespacio, cambiando con ello el modelo de negocio centrado en producto a un modelo de negocio centrado en servicios basados en tecnologías digitales (Soto Setzke, Riasanow, Böhm, & Krcmar, 2021). Esta relación entre el componente tecnológico y la infraestructura, sumado al sinnúmero de conflictos subsecuentes en el ciberespacio, ha generado que la presencia de riesgos cibernéticos varíe de acuerdo con el nivel de servicios brindado por cada entidad. Por tal razón, variables como el tamaño de la organización, el tipo de infraestructura tecnológica, los sistemas operativos, el software de aplicaciones, entre otros, representan un mayor o menor riesgo de ciberataques (Dahj, 2022).

Cada entidad afronta diversos retos dependiendo del sector en el que se desenvuelve. Factores como el tamaño, el tipo de estructura orgánica, los objetivos estratégicos, el producto o servicio ofrecido, entre otros, definen la cantidad de recursos orientados a la ciberseguridad y la adquisición de controles tecnológicos. No es lo mismo un banco, que una universidad o un hospital o una entidad gubernamental, puesto que el núcleo del negocio es distinto y, por ende, se deben aplicar medidas diferentes para minimizar el riesgo de ataques informáticos a sus infraestructuras tecnológicas. Por lo anterior, el CTI surge como un mecanismo de respuesta a las amenazas específicas de cada sector, con el propósito de orientar la toma de decisiones en cuanto a las contramedidas de seguridad. Básicamente, el enfoque es el de comprender las ciberamenazas que pueden atentar contra el núcleo del negocio y el origen de estas. (Planque, 2017).

4.1. Inteligencia de amenazas cibernéticas

En atención al ámbito empresarial y comercial, el ofrecimiento de servicios enfocados en CTI vienen aumentando, ejemplo de ello, Fireeye, Mandiant, CrowdStrike, IBM, etc. Sin embargo, cada una ofrece su propia versión del concepto de CTI y lo proyecta por medio de un producto, lo que dificulta la elección para aquellas entidades que desean adquirir este tipo de servicios. Con base en lo anterior, el concepto de inteligencia puede ser aplicado en diferentes contextos, como el militar, los negocios, el gubernamental y finalmente en el ciberespacio. De acuerdo con Planque (2017), a partir de la combinación del significado de la palabra inteligencia y amenaza, define CTI como *el resultado del proceso que combina información para crear una visión general de un adversario y sus intenciones, tácticas, técnicas y procedimientos (TTP's).*

Para Dahj (2022), CTI es un proceso mediante el cual se recolecta y procesa información que ayude a evitar la ocurrencia de ciberataques, por lo cual, las organizaciones, de forma proactiva, toman decisiones en cuanto al tipo de herramientas de seguridad, que deberán ser implementadas para proteger la infraestructura tecnológica. Así mismo, establece que CTI permite analizar el comportamiento de los adversarios o actores de amenazas, con el propósito de comprender las metodologías usadas en los ciberataques, compuestas por TTP's que pueden conllevar a identificar posibles intrusiones.

Otro concepto propuesto por Sülü y Daş (2022), acerca de CTI, hace referencia al conocimiento, habilidades e información que surge a partir de la experiencia relacionada con ataques cibernéticos y los actores de amenaza que lo realizaron, ayudando a las instituciones a entender y mitigar el riesgo de ciberataques ocasionados por una *amenaza persistente avanzada* (APT), *botnets*, *ransomware*, código malicioso, entre

otros. A partir de lo anterior, se definen lineamientos para una defensa eficaz que son entregados a las instituciones, junto con mecanismos adecuados de protección para orientar la toma de decisiones (Sülü & Daş, 2022), que permitan anticipar y prevenir de forma precisa las acciones a realizar para contrarrestar las posibles amenazas.

4.2. Ciclo de inteligencia de amenazas

El ciclo de CTI suele estar basado en el ciclo de inteligencia clásico, consistente en una serie de acciones secuenciales y repetitivas que buscan orientar la toma de decisiones y que ha sido usado en diferentes escenarios de conflicto para describir el proceso de inteligencia militar, el cual ha ido evolucionando con el tiempo como lo menciona (Phythian, 2013). Sin embargo, con base en la literatura que se tome como referencia, puede tener entre cuatro y seis fases.

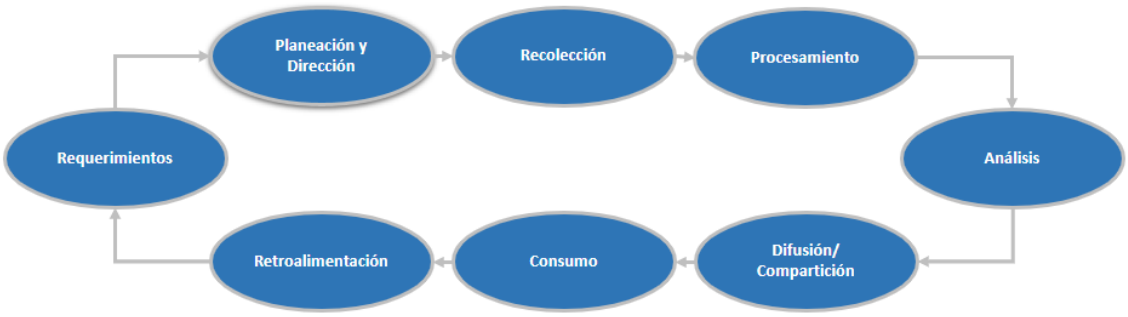
En el caso de Planque (2017), propuso un modelo que consta de dieciséis fases en las que interactúan 3 roles: el cliente, el intermediario y el analista. Cada uno con una serie de procesos que permiten el ciclo continuo del CTI y a su vez identificar a cuáles organizaciones podrían llegar a adaptarse de acuerdo con las necesidades y núcleo del negocio (ver Figura 1).

Figura 1. *Adaptado del Modelo de 16 fases CTI.*

Nota. Elaborado a partir de Planque (2017).

Por su parte, Meli Tsofou (2020) propone un ciclo CTI desde la perspectiva empresarial compuesto por 8 fases. En este modelo se tiene en cuenta la complejidad de mostrar mucho con poco, permitiendo identificar errores de forma temprana a lo largo del ciclo a través del ¿quién?, ¿qué?, ¿cuándo?, ¿dónde?, ¿por qué? y ¿cómo? La respuesta a dichas preguntas, formuladas a partir del conocimiento generado en las respuestas, permite que el proceso de CTI, ayude a los Centro de Operaciones de Seguridad (SOC) y a las personas encargadas de tomar decisiones, a orientar la protección de las empresas para generar bienestar en el ciberespacio (Meli Tsofou, 2020) (ver Figura 2).

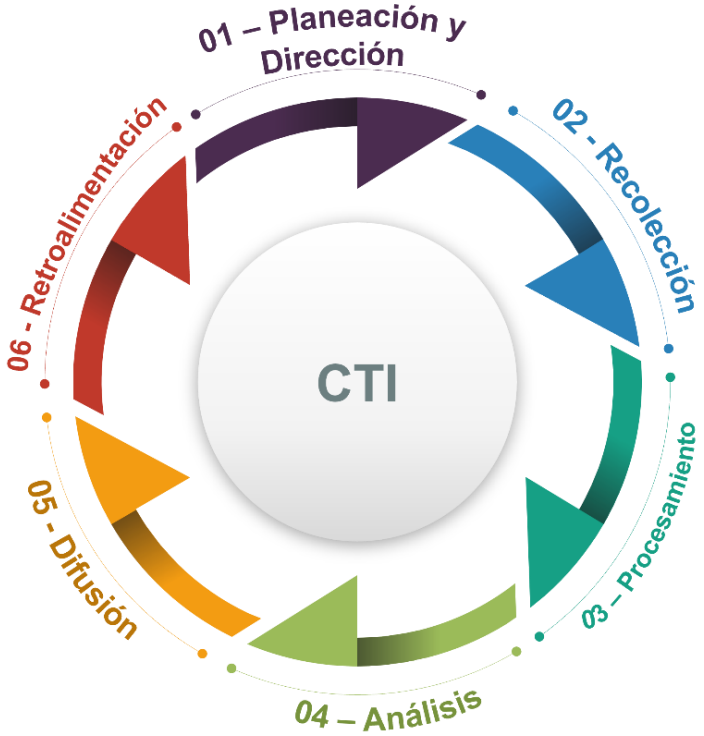
Figura 2. *Adaptado del Modelo de 8 fases de CTI.*



Nota. Elaborado a partir de Meli Tsofou (2020).

En el caso de Dahj (2022), define un ciclo CTI más sencillo en el cual se establecen 8 fases: planificación y dirección, recolección, procesamiento, análisis, difusión/compartición, consumo y retroalimentación. En este modelo, CTI se conceptúa como un proceso continuo, partiendo de la premisa que, así como los actores de amenazas actualizan y mejoran sus metodologías de ataque, también lo deben hacer los encargados de la defensa de las organizaciones. En criterio planteado, las fases necesarias para poder efectuar acciones reactivas. Tienen un componente de acciones que validan o generan un lenguaje enriquecido para la generación de nuevas formas de información, que permiten facilitar la creación de directrices a las organizaciones para ser tanto reactivas como proactivas (ver Figura 3).

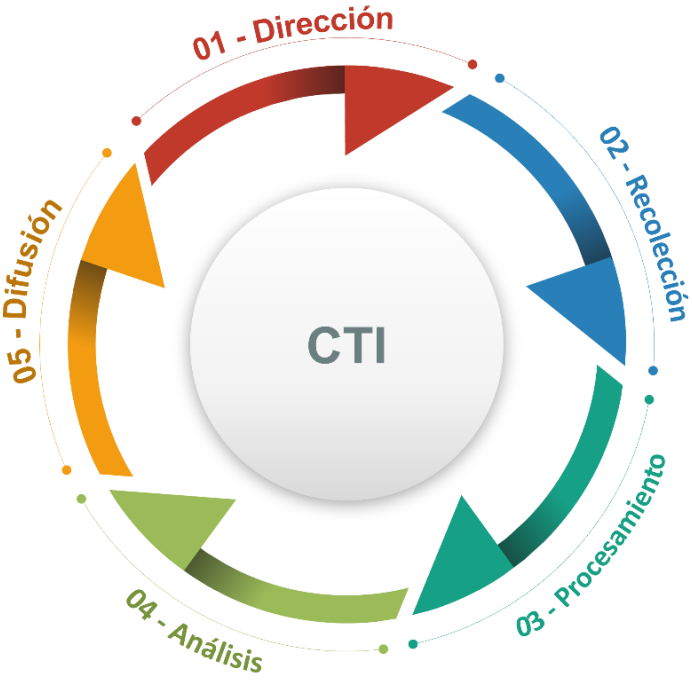
Figura 3. *Adaptado del Ciclo de 6 fases CTI.*



Nota. Propuesto por Mastering Cyber Intelligence Dahj (2022).

El Centro Nacional de Seguridad Cibernética (NCSC) de Reino Unido mediante una guía de CTI para gobierno, establece un ciclo de 5 fases (Hodigital, 2019). Para ello define CTI como un proceso de fases orientada a producir inteligencia, que permita comprender las motivaciones, capacidades y modo de actuar de los adversarios, para generar contramedidas. Lo anterior, partiendo del contexto clásico de la inteligencia militar, definido en las siguientes fases: Dirección, Recolección, Procesamiento, Análisis y Difusión (ver Figura 4).

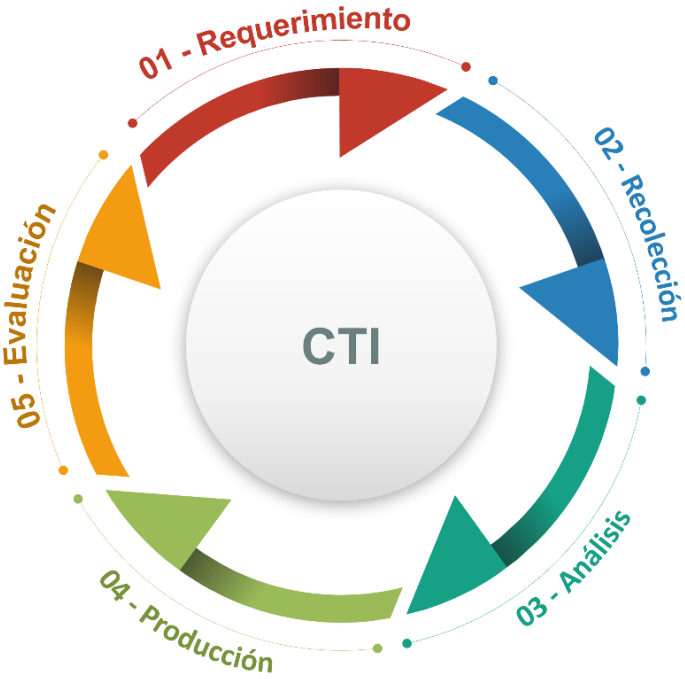
Figura 4. *Adaptado del Ciclo CTI NCSC.*



Nota. Propuesto por el Centro Nacional de Seguridad Cibernética Hodigital (2019).

De forma previa, (Chismon & Ruks, 2015) en el desarrollo de una investigación en la que participó el Equipo de Respuesta ante Emergencias informáticas de Reino Unido (CERT-UK) y el Centro para la Protección de la Infraestructura Nacional de Reino Unido (CPNI), estableció un ciclo CTI de 5 fases: Requerimientos, Recolección, Análisis, Producción y Evaluación. Este se enfoca en el desglose de funciones específicas, teniendo en cuenta las capacidades del personal para desarrollar tareas en cada una de las fases del ciclo, lo que permite evidenciar posibles falencias en cada una de ellas (ver Figura 5).

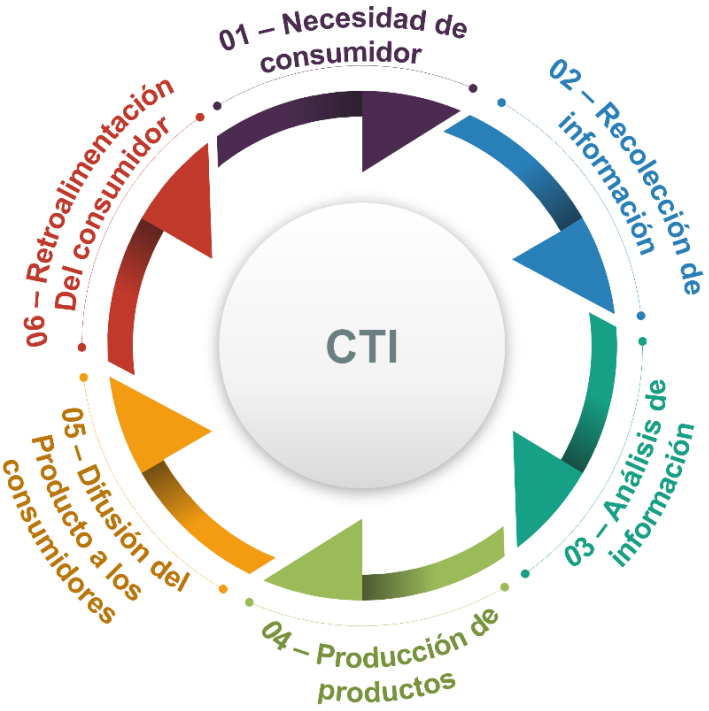
Figura 5. *Adaptado al Ciclo CTI CPNI.*



Nota. Propuesto por el Centro Nacional de Seguridad Cibernética Chismon & Ruks (2015).

En 1996 la Federación de Científicos de América (FAS) definió un ciclo de inteligencia tradicional de 6 fases: Necesidad de consumidor, Recolección de Información, Análisis de información, Producción de Productos, Difusión del Producto a los consumidores y retroalimentación del consumidor. Por medio este se establece la necesidad de proporcionar información oportuna y relevante a quienes toman decisiones, desarrollan políticas o definen estrategias de combate. Bajo este contexto, el modelo FAS de inteligencia tradicional puede ser aplicado a los requerimientos actuales de CTI (Federación de Científicos de América, 1996) (ver Figura 6).

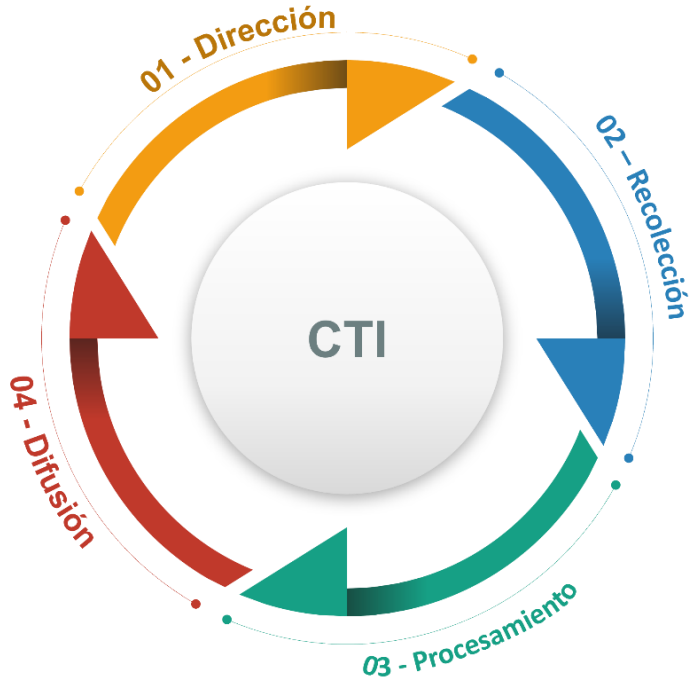
Figura 6. *Adaptado del Ciclo de inteligencia FAS.*



Nota. Propuesto por la Federación de Científicos de América (1996).

La Organización del Tratado del Atlántico Norte (OTAN) desclasificó un documento en 2016, en el que se da a conocer la doctrina de inteligencia aplicada en los países integrantes de la alianza. En este documento se establece que el ciclo de inteligencia está compuesto por 4 fases: *Dirección, Recolección, Procesamiento y Difusión.* Este consiste en una secuencia de actividades mediante la cual se obtiene información que es ensamblada y convertida en inteligencia, para ser puesta a disposición de los usuarios. La interacción entre fases es coordinada por medio de la gestión de requisitos y recolección de inteligencia (Nato Standard, 2016) (ver Figura 7).

Figura 7. *Adaptado del Ciclo de inteligencia OTAN.*



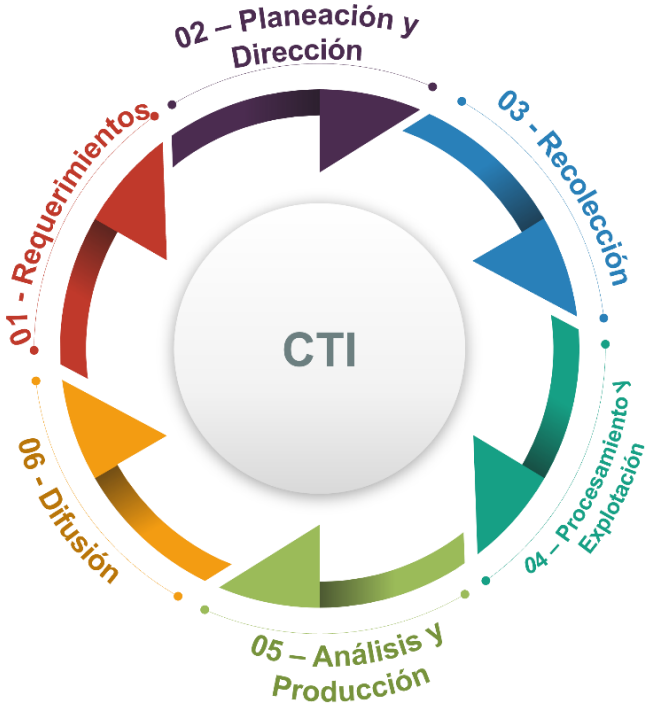
Nota. Propuesto por la Organización del Tratado del Atlántico Norte. Nato Standard (2016).

Así mismo, la OTAN define su modelo como un proceso vital en todas las operaciones de tipo militar, donde incluyen el ciberespacio como un dominio donde sus aliados recopilan, analizan y comparten información de acuerdo con la visión estratégica de cooperación entre sus integrantes. (North Atlantic Treaty Organization, 2023).

La Oficina Federal de Investigación (FBI) de Estados Unidos, establece un ciclo de inteligencia de 6 fases: Requerimientos, Planeación y Dirección, Recolección, Procesamiento y Explotación, Análisis y Producción, seguido de la Difusión. Este se define como una colaboración activa y fluida entre las fases, que permite orientar la toma

de decisiones y acoplarse a las nuevas amenazas (Federal Bureau Of Investigation, 2017) (ver Figura 8).

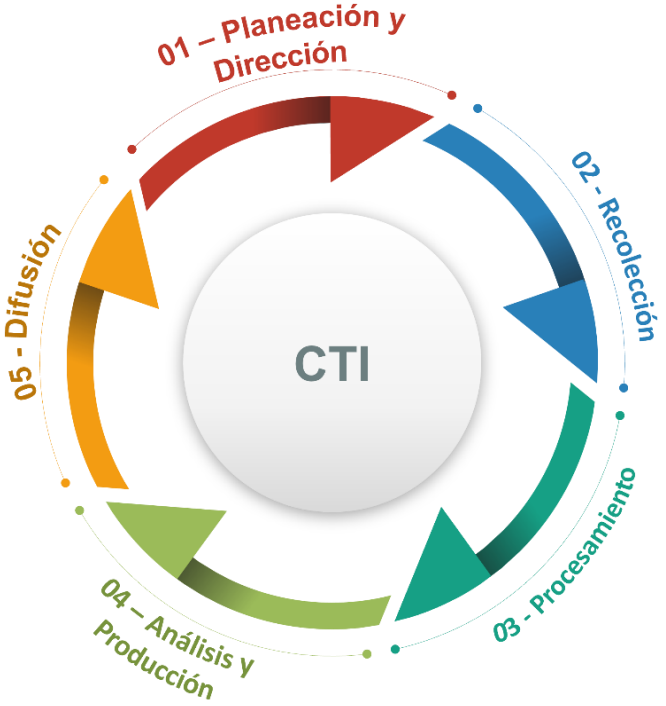
Figura 8. *Adaptado del Ciclo de inteligencia FBI.*



Nota. Propuesto por la Oficina Federal de Investigación. *(FBI)*

La Agencia Central de Inteligencia (CIA) determina un ciclo de inteligencia de 5 fases: Planeación y Dirección, Recolección, Procesamiento, Análisis y Producción, para proceder con la Difusión. Este mecanismo convierte datos sin ningún tipo de procesamiento en información procesada, la cual permite a los tomadores de decisiones una orientación clara para la realización de políticas accionables en diversos contextos (CIA, 2001) (ver Figura 9).

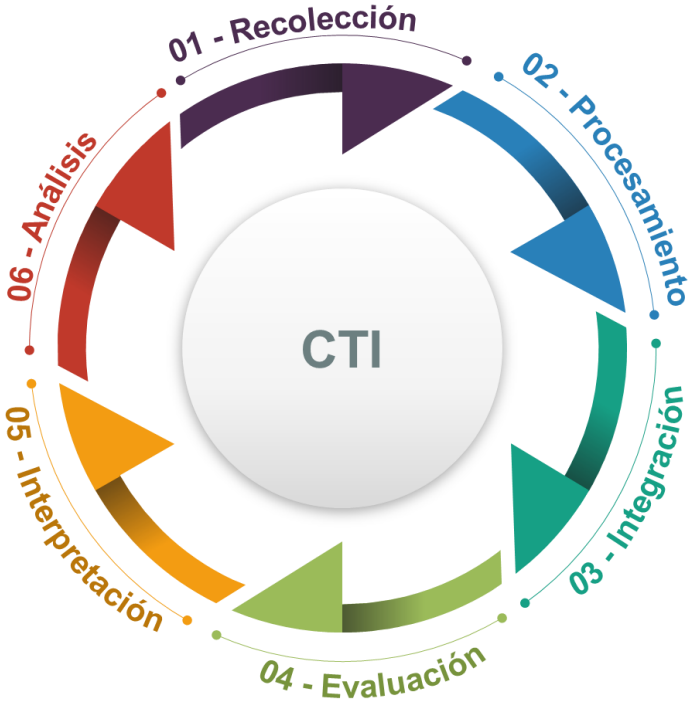
Figura 9. *Adaptado del Ciclo de inteligencia CIA.*



Nota. Propuesto por la Agencia Central de Inteligencia. CIA (2001).

La Comisión Australiana de Inteligencia Criminal (ACIC) en la estrategia de gestión criminal de 2017, establece un ciclo de inteligencia como un proceso de 6 fases: Recolección, procesamiento, integración, evaluación, interpretación y análisis de información. En este transforma porciones de datos en conocimiento o entendimiento por medio del análisis efectuado con pensamiento crítico, que ayude a la resolución de problemas. A partir de lo anterior, se desarrolla un producto que será difundido para apoyar los procesos de tomas de decisiones en diferentes niveles, como pueden ser el estratégico, operativo o táctico (ver Figura 10).

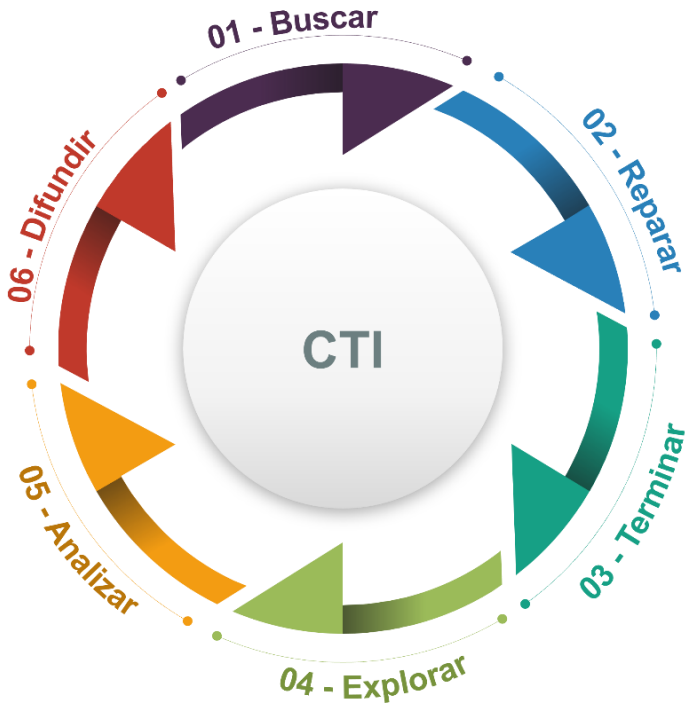
Figura 10. *Adaptado del Ciclo de inteligencia ACIC.*



Nota. Propuesto por la Comisión Australiana de Inteligencia Criminal. *(ACIC, 2017)*.

El Foro de Respuesta a Incidentes y Equipos de Seguridad (FIRST), adopta un modelo alternativo de ciclo de inteligencia usado generalmente en operaciones militares denominado F3EAD, el cual puede aplicarse a CTI y consta de 6 fases: Buscar, Reparar, Terminar, Explotar, Analizar y Difundir. Este ciclo permite dar respuesta a interrogantes de nivel táctico priorizadas cuyo impacto se verá reflejado a nivel estratégico en las organizaciones. Esta metodología debe ser considerada como un soporte al ciclo de inteligencia, puesto que se enfoca en ser rápido y responsivo ante los requerimientos de nivel operacional (First, 2015) (ver Figura 11).

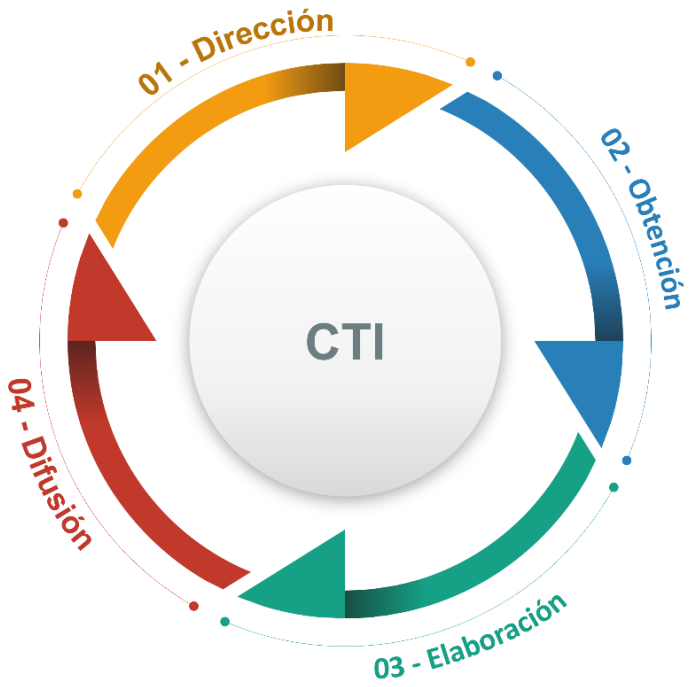
Figura 11. *Adaptado del Ciclo de Inteligencia FIRST.*



Nota. Propuesto por el Foro de Respuesta a Incidentes y Equipos de Seguridad. *(FIRST)*

Se evidencian otros modelos de inteligencia que pueden llegar a ser aplicados y los cuales constan de cuatro fases, como lo es el establecido por el Centro Nacional de Inteligencia de España, en el que se establece la dirección, obtención, elaboración y difusión (Inteligencia, 2021). Este a su vez es similar al modelo propuesto por la OTAN denominado JISR (Inteligencia, vigilancia y reconocimiento conjuntos) de acuerdo con lo establecido por (Martínez Viqueira, 2016). A través de este ciclo se busca facilitar el proceso de toma de decisiones (ver Figura 12).

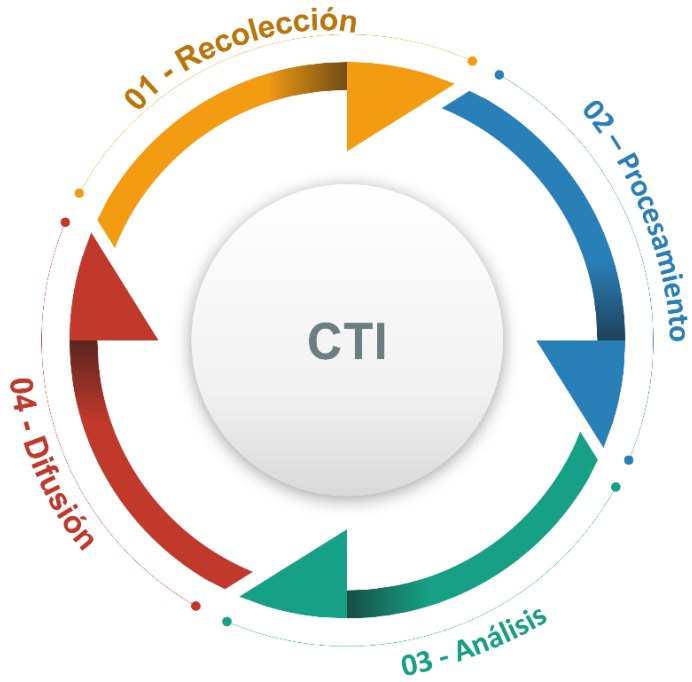
Figura 12. *Adaptado del Ciclo de Inteligencia CNI.*



Nota. Propuesto por el Centro Nacional de Inteligencia de España. *(CNI, 2021)*

En Colombia existen organismos que desarrollan actividades de inteligencia con criterio orientador, las cuales se rigen bajo los parámetros establecidos en la Ley estatutaria 1621 de 2013. Dentro de la definición de la función de inteligencia y contrainteligencia descrita en el Artículo 2 de la ley en mención, se establecen 4 fases para el ciclo de inteligencia: Recolección, Procesamiento, Análisis y Difusión de información. Lo anterior, "*con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional, y cumplir los demás fines enunciados en esta ley."* (Ley Estatutaria 1621 de 2013, s.f.) (ver Figura 13).

Figura 13. *Adaptado del Ciclo de inteligencia Colombia.*



Nota. Propuesto por los organismos que desarrollan actividades de inteligencia en Colombia. Ley Estatutaria 1621 del 2013.

4.3. Fases del ciclo de inteligencia de amenazas

A partir de lo anterior, se definen las fases de uso común en los modelos de CTI, así:

Planificación y Dirección: corresponde a la fase inicial en la que se definen los requerimientos específicos que sirven de orientación para establecer una hoja de ruta. Representa la supervisión del esfuerzo y enfoque del CTI en general, donde se identifica, emite, prioriza, desarrolla, convierte, distribuye, produce y monitorea los resultados obtenidos para que estos cumplan con los objetivos propuestos dentro de todo el ciclo (Sakib, 2022).

Recolección: es la segunda fase, en la que se recopila información que sirva al cumplimiento de los objetivos planteados en la primera fase para emitirla posteriormente hacia el procesamiento. Para ello se deben establecer métodos de recolección donde los datos provengan de diversas fuentes técnicas y, con ello, se enriquezca la construcción de un producto final de calidad. Esto permitirá, en las siguientes etapas, contradecir o validar hipótesis a partir de la obtención de información rápida, segura, confiable y sólida (Sakib, 2022).

Procesamiento: es la tercera fase, en la que los datos obtenidos en la recolección se transforman en insumos ideales para la creación de inteligencia. De esta forma, en la siguiente fase los analistas pueden hacer uso de información procesada en formato legible y fácil de entender. En esta etapa se da significado a los datos, de forma que sean útiles para la organización. En el caso de CTI, suele hacerse uso de plataformas que ayudan a correlacionar información, permitiendo identificar patrones y puntos de interacción que coincidan en las diferentes fuentes, lo que permite entender el comportamiento de los actores maliciosos (Dahj, 2022).

Análisis: es la cuarta fase, en la que la información procesada se convierte en Indicadores de compromiso (IoCs) que se pueden transformar en alertas o contextos, dirigidos a las partes interesadas a quienes se informan de posibles amenazas potenciales. En esta etapa se procede a evaluar e interpretar la información procesada, con lo cual, el analista puede determinar los tipos de datos que son irrelevantes y cuyos valores no aportan a la producción de inteligencia. De esta forma, se puede orientar la fase de recolección, con el propósito de obtener información específica que cumpla con los criterios y objetivos establecidos en la fase de planificación y dirección. Finalmente, en esta fase se crea el producto final de inteligencia, el cual brindará al usuario la comprensión de las amenazas para plantear estrategias que permitan contrarrestarlas (Sakib, 2022).

Difusión: en esta quinta fase, el objetivo es el de entregar el producto de inteligencia al usuario final en un formato comprensible, con base en los requerimientos de la primera fase. En dicho objeto encontrará información a partir de la cual pueda crear contramedidas de las amenazas. De igual forma, le permitirá conocer el nivel de exposición y las metodologías usadas por los actores de amenaza. Este paso debe realizarse garantizando que el producto llegue a su destino, para lo cual debe existir un mecanismo idóneo de comunicación entre las partes. Así mismo, se debe tener en cuenta el tipo de usuario final, por lo que la difusión debe realizarse a quienes deba llegar directamente la información y en el lenguaje apropiado (gerencial, estratégico y técnico).

Retroalimentación: es la fase final del CTI y que a su vez conecta con la primera fase. Una vez las partes interesadas reciben el producto final, y de forma posterior a la revisión de la información y posible toma de decisiones, se procede a evaluar la calidad y efectividad del producto, informando los aspectos a mejorar que deben ser dados a conocer antes de dar inicio al próximo ciclo CTI. Lo anterior refinará cada una de las fases con el propósito de atender las recomendaciones dadas. Para ser más prácticos, esta etapa define el nivel de satisfacción del cliente y el accionar a realizar una vez recibida la retroalimentación, puesto que formará parte de los objetivos en la próxima fase de planificación y dirección (Dahj, 2022).

4.4. Tipos de inteligencia de amenazas

Los datos de CTI pueden ser obtenidos de diferentes fuentes, las cuales pueden ser técnicas (herramientas de seguridad perimetral, *sandbox*, consolas de antivirus, gestores de eventos, entre otros) o humanas (foros de internet privilegiados, información de un tercero, blogs, etc.). A partir de los datos adquiridos, se genera un producto de inteligencia cuyo contenido puede estar enfocado a indicadores de compromiso (IoCs),

contextos sobre ciberataques, metodologías, vulnerabilidades, *phishing*, *exploits*, accesos no autorizados, impactos adversos y con todo ello las estrategias para contrarrestar posibles amenazas a las infraestructuras tecnológicas (Sakib, 2022).

Con base en el alcance, los objetivos planteados y las partes interesadas, los productos desarrollados en CTI se pueden clasificar en cuatro categorías: estratégicos, operacionales, técnicos y tácticos como hace mención la agencia de la Unión Europea para la Ciberseguridad (ENISA, 2019).

Inteligencia de amenazas estratégica: está dirigida a la alta dirección puesto que son quienes tienen el poder de tomar decisiones, por lo cual se considera información de alto nivel (Tounsi & Rais, 2018). El propósito de estos productos es orientar a los estrategas en la comprensión de los riesgos cibernéticos en el entorno donde desempeñan su actividad las organizaciones, como también de aquellos que no han sido tenidos en cuenta y que de alguna forma podrían impactar negativamente los activos tecnológicos de la entidad. Con los datos entregados, la alta dirección puede evaluar el daño reputacional, económico y demás aspectos de interés que se pueden desprender de un ciberataque exitoso. También, tendrá pleno conocimiento del historial, la actividad actual y las tendencias futuras de los actores de amenaza. A partir de lo anterior, los tomadores de decisiones asignarán y distribuirán tareas que pueden ir desde la asignación de presupuesto para fortalecer la ciberseguridad o simplemente refinar políticas de seguridad de los dispositivos de protección de la red, que conlleven a mitigar ataques.

Inteligencia de amenazas operacional: los productos están dirigidos a personal que desempeña cargos cuya función es defender las infraestructuras tecnológicas, realizar pruebas de vulnerabilidad y reaccionar ante intrusiones informáticas. La información entregada está relacionada con ataques inminentes, centrándose en los posibles actores de amenaza y las metodologías usadas para llevar a cabo la intrusión.

El contexto hace énfasis en comprender y poder replicar el comportamiento de los adversarios en el escenario real de la organización, con lo cual se orquesten las acciones necesarias para evitar los ataques cibernéticos (Dahj, 2022).

Inteligencia de amenazas técnica: corresponde a información destinada a ser incorporada en las herramientas de seguridad, con el objetivo de monitorear y alertar en caso de coincidir con alguno de los parámetros suministrados. De acuerdo con (Tounsi & Rais, 2018), estos datos se denominan IoCs que pueden ser agregados a cortafuegos, antivirus, detectores de intrusión, protección de correo, entre otros. Comúnmente los IoCs suelen corresponder a direcciones IP, urls, *hash* de archivos y dominios, asociados a comportamientos anómalos que han sido observados de forma previa en otros ciberataques y que pueden llegar a desencadenar algún tipo de intrusión en los sistemas de información sino son tenidos en cuenta. Quienes reciben este tipo de productos suelen tener roles de administración y gestión de herramientas de seguridad.

Inteligencia de amenazas táctica: este tipo de productos está enfocado a conocer las TTP’s utilizadas en los ciberataques, para lo cual se utiliza un modelado de amenazas como el de MITRE ATT&CK (Tácticas, Técnicas y Conocimiento Común del Adversario), un framework que recopila y analiza el comportamiento de los actores maliciosos, al igual que sus métodos (Strom, y otros, 2020), permitiendo identificar el modus operandi. Esta información permite a los encargados de la ciberseguridad establecer defensas y generar políticas actualizadas, que correspondan a la realidad de los ataques. A partir de lo anterior, los defensores pueden ajustar constantemente las metodologías de defensa, crear campañas de concientización, analizar escenarios de ataque y demás que consideren. La información de las TTP´s es entregada a quienes desempeñan cargos de atención a incidentes informáticos, puesto que, a partir de la ocurrencia de estos en otras

entidades, se obtiene experiencia que genera valor para evitar afectaciones a las infraestructuras propias (Tounsi & Rais, 2018).

4.5. Indicadores de compromiso

Los IoCs son componentes clave del CTI, puesto que permiten identificar rápidamente actividades maliciosas en las infraestructuras tecnológicas y su vez conocer las TTPs de los actores de amenaza. Son de carácter volátil y funcionales por tiempo limitado, debido al cambio constante de las metodologías usadas por los atacantes. Sin embargo, durante el periodo de actividad pueden generar bastante daño, por lo cual, el monitoreo anticipado conlleva a evitar posibles intrusiones. Estos datos son de carácter técnico y desplegables en herramientas de seguridad perimetral. Muchos IoCs suelen ser recolectados de plataformas abiertas donde los profesionales de ciberseguridad suelen publicarlos y cuyos usuarios suelen ser funcionarios de SOC. Generalmente, los IoCs de acceso público son los de menor vida útil, puesto que los actores de amenaza al quedar evidenciados en actividades maliciosas proceden a modificarlos. También existen algunos cuyo acceso es privilegiado y pueden llegar a ser accesibles por medio de una buena estrategia de CTI (Villalón Huerta, Ripoll Ripoll, & Marco Gisbert, 2022).

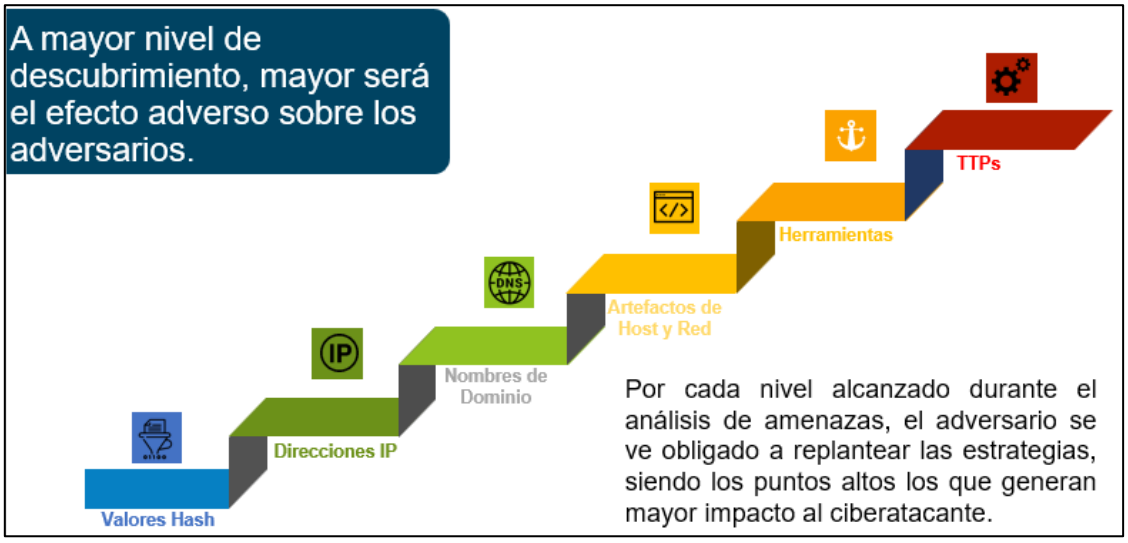
La definición básica de un IoC es que corresponde a una pieza de información útil que permite reconocer un sistema de información que ha sido comprometido. Una conexión a una dirección IP, la detección de un *hash* o acceso a una URL son indicios de una posible intrusión. Para (Villalón Huerta, Ripoll Ripoll, & Marco Gisbert, 2022), muchos investigadores aplican la siguiente clasificación de tres categorías de IoCs, con base en su complejidad y granularidad, así:

Atómicos: son los que se encuentran en su mínima expresión y que representan directamente una posible afectación a las infraestructuras tecnológicas. Dentro de esta categoría se pueden encontrar direcciones IP, direcciones de correo electrónico y nombres de dominio.

Calculados: corresponden a datos que solo pueden identificarse con tecnología. Los *hashes* de archivos maliciosos, porciones de código específicos, la firma comportamental de *software* malicioso son ejemplos de IoCs de este tipo.

Comportamentales: son la colección de las dos categorías anteriores. Estos permiten identificar posibles perfiles de los actores de amenaza a partir de las TTP's usados de forma general. Lo anterior, teniendo en cuenta que para los atacantes es imposible crear campañas maliciosas por cada víctima, por lo cual, las metodologías usadas suelen ser las mismas durante cierto tiempo, hasta que el CTI los obliga a cambiar. Un ejemplo de esta categoría, son los correos que suplantan entidades legítimas, enviados con enlaces o archivos que conllevan a la descarga de otros archivos con clave, para que las víctimas los ejecuten y así se inicie la conexión a un comando y control (ver Figura 14).

Figura 14. *Análogo de la Pirámide del Dolor.*



Nota. Propuesto por *(Bianco, 2014)*.

4.6. Beneficios de la inteligencia de amenazas

El éxito de una estrategia de CTI radica en el intercambio de información múltiple, puesto que su aplicación de forma individual conlleva a resultados poco efectivos, lo que da ventaja a los actores de amenaza. Por tal razón, las organizaciones que hagan parte del ecosistema digital deberían aprovechar las ventajas que brinda el CTI. Acceder y entregar información de amenazas por medio del uso compartido, permite mejorar las capacidades defensivas de las infraestructuras en las organizaciones, ya que según (Skopik, 2018), el conocimiento, la experiencia y las capacidades, de forma conjunta, son mucho más efectivas, dando una visión del contexto interno por medio de datos externos para llevar a cabo el despliegue de acciones contundentes.

Cuando se efectúa un ciberataque por cualquier vector y logra su objetivo, quiere decir que encontró una brecha que puede ser explotada, por lo cual, realizará una búsqueda de víctimas con características similares. Dado el caso de que la primera víctima no comparta los vectores de ataque y los IoCs asociados, puede poner a otras organizaciones en riesgo de afectación. En cambio, si la situación es contraria y se comparte información detallada sobre los hallazgos evidenciados durante la intrusión, los datos serán relevantes para evitar afectaciones en otras entidades, permitiendo identificar si son vulnerables a una amenaza y así generar estrategias, fortalecer campañas de concientización, realizar acciones de mitigación, activar los protocolos de respuesta a incidentes, entre otras (Skopik, 2018).

4.7. Retos de la inteligencia de amenazas

Aunque la CTI tiene grandes beneficios, también tiene grandes retos. El principal es el de crear la confianza que se debe establecer entre las entidades que quieren participar en el intercambio de información. Algunos de los datos pueden ser considerados como sensibles a la vista de terceros, ya que al informar los detalles de una intrusión estarían evidenciando la postura de seguridad con la que cuenta la

organización, lo que para los actores de amenaza sería información valiosa. Así mismo, la metodología usada en el ataque representaría un daño a la reputación, en el caso de que no tuviese un nivel de sofisticación avanzado, dejando al descubierto la facilidad de materializar los riesgos cibernéticos en la organización. Lo anterior, representa la causa del porqué las entidades víctimas de ciberataques son reacias a compartir información con otros (Skopik, 2018).

Tabla 1. Comparativa de ciclos de inteligencia aplicables al CTI.

Modelo de ciclo de inteligencia	Características	Beneficios
Ciclo de Inteligencia Planque	16 fases. Divididas en tres roles: cliente, intermediario y analista.	Adaptable con base a las necesidades y núcleo del negocio.
Ciclo de Inteligencia Meli Tsofou	8 fases. Enfocado en el contexto empresarial.	Orientado a mostrar mucho con poco. A su vez permite identificar errores en cada fase del ciclo.
Ciclo de Inteligencia Dahj	6 fases. Bajo la premisa de que los actores de amenaza se actualizan, por lo tanto, los encargados de defender también deben hacerlo.	Generación de lenguaje enriquecido para crear directrices que orienten a las organizaciones a ser reactivas y proactivas.
El Centro Nacional de Seguridad Cibernética (NCSC)	5 fases. Busca comprender las motivaciones, capacidades y actuar de los adversarios.	Tiene como objetivo producir inteligencia para generar contramedidas.
El Centro para la Protección de la Infraestructura Nacional de Reino Unido (CPNI)	5 fases. Despliega funciones específicas por fase y permite descubrir falencias oportunamente.	Soporta las fases según las capacidades del personal que desarrolla cada una.
Federación de Científicos de Américas (FAS)	6 fases. Aplicado en la inteligencia tradicional para proporcionar información oportuna en el ámbito de políticas o estrategias de combate.	Puede ser aplicado en una estrategia de CTI a partir de los requerimientos actuales del contexto.
Organización del Tratado del Atlántico Norte (OTAN)	4 fases. Doctrina de inteligencia aplicada por los países de la alianza.	Aplicable a CTI, ya que incluye el ciberespacio como un dominio para obtener información y ser convertida en insumo para los usuarios.
Oficina Federal de Investigación (FBI)	6 fases. Establece una colaboración activa y fluida entre las fases.	Permite acoplarse a las nuevas amenazas del entorno incluyendo las del ciberespacio.

Agencia Central de Inteligencia (CIA)	5 fases. Transforma datos sin tratamiento en información procesada	Generación de políticas accionables a partir de la orientación de los datos.
Comisión Australiana de Inteligencia Criminal. (ACIC)	6 fases. Análisis efectuado con pensamiento crítico para dar resolución a problemas.	Desarrollo de productos para apoyar la toma de decisiones estratégicas, operativas o tácticas.
Foro de Respuesta a Incidentes y Equipos de Seguridad (FIRST)	6 fases. Usado para operaciones militares y aplicable a CTI por ser rápido y responsivo.	Permite dar respuesta a interrogantes priorizadas en el ámbito táctico, cuyo resultado se refleja en el nivel estratégico.
Centro Nacional de Inteligencia de España (CNI)	4 fases. Aplicado por el organismo público encargado de prevenir y evitar peligros que atenten contra la integridad del territorio de España.	Facilita la toma de decisiones mediante un proceso de fases definidas, mediante la coordinación e intercambio de información de forma ágil y completo.
Ciclo de Inteligencia Colombia	4 fases. Establecido mediante la Ley estatutaria 1621 de 2013 para actividades de inteligencia y contrainteligencia realizado por entidades específicas para la salvaguarda del estado colombiano.	El alcance de la ley establece la coordinación y cooperación entre entidades, como también el deber de colaboración de entidades públicas y privadas.

Nota. Elaboración propia.

Otro de los retos que se evidencian en CTI, es la implementación propia del procedimiento a nivel organizacional. La incorporación en los procesos de la organización y su alineación para cumplir con los objetivos de compartir información con terceros conlleva a evaluar el tipo de información que será accesible por otros, la forma de entrega y los roles de responsabilidad. De igual forma, garantizar que la información recibida de terceros cumpla con el mismo protocolo (Skopik, 2018).

A nivel técnico surgen otra serie de retos. La interacción entre sistemas propios y de terceros requiere de un gran nivel de automatización para que el CTI tenga un nivel alto de efectividad. Aunque también es necesaria la interacción humana para comprender el alcance y riesgo potencial de la información, ya que en algunos casos lo que se puede considerar sospechoso para unas entidades, puede no serlo para otras. Todo depende del Core de negocio y el contexto en el que se desenvuelvan (Skopik, 2018).

Al final, compartir información de CTI trae consigo riesgos legales y normativos que deben ser de mutuo conocimiento entre las partes. Sobrepasar los límites

establecidos a nivel de leyes y normas, puede conllevar a daños jurídicos en las organizaciones. La fuga o exposición de datos representan una de las mayores afectaciones a las entidades, por lo que, hacer publicaciones al respecto por parte de terceros va en contravía de la protección de datos personales. Sin embargo, el no informar puede acarrear sanciones cuyas consecuencias pueden ser graves de acuerdo con el alcance legal de cada país.

4.8. Panorama actual de la inteligencia de amenazas

En el 2018, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) dedicó una sección a CTI en el informe del panorama de amenazas, en el que resalta el crecimiento del interés en la temática durante los cinco años anteriores a la publicación del documento. Lo anterior a partir de la necesidad de comprender las amenazas, el comportamiento de los actores de amenazas y las TTP’s al momento de realizar un ciberataque. Esto con el propósito de adoptar medidas adecuadas de protección a través de estrategias proactivas, para lo cual es imperativo implementar CTI en las organizaciones.

La demanda de formación, herramientas y buenas prácticas en CTI sigue creciendo, puesto que las organizaciones requieren de datos y contextos actualizados de las amenazas. Sin embargo, en el informe de (ENISA, 2019), se deja claro que las grandes empresas son las que tienen mayor posibilidad de acceder a este tipo de información, debido a que cuenta con mayor presupuesto y gracias a ello pueden implementar SOCs con su respectiva infraestructura de ciberseguridad, en la cual pueden generar y consumir información de CTI. Algo que a las medianas y pequeñas empresas se les puede dificultar, dejándolas expuestas en el ciberespacio.

De la temática de CTI vista en el informe de (ENISA, 2019), se puede analizar o preliminarmente inferir que las empresas, los gobiernos y entidades en general deben comprometerse con el desarrollo de CTI, para lo cual, se deben implementar repositorios de datos, definir un ciclo estándar, madurar modelos existentes, fortalecer habilidades, ofrecer servicios y generar cultura.

Por otra parte, en el último reporte sobre el “Panorama de amenazas” (ENISA, 2022), se relacionan los sectores que más incidentes presentaron de junio de 2021 a junio de 2022. Dentro de estos se evidencia que el sector gubernamental y de administración pública son los más afectados, ya que con una cifra del 24 % ocupan el primer lugar, seguido por los proveedores de servicios digitales con un 13 % y, en tercer lugar, con un 12 %, la afectación de usuarios en general. De lo anterior, se resalta que el sector más afectado podría tener un impacto mayor, toda vez que los servicios ofrecidos son de mayor alcance que los privados, lo que representa un mayor daño colateral.

De igual forma, el informe de ENISA (2022) describe las amenazas frecuentes de mayor impacto que se presentaron en los sectores mencionados anteriormente, consistentes en *ransomware*, código malicioso, ingeniería social, fuga de datos, denegaciones de servicio, daño de infraestructura y censura del internet, eventos de desinformación y ataques a las cadenas de suministro. Esto indica que las organizaciones deben estar a la vanguardia de los contextos de amenazas, acciones en las que CTI puede ser de gran utilidad.

4.9. Contexto de inteligencia de amenazas cibernéticas en Colombia

Desde el 2011, Colombia ha venido desarrollando capacidades en ciberseguridad para fortalecer las defensas contra los actores de amenazas. A partir de lo anterior, fueron elaborados los documentos CONPES 3701 (2011), CONPES 3854 (2016) y CONPES 3995 (2020), enfocados en mejorar la postura de seguridad digital del país, creando las condiciones suficientes para la protección del ciberespacio. A su vez, buscan

integrar a las partes interesadas para cooperar, colaborar y asistir en la seguridad del entorno digital creando confianza digital a sus ciudadanos. También es de resaltar la ley 1273 conocida como la ley de delitos informáticos, en la que se definen las conductas delictivas que convergen en el ciberespacio.

En este aspecto, es importante resaltar el concepto de incidentes informáticos, que corresponde a las afectaciones de confidencialidad, disponibilidad e integridad que ocurren sobre los activos de información y desde esta perspectiva el concepto tiene similitud a delito informático (MINTIC, 2016). La diferencia radica en, para algunos casos, el incidente informático no tiene autor y representa el comportamiento de un sistema de información, dado que, en ocasiones puede llegar a fallar por diversas razones (actualizaciones, ventanas de mantenimiento, entre otras). En el caso de los delitos informáticos, suele existir un actor cuyas intenciones y actividades desarrolladas conllevan a una conducta típica y antijuridica que son catalogadas como conductas penales (Función Pública, Ley 599, 2000).

Existen organizaciones como el ColCERT, CsirtGob, CSIRT PONAL, CaiVirtual, entre otros, a los que se les ha delegado la responsabilidad de salvaguardar los activos de información con los que interactúan los colombianos. Sin embargo, como se observa en los documentos CONPES, las estrategias se han enfocado hacia la parte reactiva, dejando de lado la parte proactiva. Este enfoque se da desde la parte pública, puesto que a nivel privado algunas organizaciones hacen uso de CTI para proteger sus infraestructuras. Por lo anterior, no se identifica una capacidad CTI compartida a nivel gubernamental que minimice el riesgo de amenazas cibernéticas en las entidades del estado. No obstante, es posible que alguna entidad con el conocimiento y experiencia

pudiese liderar la estrategia que permita su implantación. De esta forma se podría minimizar el impacto y alcance de los actores de amenazas.

5. Análisis PESTEL

5.1. Político

El CONPES como máxima autoridad en temas de planeación y en su rol de asesor a nivel gubernamental en cuanto al desarrollo económico y social del país, (CONPES), ha emitido tres documentos asociados a temáticas de ciberseguridad, en los que se determinaron una serie de acciones que conllevaran al cumplimiento de unos objetivos, sin afectar el ordenamiento jurídico, así:

CONPES 3701 de 2011: Lineamientos de Política para ciberseguridad y Ciberdefensa

CONPES 3854 de 2016: Política Nacional de Seguridad Digital

CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.

En las bases del PND 2022-2026, específicamente en *"Seguridad humana y justicia social"* se planteaba la creación de la Dirección Nacional de Seguridad Digital. Sin embargo, en el PND aprobado por el Congreso de la República no se dio viabilidad a esta iniciativa. Adicional a lo anterior, se plantearon dos proyectos de ley para la creación de una agencia nacional de seguridad. En senado, el proyecto 331/23 archivado por falta de ponencia y en cámara el proyecto 023/2023C que a la fecha del presente documento se encuentra en trámite.

5.2. Económico

Previo a la aprobación de la reforma tributaria mediante la ley 2277 de 2022, algunos sectores manifestaron preocupación, entre ellos el tecnológico, ya que por parte del presidente de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) se manifestó que podría llegar a existir encarecimiento de algunos servicios digitales debido al incremento de impuestos sobre estos (Portafolio, 2022).

De acuerdo con el informe de Política Monetaria de Julio, la economía en Colombia siguió reportando altos niveles de actividad, como también mejoras en el mercado laboral, lo que proyecta un descenso en la inflación para lograr la meta propuesta del 3% a finales del 2024 (Banco de la República de Colombia, 2023).

El Departamento Administrativo Nacional de Estadística (DANE) publicó las cifras del producto interno bruto (PIB) del segundo trimestre del 2023, donde se establece el valor total de los bienes y servicios producidos durante el trimestre en mención. La cifra creció el 0.3% respecto al mismo periodo del año anterior y con relación al trimestre anterior decreció el 1.0% (DANE, 2023). Estos valores podrían representar una preocupación para diferentes sectores de la economía, teniendo en cuenta lo manifestado por el exministro de Hacienda José Manuel restrepo sobre la necesidad de "cuidar la economía y sus empresas" (Semana, 2023).

5.3. Social

En Manizales, el ministro TIC Mauricio Lizcano manifestó la inversión de 1.500 millones de pesos, con el objetivo de colocar en marcha la supercomputadora del Centro de Bioinformática y Biología Computacional de Colombia –BIOS-, para fortalecer y llevar a la sostenibilidad estas instalaciones, consideradas como la más importante del país (MinTIC, MinTIC anunció $1.500 millones para el centro BIOS, 2023). De igual forma, se realizó el anuncio de querer "*convertir a Manizales en un epicentro mundial de la ciberseguridad*", por lo cual se destinarían 4.000 millones para capacitación y 10.000 mil millones para consolidar un centro de Operaciones de Ciberseguridad (MinTIC, 2023).

Mediante alianza realizada por Google, Colnodo y MinTIC se ofrecieron 4.000 mil becas para jóvenes colombianos, con el objetivo de fortalecer el ámbito de

ciberseguridad y dar la oportunidad de adquirir nuevas habilidades de alta demanda en la industria, apoyando a su vez la transformación digital (MinTIC, 2023).

Mediante la estrategia de “Sociedad Digital”, MinTIC en alianza con 13 referentes de la industria de tecnología (Cisco, IBM, Microsoft, Oracle, entre otros) generó una oferta de 200.000 mil cursos sobre temáticas como ciberseguridad, inteligencia artificial, internet de las cosas, entre otros, con el propósito de responder a la demanda de talento que se requieren en este sector (MinTIC, 2023).

5.4. Tecnológico

El Índice Nacional de Seguridad Cibernética (NCSI) cuyo propósito es el de medir la preparación que tienen los países para prevenir amenazas cibernéticas y la gestión de incidentes, ubica a Colombia en el puesto 69 del ranking global con relación a su nivel de seguridad cibernética (NCSI, 2022), teniendo en cuenta las evidencias aportadas por los colaboradores y que ha sido verificada por la NCSI.

Según el reporte global de Innovación (WIPO, 2022) realizado junto con la Organización Mundial de la Propiedad Intelectual, Colombia ocupa el puesto 63 dentro del seguimiento realizado a 132 países respecto al estado actual de innovación a nivel mundial. En este se toma como referencia el tema de los resultados del conocimiento y la tecnología en cuanto a su creación, impacto y difusión.

El ministro TIC anunció la creación de un centro de ciberseguridad con el que se busca realizar una transformación misional hacía un enfoque de seguridad digital, con el cual se busca incrementar capacidades para salvaguardar las infraestructuras tecnológicas del país de las diferentes ciberamenazas (Lesme Díaz, 2023).

5.5. Ambiental

Colombia cuenta con Política Nacional para la Gestión Integral de Residuos de Aparatos Eléctricos y Electrónicos (RAEE). En esta se define la hoja de ruta que deben

seguir hasta el 2032 los organismos del estado en todos sus niveles, los sectores productivos y empresarial, como también la sociedad colombiana en general, para contrarrestar el impacto negativo que genera a nivel mundial y local el incremento de los RAEE, cuyos efectos se ven reflejados en la salud de las personas y en el medio ambiente (Minambiente, 2013).

5.6. Legal

Al Código Penal Colombiano se agregó un título denominado “De la protección de la información y de los datos”, por medio de la ley 1273 de 2009. Lo anterior con el propósito de proteger la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos, de las amenazas del existentes en el ciberespacio (Congreso de la República, 2009).

Mediante el Decreto 338 de 2022 se establecen los lineamientos para realizar el fortalecimiento de la gobernanza de la seguridad digital, llevar a cabo la identificación de infraestructuras críticas a nivel cibernético y los servicios esenciales, como también la gestión de riesgos y la respuesta a incidentes de seguridad (Función Pública, Decreto 338 de 2022, 2022).

La ley 1581 de 2012 y su decreto reglamentario 1377 de 2013, tratan de la protección de datos personales, aplicable a cualquier registro que sea susceptible a tratamiento por parte de cualquier entidad sea pública o privada (Función Pública, 2012).

La ley 1621 de 2013 establece el marco jurídico mediante el cual las entidades encargadas de desarrollar actividades de inteligencia y contrainteligencia pueden cumplir su misión constitucional y legal (Función Pública, 2013). En esta también se estable un ciclo de inteligencia que puede ser aplicado a CTI.

6. Hipótesis

Según Hernández-Sampieri & Mendoza-Torres (2018) establece que la hipótesis es una guía para la investigación, mediante la cual se indica lo que se quiere probar, convirtiéndose en una posible explicación del fenómeno investigado a partir de la pregunta de investigación, dada como una respuesta provisional. Bajo este planteamiento y con relación a lo que manifiesta (Aggarwal & Gautam, 2017), los actores de amenaza cada día son más fuertes y la preocupación ante el incremento del uso de aplicaciones en internet, ha hecho que las organizaciones inviertan dinero para proteger sus activos de información, ante lo cual surge la necesidad de adoptar un modelo de inteligencia que permita analizar y reportar de forma anticipada ataques cibernéticos, por lo cual se plantea la siguiente hipótesis en este trabajo de investigación:

La implementación de una estrategia de inteligencia de amenazas cibernéticas anticipa la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos en las entidades gubernamentales de Colombia.

7. Variables

En cuanto al presente proyecto, basados en el objetivo principal con el que se busca definir una estrategia de CTI, el acceso a la información puede representar una limitante, dependiendo desde el punto de vista que se tome. Por un lado, los conceptos, modelos CTI, experiencias e investigaciones son relevantes, teniendo en cuenta que es una temática en crecimiento y cuya literatura es accesible. Sin embargo, obtener información relacionada con la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos en entidades gubernamentales puede ser difícil, por lo cual, el diseño del instrumento a aplicar en la investigación es crucial para obtener buenos resultados.

La continuidad de investigación es factible, ya que al ser una temática en tendencia y creciente a nivel mundial es relevante para futuros investigadores, quienes desde la inteligencia de amenazas cibernéticas buscan mejorar y cerrar las brechas que usan los ciberdelincuentes.

Teniendo en cuenta el tipo de investigación a realizar, en la Tabla 2 se relacionan las variables objeto de estudio de carácter cuantitativo y en la Tabla 3 las de carácter cualitativo.

Tabla 2. Cuantitativo: Apropiación del conocimiento de CTI.

Concepto	Dimensiones	Variables	Indicadores
Apropiación del conocimiento de CTI: Medir el nivel de concientización, utilización y beneficios existente en las entidades	Aplicación en la entidad	Conocimiento de CTI	Porcentaje de apropiación de los conceptos de CTI
	Usabilidad de inteligencia de amenazas	Recursos asociados a inteligencia de amenazas	Cantidad de recursos dispuestos a CTI
	Beneficios de la utilización de estrategias de	Capacidad de anticipación y respuesta incidentes	Posibles amenazas que afecten a la seguridad de una organización y sus activos

	inteligencia de amenazas

Nota. Elaboración propia.

A continuación, se describen las variables propuestas, así:

7.1. Conocimiento de CTI

Con esta se busca medir el nivel de conocimiento de la inteligencia de amenazas cibernéticas en la población encuestada.

7.2. Recursos asociados a inteligencia de amenazas

Identifica los recursos humanos, técnicos y de servicios utilizados en la inteligencia de amenazas cibernéticas.

7.3. Capacidad de anticipación y respuesta incidentes

Nivel de ocurrencia de incidentes dentro las organizaciones que hacen parte de la población encuestada.

Tabla 3. Cualitativo: Impacto del CTI en la anticipación de eventos, incidentes o materialización de riesgos cibernéticos.

Concepto	Dimensiones	Variables	Indicadores
Impacto del CTI en la anticipación de eventos, incidentes o materialización de riesgos cibernéticos: Medir el nivel de efectividad que se podría alcanzar al aplicar CTI.	Conocimiento y aplicación de S.I. y su componente de inteligencia de amenazas	Sector/roles y aplicabilidad del CTI	% Conocimiento y beneficios del CTI
	Capacidades para aplicar en Colombia la CTI como insumo de la seguridad de la información	Implementación y uso de CTI	Probabilidad de aplicación en el Estado.
	Liderazgo de la estrategia de inteligencia de amenazas	Entidad líder de la estrategia	% de preferencia sobre el ente idóneo

Nota. Elaboración propia.

A continuación, se describen las variables propuestas, así:

7.4. Sector/roles y aplicabilidad del CTI

Identificar el punto de vista sobre la aplicabilidad de CTI, teniendo en cuenta el sector y la experticia del personal entrevistado.

7.5. Implementación y uso de CTI

Viabilidad en la implementación y aplicación de CTI en el entorno de las entidades gubernamentales a partir de los conceptos dados por los expertos entrevistados sobre la temática.

7.6. Entidad líder de la estrategia

Establecer la preferencia de la entidad sobre el liderazgo de la estrategia de inteligencia de amenazas.

8. Metodología

8.1. Enfoque y alcance de la investigación

8.2. Enfoque de la investigación

A partir del planteamiento del problema, se determina que la investigación a realizar es de carácter mixto y de tipo exploratoria descriptiva y cuantitativa. Por medio de esta se busca efectuar el reconocimiento del contexto y la apropiación de la temática de estudio de CTI. Lo anterior se establece para dar respuesta a la pregunta planteada y dar cumplimiento a los objetivos propuestos en el proyecto, de acuerdo con lo definido por (Hernández-Sampieri & Mendoza-Torres, 2018) al referirse al diseño metodológico como una estrategia concebida para obtener la información.

Se toma el camino del enfoque exploratorio porque permite analizar e investigar factores concretos de CTI, con lo cual, futuros investigadores pueden tener referentes para desarrollar nuevos análisis de la temática. Los resultados obtenidos permitirán definir futuras estrategias que deban ser aplicadas a partir de la incidencia de CTI en la reducción de los delitos informáticos en las entidades gubernamentales, e inclusive aplicable a estudios en otros sectores.

8.3. Tipo de la investigación

Al seleccionar este tipo de investigación exploratoria descriptiva y cuantitativa, se tiene la opción de poder usar el instrumento de entrevista a expertos en la temática con base en las variables planteadas. Así mismo, permite el análisis cuantitativo por medio de la realización de encuestas a una muestra de la población seleccionada para determinar si la hipótesis es aceptable o no. Adicionalmente, se recalca que, aplicado en Colombia, no existen investigaciones similares sobre CTI, salvo lo planteado por Almanza (2022) en la XXIII Encuesta Nacional de Seguridad Informática aplicada en Colombia, la cual determinó que CTI es un tema emergente con 33 % y que, al ser disgregado por

sectores, representa un 16,98 % de dicho valor a nivel gubernamental. Esto indica que no existen datos relevantes o que al ser un tema innovador aún no ha sido estudiado suficientemente en el país.

Con el fin de lograr los objetivos de la presente investigación, se requiere aplicar el tipo no experimental, que permita el análisis de información que conlleve a definir una posible estrategia para contrarrestar la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos en las entidades gubernamentales de Colombia mediante la aplicación de CTI. Este tipo de estudios no manipula las variables, puesto que los datos son tomados de entorno natural para su posterior análisis (Hernández y Mendoza, 2018).

8.4. Diseño de la investigación

Una vez seleccionado el tipo de investigación, se procede a plantear las etapas por medio de las cuales se busca dar respuesta al planteamiento del problema y cumplir con los objetivos propuestos, así:

Etapa I: Planteamiento de las preguntas de investigación.

Etapa II: Revisión del marco normativo de ciberseguridad en Colombia.

Etapa III: Selección de los instrumentos. A nivel cuantitativo encuestas y a nivel cualitativo entrevistas.

Etapa IV: Aplicación del instrumento y recolección de información.

Etapa V: Análisis de la información.

Etapa VI: Resultados obtenidos.

Etapa VII: Desarrollo de la propuesta.

Etapa VIII: Conclusiones.

Las etapas son acciones que permiten al investigador profundizar en el problema identificado con el fin de recolectar datos y posteriormente analizarlos. Para ello se hace necesario conocer el contexto de la problemática y no solo enfocarse en el objetivo, puesto que existen conceptos que deben ser tenidos en cuenta y cuya exclusión puede afectar los resultados de la investigación (Hernández y Mendoza, 2018).

8.5. Población

A nivel cuantitativo, la población está definida como las entidades públicas del orden nacional y territorial del Estado colombiano, que de acuerdo con la Constitución Política y la Ley 489 de 1998 se clasifican en las tres ramas del poder (Ejecutiva, Legislativa y Judicial) divididos en, organismos de control, entes autónomos y organización electoral. De acuerdo con las cifras del 14/11/23 publicadas en el portal de la Función Pública, existen 6341 entidades públicas (Función Pública, 2023). Sin embargo, con base en la temática de estudio, se toman las 297 de carácter nacional, teniendo como premisa la infraestructura tecnológica con la que pueden contar, ya que existen entidades territoriales que pueden no contar con este recurso o dependen directamente de una entidad nacional. Por tal razón y con base al problema en estudio, se busca que la investigación tenga resultados concluyentes a partir de la población en estudio y que está relacionada con tecnologías de la información.

Es importante resaltar que al ser una investigación de tipo exploratoria descriptiva y cuantitativa, también es viable el método entrevista, para lo cual se puede aplicar a 5 o más expertos en temáticas de ciberseguridad, quienes pueden tener un amplio contexto de la aplicación de CTI para contrarrestar los delitos informáticos en el sector gobierno a través de una estrategia.

8.6. Muestra

A nivel cuantitativo, la muestra estará conformada por personal de TI o quien haga sus veces en las entidades gubernamentales del orden nacional, por lo cual se hace uso de la formula estadística, así:

$$n = \frac{N.Z^2.p.q}{e^2.(N-1) + Z^2.p.q}$$

Donde,

Z= Nivel de confianza 90% y cuya constante es 1,645

p= Proporción de la población que tiene el atributo deseado 50%

q= Proporción de la población que no tiene el atributo deseado 50%

e= Estimación del error máximo aceptado 10%

N= Tamaño de la población 297

n= Tamaño de la muestra

Al aplicar la fórmula de muestras finitas se obtiene como tamaño de muestra mínima un resultado de 56 encuestas, teniendo en cuenta que la cifra se redondea puesto que se trata de personas. Para el despliegue y aplicación de este instrumento, se contó con el apoyo el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT).

En el caso de las entrevistas, se toma como referentes aquellos funcionarios de alto nivel que se desempeñan en cargos relacionados con la generación de estrategias enfocadas a la salvaguarda del ciberespacio en entidades del contexto colombiano, dentro de las que se destacan el COLCERT, el CSIRT PONAL, el DAPRE, el CCOCI, el CSIRT financiero, el grupo ciberinteligencia de la Policía Nacional y algunos referentes académicos en temas de TI del sector público-privado.

8.7. Diseño del instrumento

Con base en el planteamiento del problema y para lograr el cumplimiento de los objetivos, se debe llevar a cabo la recolección de información, procediendo a realizar el diseño de un instrumento de medición para cumplir dicho propósito. Esto permitirá el suministro de datos asociados a las variables propuestas en la investigación, por lo que el instrumento debe cumplir con tres requisitos esenciales: “confiabilidad, validez y objetividad*”, según* Hernández-Sampieri y Mendoza-Torres (2018, p. 501).

Uno de los instrumentos que más se utiliza en la investigación cuantitativa son los cuestionarios. Este suele constar de una serie de preguntas que buscan recolectar datos sobre una o más variables, relacionadas con el planteamiento del problema. A su vez, permiten la creación de preguntas variadas de selección múltiple, abiertas, cerradas, entre otras, que conllevan a una tabulación y análisis practico de la información (Hernández-Sampieri & Mendoza-Torres, 2018).

Otro instrumento que es usado es la entrevista, que desarrolla o considera otras variables para reunir la base de expertos en la temática de estudio o que pueden aportar gran valor a las variables planteadas, desde los cargos de alto nivel en los que se funda o se argumenta la toma de decisiones estratégicas y que para el problema de investigación pueden ser determinantes en el cumplimento de los objetivos (Hernández-Sampieri & Mendoza-Torres, 2018).

Con base en lo anterior, se diseña el modelo del instrumento tipo encuesta que se aplicaría para el análisis de las variables, como se observa en el Anexo. Encuesta No.1. Así mismo, se definen las preguntas a realizar por medio de entrevista a personas en cargo relevantes en la toma de decisiones sobre estrategias de ciberseguridad, con el fin de evaluar la aplicación de CTI como una estrategia para anticipar los eventos, incidentes o materialización de riesgos cibernéticos en las entidades gubernamentales, como se observa en el Anexo Entrevista No.1.

8.8. Técnicas para el análisis de la información

Una vez obtenidos los datos por medio del instrumento tipo encuesta (datos cuantitativos) y entrevista (datos cualitativos). Se procedió a organizar los datos cuantitativos mediante una matriz de Excel con el objetivo de graficar los resultados. Teniendo en cuenta las capacidades de la herramienta para el procesamiento de datos y dado el volumen de información obtenida mediante el instrumento, se hace uso de tablas dinámicas que permiten evidenciar los resultados obtenidos.

A partir de lo anterior, se parametrizaron los datos para ser asociados a las variables cuantitativas propuestas y analizar cada uno de los resultados, dando una lectura a los mismos, permitiendo el desarrollo de los objetivos propuestos con base al nivel de apropiación de CTI en las entidades gubernamentales del orden nacional, conllevando a la definición del modelo de estrategia de CTI.

En cuanto a los datos cualitativos obtenidos mediante la entrevista, se realizó la obtención de información que pudiese ser transformada en conocimiento a partir de la muestra recolectada, sin tener en cuenta solo las cifras del ámbito cuantitativo. Para ello se tomó la idea central de cada aporte de los participantes a las preguntas realizadas, orientando de esta forma el modelo de la estrategia desde la interpretación de los datos.

Como último paso, se verificó cada una de las respuestas tanto cuantitativas como cualitativas para definir el modelo de estrategia de CTI en entidades gubernamentales de Colombia como mecanismo de anticipación de delitos informáticos.

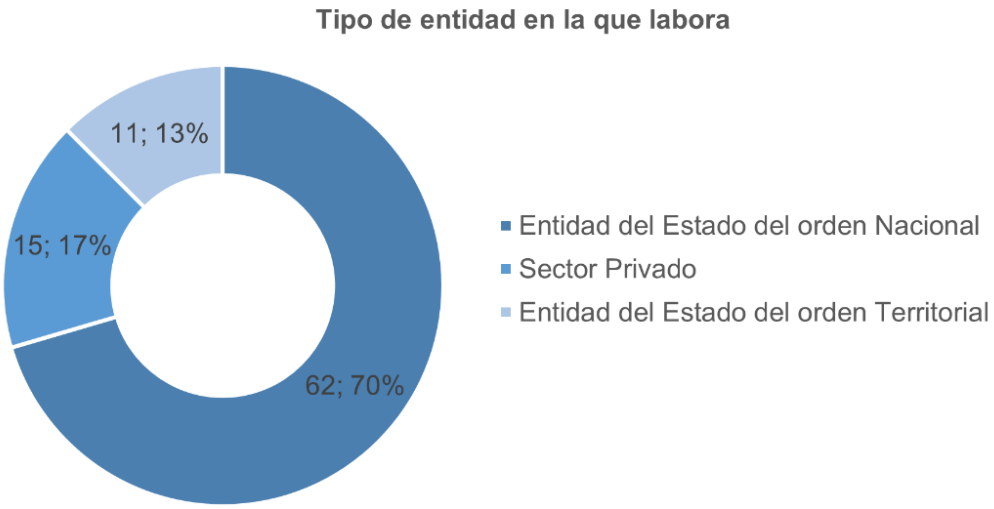
9. Trabajo de Campo

Para cumplir los objetivos propuestos, se empleó en primer lugar un instrumento de recolección de datos tipo encuesta a entidades del Estado del orden nacional, las cuales fueron diligenciadas por sesenta y dos (62) de estas entidades, lo que representa un 20,8 % del tamaño de la población objetivo en Colombia (297).

Sumado a lo anterior, a través de la encuesta se buscó tener información de referencia de otras entidades de orden nacional, sin embargo, no hubo gran participación de estos, ya que, de las ochenta y ocho (88) respuestas, el 13 % fueron entidades del Estado del orden Territorial y el 17% del sector privado, por lo que dichos datos no se consideran en el análisis de la información.

En cuanto al 70% restante de las respuestas (62), corresponde a la población objeto de estudio (Entidad del estado del orden nacional), por lo que, se procesaron los datos obtenidos, para el desarrollo de los objetivos (Ver Figura 15).

Figura 15. Resultado 1 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

En segundo lugar, se utilizó el instrumento tipo entrevista para recolectar información, en la que participaron diez (10) expertos en el entorno de ciberseguridad y

seguridad de la información. De los participantes, el 50% pertenece a entidades del Estado del orden del Nacional como son, Presidencia de la República, Policía Nacional de Colombia, Comando Conjunto Cibernético y Ministerio TIC. El 50% restante de participantes son del sector privado y corresponden al Centro de Investigación de Cibercrimen y Ciberseguridad (Center for CIC), la Universidad de los Andes, el CSIRT financiero, la Universidad EAN y CISOS.CLUB.

Considerando las respuestas obtenidas con la entrevista, se procesan los datos y se toman algunos de los aportes que contribuyeron al desarrollo de los objetivos, siendo referenciado el autor de cada uno (Ver Figura 16).

Figura 16. *Resultado 1 encuesta nivel de apropiación del CTI - expertos.*

Nota. Elaboración propia.

Para el análisis de los resultados de las preguntas cuyas opciones eran Totalmente de acuerdo, De acuerdo, Ni de acuerdo ni en desacuerdo, En desacuerdo y Totalmente en desacuerdo, se procedió a realizar la siguiente agrupación, con el propósito de definir el aspecto positivo, neutro y negativo de los resultados, así:

- Aspecto positivo: Totalmente de acuerdo y De acuerdo.
- Aspecto neutro: Ni de acuerdo, ni en desacuerdo.
- Aspecto negativo: En desacuerdo y Totalmente en desacuerdo.

9.1. Revisión frente a la normatividad, medidas y controles existentes en Colombia sobre la prevención en la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos, enfocado en la inteligencia de amenazas (CTI).

Para dar cumplimiento a este objetivo, se realizó la revisión documental de la normatividad asociada a gobierno digital, en la cual se establecen las directrices para las entidades gubernamentales en cuanto a la protección de la confidencialidad, disponibilidad e integridad de la información, teniendo en cuenta la temática de estudio en el ámbito de la inteligencia de amenazas y las bases que podrían soportar el desarrollo de una estrategia asociada a la misma. En virtud de lo anterior se referencian las políticas, iniciativas de proyecto, leyes, lineamientos, entre otros, permitiendo generar el siguiente contexto.

La protección del ciberespacio es una temática en tendencia y que a nivel mundial está siendo tomada como referente para generar un mundo digital más seguro. Así mismo, se trata de un tópico de interés gubernamental como se demuestra en las bases iniciales del Plan Nacional de Desarrollo 2023-2026, donde se mencionó la creación de una Dirección Nacional de Seguridad Digital con el objetivo de lograr un “ecosistema digital confiable” para garantizar la protección del Estado (Planeación, 2023).

Si bien es cierto que en los debates del PND esta iniciativa no fue aprobada (García R., 2023), existen otros mecanismos mediante los cuales el gobierno puede abordar la temática con el objetivo de garantizar la ciberseguridad del país. Ante esto, la generación de estrategias enfocadas con dicho propósito, pueden ser adoptadas por el

gobierno y delegadas a entidades con responsabilidades para la protección del ciberespacio como el ColCERT y/o CsirtGob. Además, al ser un tema emergente en el mundo y a nivel nacional, conlleva a la proliferación de conocimiento y colaboradores para tal fin, cuyo origen puede ser de entidades tanto públicas como privadas y a su vez de diversos sectores económicos.

Con base a lo anterior, fue propuesto en cámara el proyecto de ley 023/2023C, por medio del cual se busca la creación de la agencia nacional de seguridad digital y asuntos espaciales, junto con algunas competencias especificas (Cámara de Representantes, 2023); como también en el proyecto de ley 331/23 propuesto en el senado, mediante el cual se buscaba la creación de la agencia nacional de seguridad digital entre otras disposiciones (Senado de la República, 2023).

Sin embargo, para abordar el tema de CTI en Colombia, en primer lugar, se debe tomar como referencia la ley 1273 del 5 de enero de 2009, mediante la cual se estableció un nuevo bien jurídico tutelado teniendo en cuenta la protección de la información y de los datos, preservando la integridad de los sistemas que hacen uso de las tecnologías de la información y las comunicaciones (Ley 1273, 2009).

En el capítulo uno de la ley en mención se hace énfasis en los atentados contra la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos. En el capítulo segundo se enfoca en los atentados informáticos y otras infracciones.

En esta ley se tipifican una serie de conductas punibles enmarcadas en el ámbito de los delitos informáticos bajo los siguientes contextos:

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño Informático.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269I: Hurto por medios informáticos y semejantes.
- Artículo 269J: Transferencia no consentida de activos.

En vista de lo anterior, este marco normativo describe las acciones que entidades públicas y privadas desean prevenir, ya que en la era tecnológica la información es el activo más valioso para cualquier organización. Esto según diferentes estándares internacionales como lo son: la familia de la norma ISO 27000 - Gestión de seguridad de la información; el Instituto Nacional de Estándares y Tecnologías (NIST); el modelo Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas (COBIT); entre otros.

En agosto del 2011, el grupo hacktivista “Anonymous” llevó a cabo una serie de ataques cibernéticos en Colombia a diferentes infraestructuras gubernamentales. Un mes antes se plantaron las bases de la ciberseguridad en el país a través del CONPES 3701 del 2011. Según lo manifestado por (Díaz Acevedo & Cremades Guisado, 2023), este documento mediante el cual se definieron los “Lineamientos de Política para Ciberseguridad y Ciberdefensa” contenía un plan de acción para desplegar actividades en tres componentes esenciales: la institucionalidad, capacitación e investigación y el ámbito legislativo. También designó tareas y responsables de las mismas, lo que dio como resultado la creación del ColCERT, y el despliegue de actividades para Centro Cibernético Policial y el Comando Conjunto Cibernético, encargados de velar por la seguridad digital de los ciudadanos y del país. Finalmente, dejó abierto el escenario para desarrollar y complementar las capacidades para la protección del ciberespacio.

Posteriormente se dio paso al CONPES 3854 del 2016, mediante el cual se estableció la “Política Nacional de Seguridad Digital” enfocado en la gestión de riesgos digitales, teniendo en cuenta los conceptos básicos sobre riesgos, emitidos por la Organización para la Cooperación y el Desarrollo Económico (OCDE) en las recomendaciones sobre gestión de riesgos de seguridad digital (OCDE, 2015). En este documento se define el riesgo como un estado de incertidumbre que puede generar una serie de consecuencias adversas de carácter económico. Esto desde el aspecto de seguridad digital se asocia al estado de incertidumbre de las actividades que se desarrollan en el contexto digital y la gestión de riesgos se enfoca en identificar amenazas y tomar medidas para reducir la probabilidad de ocurrencia. Lo anterior conllevo al fortalecimiento de las capacidades en la identificación, gestión y mitigación de riesgos en el ámbito cibernético, para lo cual, se buscó involucrar múltiples partes interesadas del entorno digital con el ámbito de fortalecer las capacidades de cooperación, colaboración y asistencia tanto a nivel nacional como internacional (Departamento Nacional de Planeación, CONPES 3854, 2016).

Dentro de la línea del (Departamento Nacional de Planeación, CONPES 3995, 2020), se emite la “Política Nacional de Confianza y Seguridad Digital” cuyos objetivos se encuentran orientados a generar confianza en el entorno digital, por medio del fortalecimiento de capacidades de seguridad digital de los ciudadanos, el sector público y el privado, la actualización del marco de gobernanza existente y la búsqueda de nuevas tecnologías para afrontar los retos de la cuarta revolución industrial.

Los planteamientos y acciones establecidas en el país de los documentos de política de estado CONPES hasta ahora, asociados a ciberseguridad han tenido una visión y enfoque reactivo, dicho esto la palabra anticipación solo aparece tres veces en

las 185 páginas de lo que serían las bases para implementar estrategias de fortalecimiento de capacidades en seguridad digital en el país. Esto deja claro la no existencia de una estrategia anticipativa que saque provecho del concepto CTI, lo que conlleva a que las instituciones gubernamentales estén expuestas a ser vulneradas por actores maliciosos, donde sus motivaciones e intenciones buscan deliberadamente causar daño a los componentes tecnológicos, mediante los cuales brindan servicio a la ciudadanía en general.

En el 2022 se emitió la “Política de Gobierno Digital” mediante el decreto 767 de (Función pública, 2022), mediante la cual se buscaba impactar a los ciudadanos, aprovechando las Tecnologías de la Información y las Comunicaciones para mejorar la calidad de vida, haciendo uso de la transformación digital del Estado para garantizar los derechos en el ciberespacio. Para conseguir este objetivo, se planteó la colaboración y coordinación de las diferentes entidades del estado, con el fin de dar una correcta aplicación y mejorar la competitividad del país a nivel digital.

Al llevar a cabo la revisión de la normatividad aplicable a la Política de Gobierno Digital actual, se encuentran algunos datos de interés como lo son: la (Directiva Presidencial 02, 2022) del 24 de febrero de 2022, en la que se reitera la política pública en materia de seguridad digital; el Decreto 338 del 08 de marzo de 2022 (Departamento Administrativo de Presidencia, 2022), en el que se establecen los lineamientos generales para fortalecer la gobernanza digital, creando el modelo y las instancias para tal fin; la Resolución 00500 del 10 de marzo de 2021 (MINTIC, 2021) y la resolución 000746 del 11 de marzo de 2022 (MinTIC, Resolución N° 000746, 2022), mediante las cuales se adoptó y fortaleció el Modelo de Seguridad y Privacidad de la Información (MSPI). En esta normatividad se dan instrucciones sobre las actividades que deben realizar las entidades de la administración pública, con el propósito de reducir el riesgo de afectación de incidentes de seguridad, soportándose en el MSPI y la gobernanza digital.

Con relación al MSPI, en el 2022 se llevó a cabo una medición del desempeño institucional de las entidades a nivel nacional y territorial (MIPG - Función Pública;, 2022) a través de la evaluación del Modelo Integrado de Planeación y Gestión (MIPG), en el que se estableció la medición de los índices de política de gestión y desempeño en seguridad digital (POL08). En esta evaluación nacional el puntaje fue de 75,5, mientras que a nivel territorial fue de 46,7, en la que las variables a evaluar fueron: asignación de recursos, implementación de lineamientos de política y despliegue de controles.

De igual forma, MINTIC a través del portal de Gobierno Digital permite la consulta de datos asociados a la Política de Gobierno Digital (Gobierno Digital, 2023), para lo cual, en el micrositio de mediciones se tiene una métrica denominada “Índice de Gobierno Digital”, para medir el nivel de desempeño de las entidades públicas en cuanto a gobierno digital, haciendo uso del Formulario Único de Reporte de avances en la Gestión (FURAG) para la recolección de los datos. Dentro de las variables evaluadas, se tiene el habilitador de “Seguridad y Privacidad de la Información”, el cual a nivel nacional obtuvo un puntaje promedio de 68 puntos y a nivel territorial un puntaje promedio de 37,1.

Sumado a lo anterior, el instrumento del MISP tiene como objetivo principal orientar a las instituciones públicas del orden nacional y territorial, en cuanto a seguridad de la información, creando confianza en las partes interesadas y asegurando los activos de información (MinTic, 2021). Para ello, toma como referente la ISO 27001:2013 llevando a cabo la identificación de activos, los controles existentes y el tratamiento de riesgos a partir del anexo A, el cual sirve de guía para la implementación de un Sistema de Gestión de seguridad de la información (SGSI) en las entidades colombianas.

A partir de lo anterior, la ISO 27001 se actualizó en octubre de 2022, pasando de 14 categorías de controles a 4, disminuyendo la cantidad de controles de 114 a 93, de los

que 35 mantuvieron el nombre, 23 se renombraron, 57 se fusionaron por 24, 1 se dividió en 2 y 11 se crearon nuevos. Estos últimos fueron agregados para ajustarse a las necesidades del mundo actual (Ta-Seen, 2023). En los nuevos controles destaca la inteligencia de amenazas, consistente en el desarrollo de actividades que debe realizar una organización para recolectar y analizar información que permita anticipar ataques a sus infraestructuras tecnológicas.

La actualización de versión de la ISO 27001 implica necesariamente una actualización del MSPI, lo que conlleva a identificar que el CTI debe ser tenido en cuenta como un control a implementar dentro de las entidades. Ya sea que quieran incorporar la seguridad de la información o llevar a cabo el proceso de transición a la nueva versión. Puesto que actualmente y con base a los documentos revisados en el sitio web de (Gobierno Digital, 2023), se logra evidenciar que a nivel gubernamental no existen referentes enfocados en la inteligencia de amenazas cibernéticas como estrategia de prevención y anticipación de eventos, incidentes o materialización de riesgos cibernéticos, al no ser mencionada en ninguno de ellos.

Con relación a los puntos de vista de las personas entrevistadas sobre las políticas gubernamentales para salvaguardar la confidencialidad, integridad y disponibilidad de la información en las entidades del sector gobierno, se tiene lo siguiente:

“Las políticas de las entidades no tienen el alcance, la fuerza y la implementación necesaria. Se han desviado de su objetivo primario (…) La falta de gobernanza y de políticas no vinculantes no permiten que las entidades se integren al ecosistema y mejoren su postura de seguridad.” (Entrevista a Julio Mancipe, asesor de seguridad digital y ciberseguridad de la Presidencia de la República de Colombia, 08/11/23).

“Falta mucho aún para considerar que son suficientes, partiendo del hecho de que nunca serán suficientes debido al gran dinamismo de los riesgos y sus vulnerabilidades y amenazas asociadas. Los hechos pasados y actuales de incidentes informáticos nos han demostrado que nos falta mucho por recorrer en este tema (...) De hecho muchos casos han seguido siendo recurrentes.” (Entrevista a Yesid Donoso, exdirector del departamento de ingeniería de sistemas y computación de la Universidad de los Andes, 09/11/23).

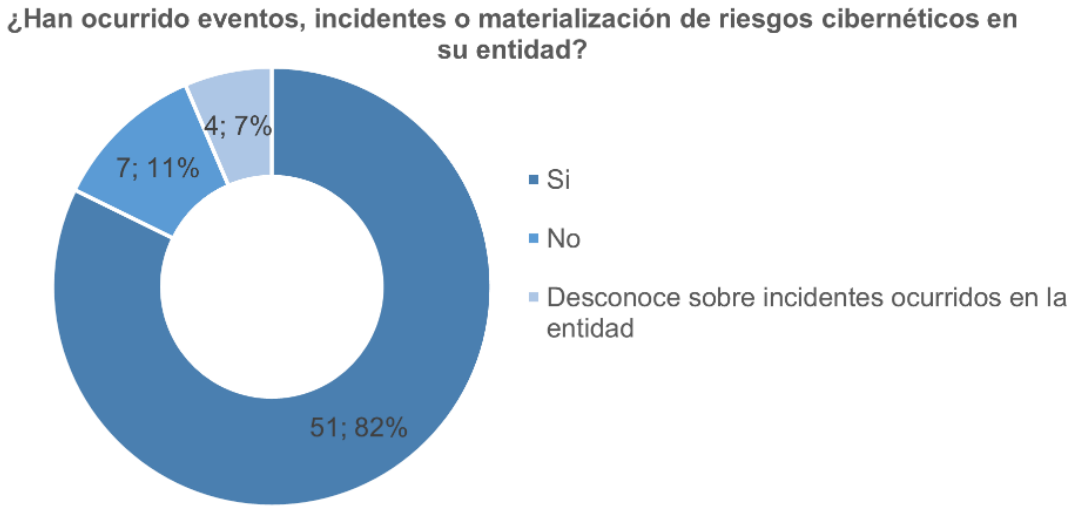
“Las políticas gubernamentales no son suficientes, ya que se deben adoptar medidas más concretas, como la concientización real sobre los usuarios, lo que sin duda va a permitir conocer los riesgos y peligros que trae consigo la evolución constante de las ciberamenazas. Por eso es fundamental que las autoridades gubernamentales se mantengan actualizadas sobre las amenazas emergentes y asignen recursos adecuados para implementar y hacer cumplir políticas de seguridad cibernética más efectivas (...) Los incidentes cibernéticos pueden servir como lecciones aprendidas para mejorar la postura de seguridad de una entidad y pueden llevar a la implementación de medidas más robustas para prevenir futuros eventos similares.” (Entrevista a Carlos Beltrán, director de operaciones del CSIRT Financiero, 14/11/23).

“Se mantiene un sesgo frente al conocimiento general de las políticas y no son de impacto real en la actualidad en los diferentes sectores, no se tiene una hoja de ruta clara sobre los elementos claves en materia de obligaciones y ventajas en materia de seguimiento a ciberataques o tratamiento de una política de Cibercrimen (...) Es importante que las entidades posean una herramienta o instrumento vital para gestionar y activar defensas ante posibles ciberataques.” (Entrevista a Emanuel Ortíz, Presidente RedCiber, 16/11/23).

9.2. Afectación causada por la materialización de riesgos cibernéticos en las entidades gubernamentales de Colombia.

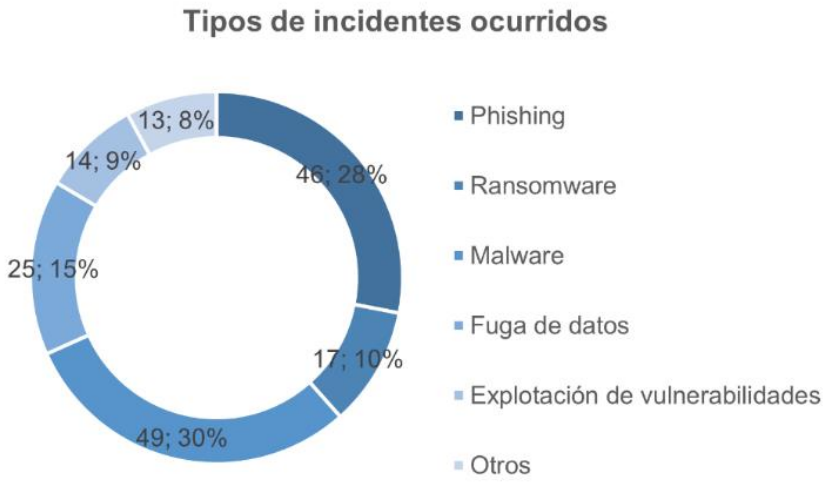
Teniendo en cuenta los datos recolectados, se logra evidenciar que, un 82% de las entidades gubernamentales de orden Nacional han sido víctimas de riesgos cibernéticos, entre los que resalta el malware con un 30% y el phishing con un 28%, tal y como se observa en la figura No 17 y 18.

Figura 17. Resultado 21 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

Figura 18. Tipo de incidentes ocurridos.



Nota. Elaboración propia.

Además, según cifras del C4, en 2022 aumentaron las denuncias de delitos informáticos respecto al 2021. Estas cifras concuerdan con las afectaciones presentadas a entidades públicas y privadas en los últimos años, lo que pareciera indicar que estos datos irán en aumento, tal y como lo pronostican múltiples reportes de la industria recopilados (Cisos, 2023). Sin embargo, en comparación con las cifras del periodo 2022-2023, se observa una reducción de denuncias, lo que podría suponer una efectividad en las estrategias de seguridad digital desarrolladas o algún factor diferencial respecto al periodo anterior. No obstante, ese análisis no hace parte de la investigación propuesta en el presente documento. (ver Figura 19).

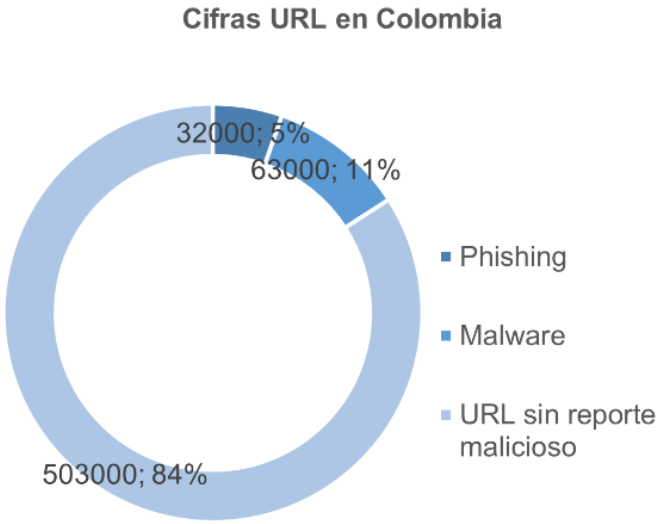
Figura 19. Comparativo conductas delictivas en el ciberespacio

COMPARATIVO DENUNCIAS 2021-2022			COMPARATIVO DENUNCIAS 2022-2023		
2021	2022	Diferencia en %	2022	2023	Diferencia en %
Hurto por medio informático y semejantes			Hurto por medio informático y semejantes		
19.354	26.366	+26%	26.366	28.477	8%
Violación de datos personales			Violación de datos personales		
12.635	13.081	+3,4%	13.081	9.632	-29%
Acceso abusivo a un sistema informático			Acceso abusivo a un sistema informático		
8.375	13.588	+38%	13.588	10.875	-17%
Suplantación sitio web			Suplantación sitio web		
5.453	5.751	+5%	5.751	4.390	-24%
Transparencia no consentida de activos			Transparencia no consentida de activos		
3.277	3.578	+8%	3.578	3.298	-8%
Interceptación de datos informáticos			Interceptación de datos informáticos		
1.357	1.989	+32%	1.989	1.308	-34%
Daño informático			Daño informático		
489	631	+23%	631	397	-37%
Uso d software malicioso			Uso d software malicioso		
359	418	+14%	418	297	-29%
Obstaculización ilegitima de sistema informático o red de telecomunicaciones			Obstaculización ilegitima de sistema informático o red de telecomunicaciones		
280	391	+28%	391	296	-25%

Nota. Adaptado del *(Centro Cibernético Policial, 2023)*

Por otra parte, con relación a las cifras obtenidas de Virustotal, durante el 2023 en Colombia se subieron a esta plataforma un aproximado de 598 mil URLS para ser analizadas. De estas, el 11% (63 mil) fueron reportadas como phishing y el 5% (32 mil) se encontraron asociadas a malware (Ver Figura 20).

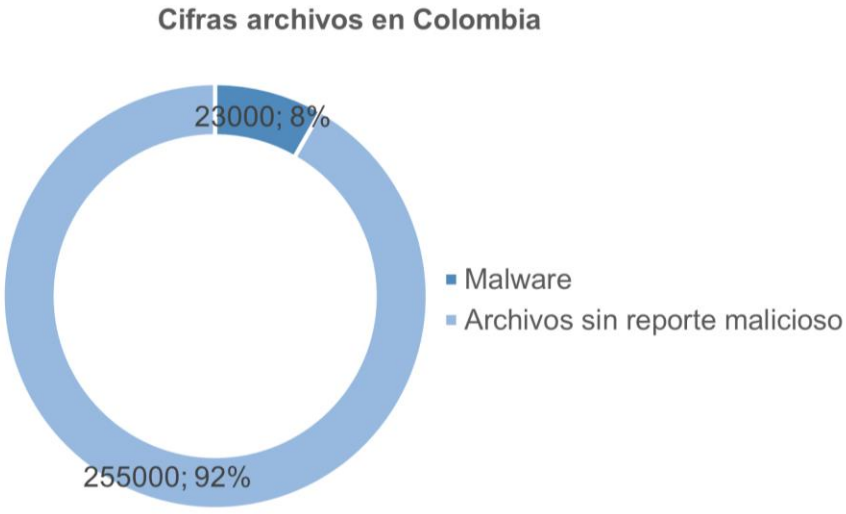
Figura 20. Cirfras URL en Colombia.



Nota. Adaptado de *(Virustotal, 2023)*

En cuanto a las cifras de archivos, en el 2023 se adjuntaron 278 mil muestras en Colombia, de las cuales el 8% (23 mil) fueron reportadas como malware (Ver Figura 21).

Figura 21. Cifras archivos en Colombia.



Nota. Adaptado de *(Virustotal, 2023)*

Lo anterior evidencia una gran diferencia entre las cifras de denuncias reportadas en el país durante el 2023 y la cantidad de vectores de amenazas que circularon según Virustotal.

Adicionalmente, para poder analizar las afectaciones de eventos, incidentes o materialización de riesgos cibernéticos en las entidades gubernamentales de Colombia, se realizaron consultas en fuentes abiertas, de lo cual se relacionan algunos de los hechos destacados con relación a ciberataques ocurridos durante el 2023 hasta la fecha, como parte de la investigación realizada, así:

- El 17/01/2023 el usuario *"PieWithNothing"* en el foro de *"BreachForums"*, puso a la venta 25 millones de registros por $900 dólares, destacando un aproximado de 8.5 millones abonados telefónicos y 1 millón correos electrónicos. Estos datos estarían asociados a usuarios del Sistema de Identificación de Potenciales Beneficiarios de Programas Sociales (SISBEN) y que posiblemente habrían sido obtenidos del sitio web sisben.gov.co (García, Camilo Andrés, 2023).
- El 02/02/23, la alcaldía de Medellín emitió un comunicado en el que manifestó, que el Sistema Integrado de Emergencias y Seguridad de Medellín (SIES-M) fue víctima de un ataque cibernético (Secretaría de Seguridad y Convivencia, 2023). Posteriormente se identificó que el ataque fue de tipo *ransomware* llevado a cabo por el actor malicioso "*Lockbit*", quien tiempo después publicó en la dark web un aproximado de 5.8 Gb de información. Estos datos serían de funcionarios de la Policía Nacional, atención de casos de homicidios, abonados telefónicos y correos de ciudadanos, entre otros (García, 2023).

- El 20/02/23 el grupo "*Colombian Cyber Army A.k.a ColHackers*" a través de su canal de Telegram manifestó haber explotado una vulnerabilidad de ejecución de código remoto y que, por medio de acceso a correo le fue posible ingresar a la red

de la Universidad Nacional (UNAL), publicando capturas de pantallas de los servicios de directorio activo, servicios VOIP, el circuito cerrado de televisión, entre otros. Posteriormente, el 18/03/23 la infraestructura tecnológica de la UNAL fue víctima de un ciberataque de tipo *ransomware* que conllevó a detener sus actividades durante un tiempo (Semana, 2023).

- El 07/03/23 el mismo actor que atacó a la UNAL, publicó nuevamente en telegram que obtuvo un acceso no autorizado a varios servicios de MINTIC y, además, habría obtenido un aproximado de 785 MB de información en la que podrían existir un aproximado de 13 mil registros (nombres, teléfonos, correos, entre otros) de personas asociadas a proyectos del Viceministerio de Transformación Digital (Mucho Hacker, 2023).
- El 23/05/23 la Sociedad Fiduciaria de Desarrollo Agropecuario S.A (Fiduagraria) fue víctima de un ciberataque que ocasionó fallas e intermitencias (Fiduagraria, 2023). Poco después en redes sociales comenzó a circular que el actor malicioso Lockbit se atribuía los hechos, confirmando que se habría tratado de un ataque tipo ransomware. Asimismo, otro actor malicioso conocido como medusa publicó en su canal de telegram los enlaces para realizar la descarga de un aproximado de 3.6 TB de información, correspondiente a posibles datos personales de clientes y empleados de la entidad, contratos y obligaciones financieras entre otras (García, Camilo Andrés, 2023).
- El 12/09/23 el proveedor de servicios IFX Networks fue víctima de un ciberataque de tipo ransomware que afectó considerablemente el componente de virtualización y con ello una gran cantidad de entornos de sus clientes de múltiples países, incluido Colombia (IFXNetworks, 2023). Aunque la empresa no

es de carácter gubernamental si presta servicios al Estado, al momento del ataque muchas entidades de este tipo se vieron afectadas en el país, destacando la Superintendencia de Salud, la Rama Judicial, la Superintendencia de Industria y Comercio, el Ministerio de Salud y Protección Social, entre otros (Portafolio, 2023). De acuerdo con la nota de rescate, el actor malicioso *RansomHouse* habría realizado el ataque, pero a la fecha del presente documento, el grupo no ha publicado información al respecto en su canal de Telegram.

Complementando lo anterior, en el 2022 el INVIMA, la fiscalía general de la Nación, las Empresas Públicas de Medellín (EPM), Keralty, junto a otras entidades de carácter privado, fueron víctimas de ciberataques (Nsit, 2022). De igual forma, 20 actores maliciosos realizaron acciones contra la infraestructura tecnológica de múltiples organizaciones del país, siendo un aproximado de 34 víctimas (Lumu Technologies, 2022).

Como se puede observar en la recopilación de información realizada, existe una afectación evidente a la confidencialidad, integridad y disponibilidad de la información, en la que tanto las entidades gubernamentales como sus clientes se han convertido en víctimas de los ciberdelincuentes. A partir de lo anterior, el funcionamiento de los servicios que usan los ciudadanos se ha visto impactado considerablemente, tanto así que en algunos casos se han paralizado las operaciones de estas entidades.

En el caso del ciberataque al INVIMA, conllevó al retraso de las importaciones y exportaciones de algunos productos, afectando las actividades de comercio en el país (Mouthón, 2022). Algo similar ocurrió con el ciberataque a EPM, que afectó a los ciudadanos que hacían uso de los servicios públicos prepagados de dicha entidad, debido a que la plataforma de recargas fue afectada y con ello el derecho al acceso a este tipo de servicios (El Colombiano, 2022). En los hechos ocurridos con Keralty por el

ciberataque, los servicios digitales de algunas entidades promotoras de salud (EPS) quedaron fuera de línea, afectando a cientos de usuarios en su derecho a la salud (Betancourt, 2022).

Como se puede observar, un delito informático realizado sobre las entidades gubernamentales o privadas afecta derechos fundamentales de los ciudadanos, inclusive la violación de datos personales conlleva a que los ciberdelincuentes amplíen su rango de acción, puesto que información como correos electrónicos, números de teléfono, números de cedula, entre otros, pueden servir como vectores de ataque para desplegar nuevos ciberataques, tanto a nivel gubernamental, empresarial o personal, dependiendo de la motivación del atacante, que puede ir desde obtener beneficios económicos hasta afectar la normal operación de un país, como fue el caso de estonia en el 2007 (Cardash, Cilluffo, & Ottis, 2013) y Ucrania en el 2017 (Nava Chan, 2022).

A partir de la recolección realizada a través de la entrevista se obtuvieron los siguientes puntos de vista:

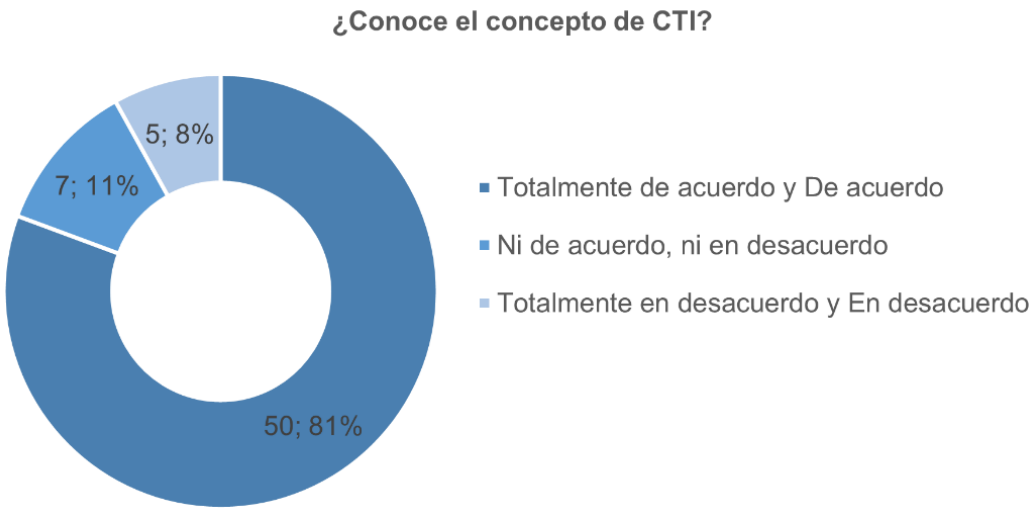
“Teniendo en cuenta los últimos incidentes de seguridad digital presentados en varias entidades de gobierno de algunos sectores económicos de país y frente a las acciones de gestión realizadas de manera puntual, se observa que las recomendaciones y acciones de prevención no se despliegan a las entidades, así mismo al interior de las entidades los ajustes a las posturas de seguridad, no se realizan cada vez que sucede un incidente a nivel nacional.” (Entrevista a Nelson Barrios, Líder de Operaciones ColCERT, 04/12/23).

9.3. Propuesta de una estrategia orientada a la anticipación y prevención por medio de la inteligencia de amenazas cibernéticas que complemente las capacidades existentes de seguridad informática y ciberseguridad en las entidades gubernamentales de Colombia.

Para el desarrollo del último objetivo que confluye en el cumplimiento del objetivo general, se realizó el análisis de los resultados restantes de la encuesta teniendo en cuenta la agrupación descrita anteriormente, ya que a partir de estos se determina la orientación de la estrategia a plantear, puesto que se requiere conocer el contexto actual de CTI para definirla.

A partir de lo anterior, el nivel de conocimiento del concepto de CTI es relevante para el planteamiento de acciones. En este sentido, se entiende el concepto de CTI, ya que se tiene un aspecto positivo del 81% por parte de la población encuestada. Esto implica un alto nivel de apropiación de los conceptos asociados a CTI, con lo que una estrategia con terminología de CTI es fácilmente comprensible.

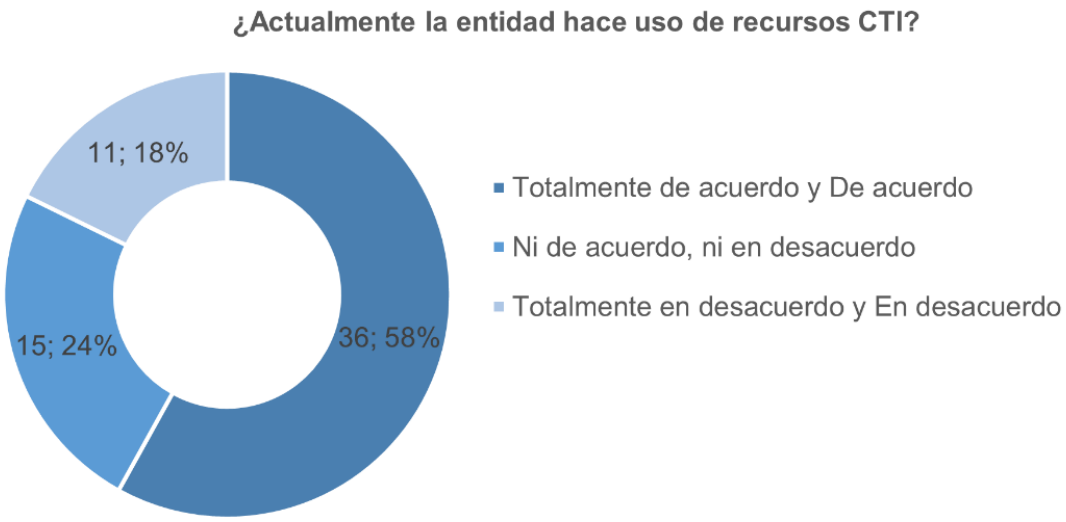
Figura 22. Resultado 2 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

En referencia al uso de recursos de CTI, se tiene un aspecto positivo del 58% con base a las respuestas de la población encuestada. Esto indica que un gran número de entidades tiene implementado el uso de recursos de CTI.

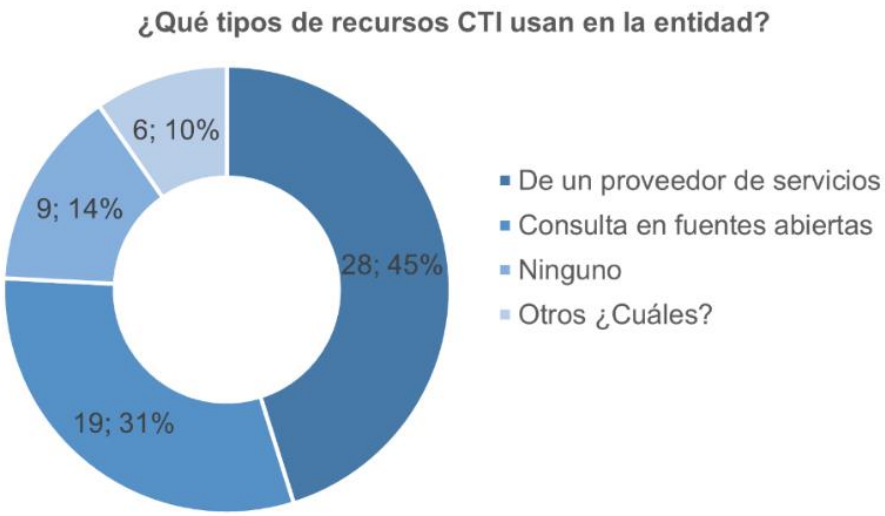
Figura 23. Resultado 3 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

El 45% de la población encuestada manifestó depender de un proveedor de servicios para hacer uso de los recursos de CTI. Esto representa la dependencia de terceros en este aspecto, ante lo cual, las entidades están sujetas a la información suministrada por estos. Un 31% realiza consulta en fuentes abiertas. En cuanto a otros recursos usados solo el 10% lo hace, dentro de los que destacan boletines y reportes de diversas empresas de TI, aunque también mencionan servicios de SOC, gestión de contratistas, operadores de TI, los cuales entran en la categoría de proveedor de servicio. Esto representa un aumento en cuanto al uso de proveedores de servicio en la gestión de CTI.

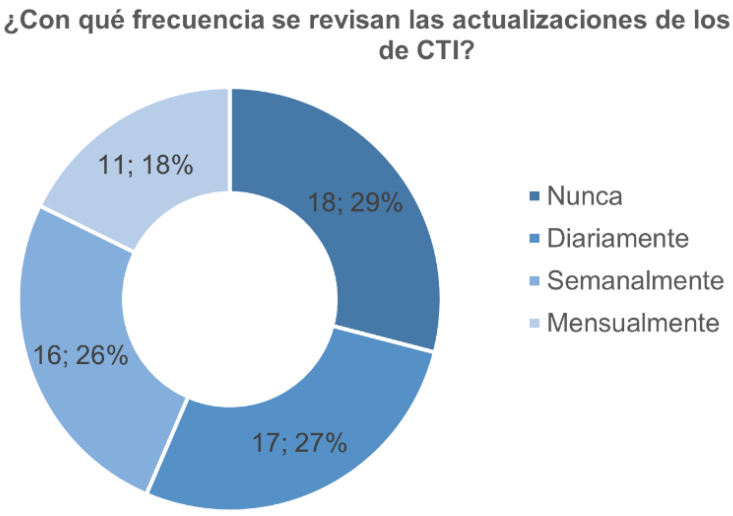
Figura 24. Resultado 4 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

En lo relacionado a la frecuencia de revisión de las actualizaciones de los recursos de CTI, el 27% de la población encuestada lo realiza diariamente, el 26% de forma semanal y el 18% mensualmente. El 29% restante manifestó no revisar nunca, lo que indica la relación con la pregunta anterior en cuanto al uso de un proveedor de servicios para el uso de CTI y con ello la delegación de responsabilidad en este aspecto.

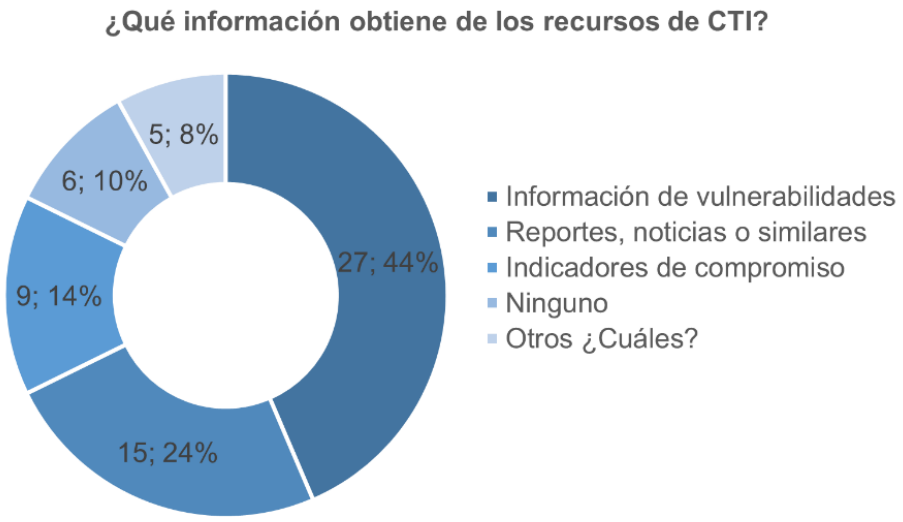
Figura 25. Resultado 6 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

CTI ofrece diferentes tipos de información, de lo cual, 44% de la población encuestada manifestó interés sobre información de vulnerabilidades; el 24 % se enfoca en reportes y noticias asociados; el 14% se asocia con los indicadores de compromiso. Estos tres aspectos son fundamentales en las organizaciones para contrarrestar diversas ciberamenazas.

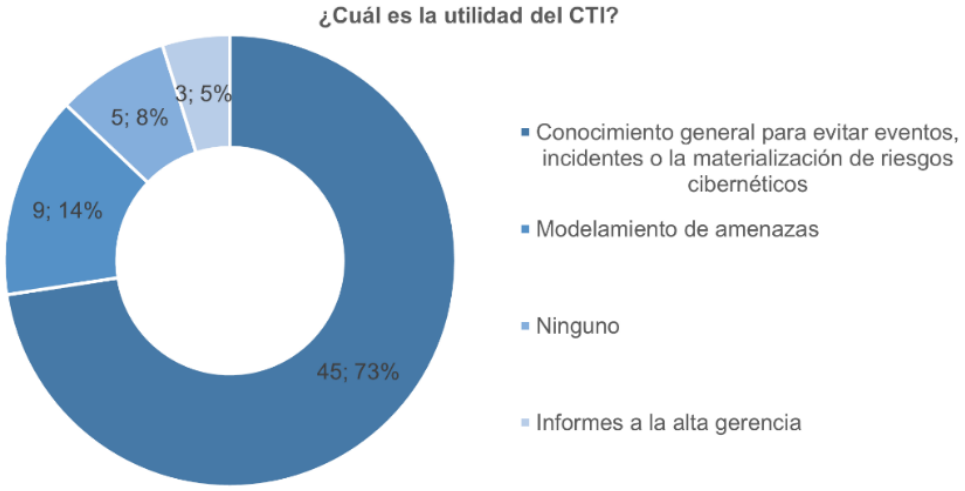
Figura 26. Resultado 7 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

En cuanto a la utilidad del CTI en la población en encuestada, el 73% manifestó interesarse por el conocimiento general para evitar eventos, incidentes o la materialización de riesgos cibernéticos. Esto indica que las entidades se preocupan por la protección de sus entornos digitales, por lo cual recurren a CTI.

Figura 27. Resultado 9 encuesta nivel de apropiación del CTI.

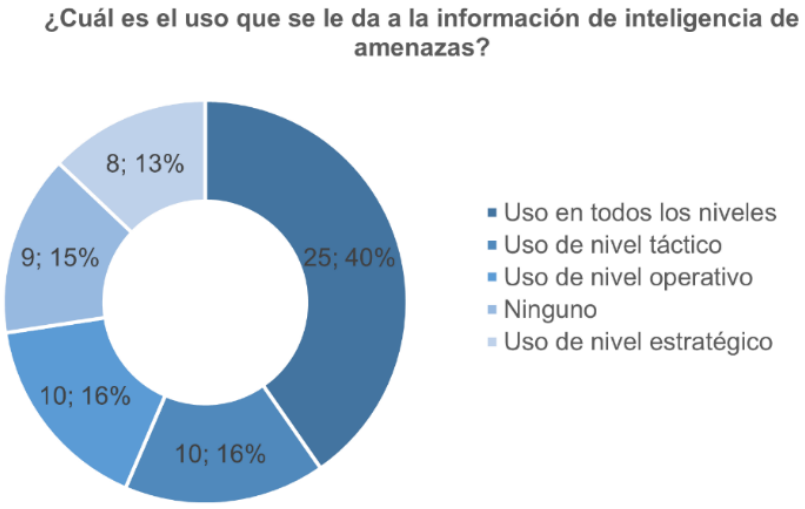


Nota. Elaboración propia.

Según la encuesta, la información que se obtiene de CTI se usa en un 40% en los niveles estratégico, operativo y táctico transversalmente; mientras que de forma individual su uso es de un 16% y un 13% exclusivamente a nivel estratégico. Cada entidad tiene procesos y procedimientos diferentes basados en el objetivo del negocio, por lo que, el interés por un nivel en específico esta dado por las necesidades propias de las organizaciones.

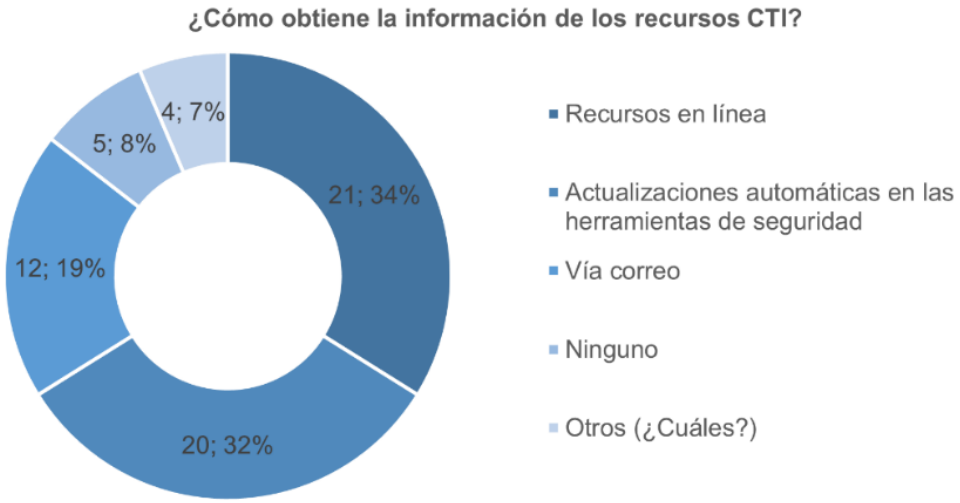
Sumado a lo anterior, es importante anotar que en la pregunta relacionada con la forma de obtención de los datos de CTI, las respuestas se inclinan en mayor medida a recursos en línea un 34%, seguido por un 32 % por actualizaciones automáticas y al final un 19% por medio de correo electrónico. El restante 15 % no utiliza o no define los métodos por los que obtiene esta información.

Figura 28. Resultado 10 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

Figura 29. Resultado 11 encuesta nivel de apropiación del CTI.



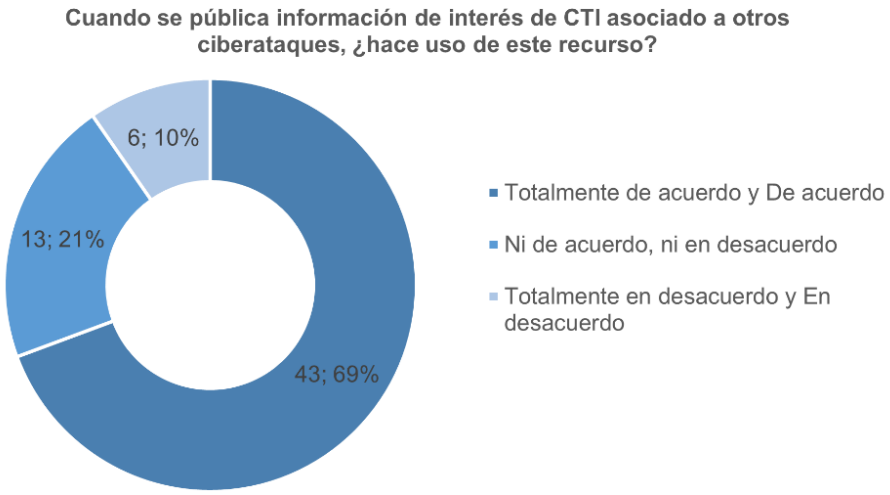
Nota. Elaboración propia.

Otro aspecto de interés es que, para las organizaciones es relevante la información de CTI por su relación con ciberataques materializados, ya que se tiene un

69% de aspecto positivo en el que la población encuestada manifestó hacer uso de dichos insumos.

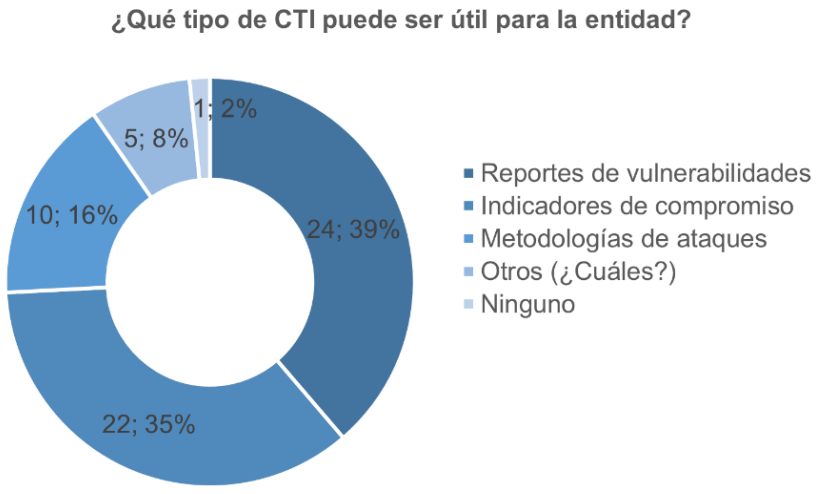
Dentro del tipo de datos de interés de la población encuestada, están los reportes de vulnerabilidades con un 39 % y los indicadores de compromiso con un 35 %.

Figura 30. Resultado 13 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

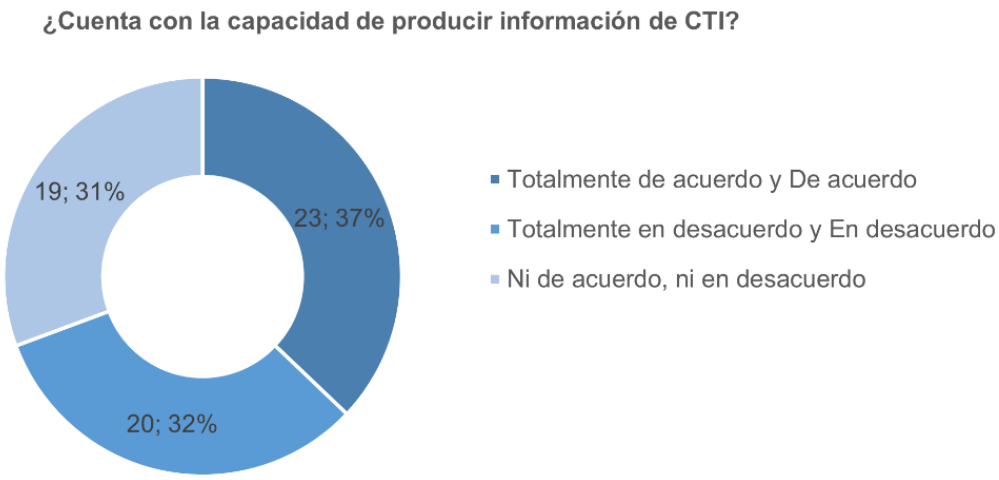
Figura 31. Resultado 14 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

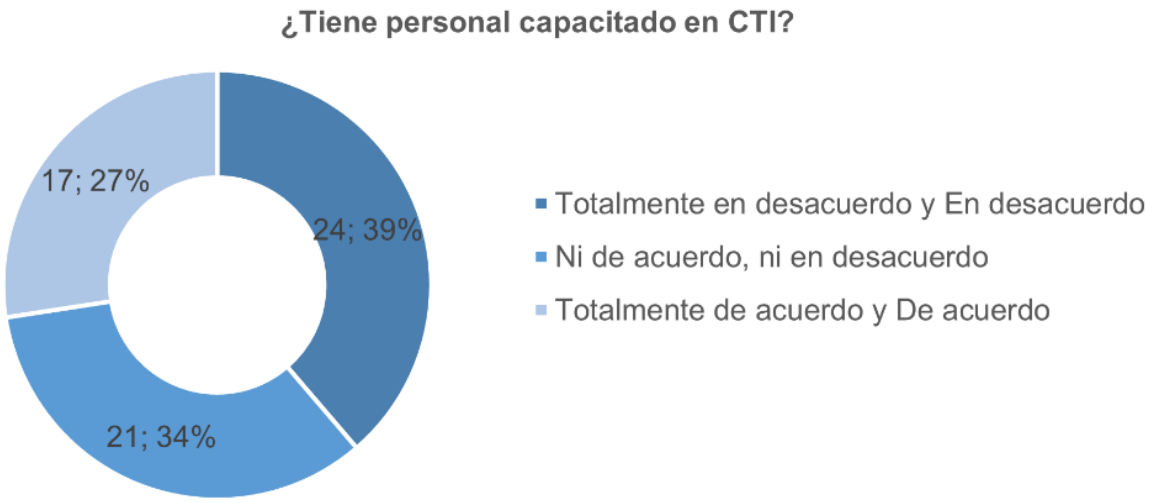
Por otra parte, se evidencia que las entidades no tienen suficiente capacidad de producir CTI, considerando que la población manifestó un aspecto positivo del 37%, mientras que el 32% se mostró neutro y el 31% manifestó un aspecto negativo. Estas cifras se relacionan con los resultados sobre el personal capacitado, ya que se expresó un aspecto negativo del 39 %, con un estado neutro del 34 % y el 27 % positivo. Con base a estos resultados, se entiende porque las entidades hacen uso de servicios tercerizados para los recursos de CTI.

Figura 32. Resultado 16 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

Figura 33. Resultado 17 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

Uno de los propósitos de esta investigación, corresponde a que tan viable puede ser una estrategia de CTI como medida de anticipación de eventos, incidentes o la materialización de riesgos cibernéticos. Los encuestados manifestaron un aspecto positivo del 93%, en cuanto a que este mecanismo puede ayudar a anticipar este tipo de conductas, lo que muestra ser un buen indicador de éxito al momento que se pretenda por parte del gobierno colombiano generar una estrategia de este estilo.

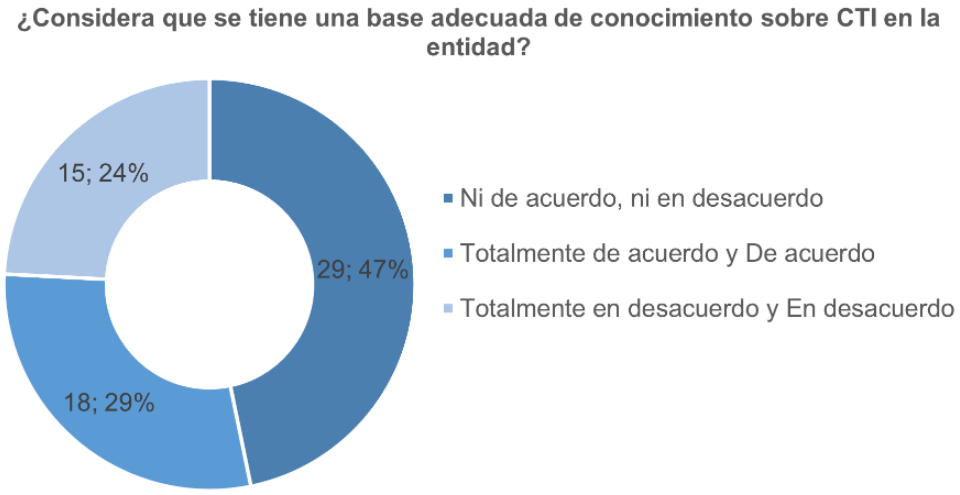
Figura 34. Resultado 18 encuesta nivel de apropiación del CTI.

Nota. Elaboración propia.

En este sentido, "…Una adecuada estrategia de CTI, permitiría cambiar el rol de reacción que se aplica en la actualidad a un rol proactivo, con el fin de minimizar el riesgo que existe sobre las plataformas tecnologías. Es importante, enseñar a las entidades a conocer quién es su enemigo, de esta forma las estrategias de CTI, se pueden encaminar de mejor manera…" (Entrevista a John Guevara, Jefe Grupo Ciberinteligencia de la Policía Nacional, 15/11/23).

Se observa un aspecto de atención relacionado con las bases de datos de conocimiento que permiten generar un adecuado CTI, considerando que, la población encuestada se muestra neutral en un 47 %, mientras que el 29 % muestra un aspecto positivo y un 24 % manifiesta un aspecto negativo con la utilidad de las bases de conocimiento, con lo que la estrategia debe plantear un escenario que permita fortalecer el conocimiento en las organizaciones.

Figura 35. Resultado 19 encuesta nivel de apropiación del CTI.

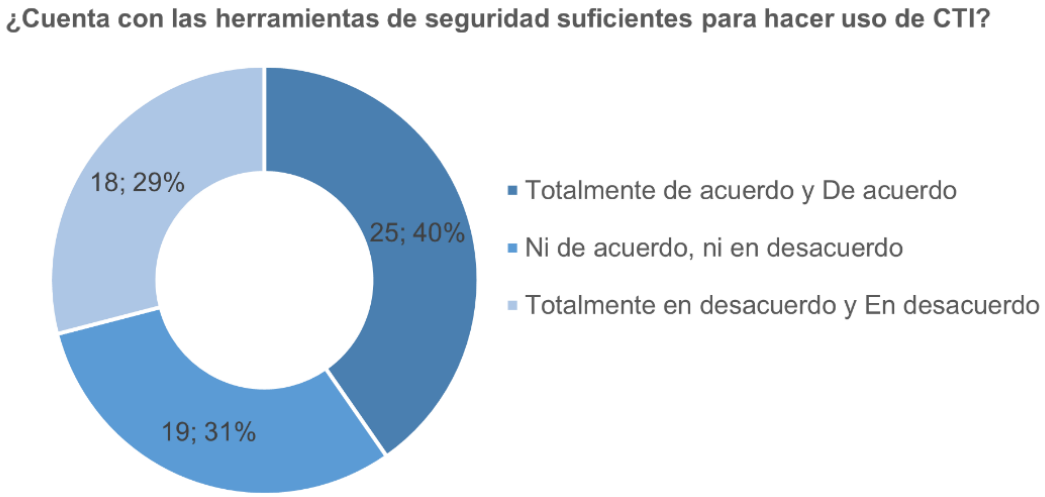


Nota. Elaboración propia.

Ante esto, “La gestión adecuada y anticipada de procesos de inteligencia contra actores maliciosos puede ser de gran ayuda para mitigar su accionar y efectos relacionados (…) Una estrategia CTI debe estar adaptada a los intereses y activos a proteger por cada organización. Los mecanismos de articulación y difusión de información son otro escenario que puede estar liderado por un ente concentrador.” (Entrevista a Mike Toro, director tecnologías avanzadas del Center for CIC, 09/11/23).

El uso de CTI generalmente requiere de herramientas, especialmente en el nivel operacional y táctico, siendo importante conocer la capacidad con la que cuentan las entidades para la implementación de CTI. Ante esto, el 40% de la población encuestada manifestó un aspecto positivo en cuanto a contar con herramientas de seguridad suficientes para el uso de CTI. El 31 % ser mostró neutro y el 29 % manifestó un aspecto negativo.

Figura 36. Resultado 20 encuesta nivel de apropiación del CTI.



Nota. Elaboración propia.

En este punto es importante resaltar que, “En general, las entidades tienen una buena gestión de infraestructura para aplicar CTI. Sin embargo, hay algunas áreas que

podrían mejorarse. Una de las áreas que podrían mejorarse es la integración de la CTI con las herramientas y procesos de seguridad existentes. La CTI debe ser fácil de integrar con las herramientas y procesos de seguridad existentes para que las entidades puedan aprovecharla de manera efectiva. Otra área que podría mejorarse es la capacitación del personal de seguridad de la información en CTI. El personal de seguridad de la información debe estar capacitado para comprender y aplicar la CTI para que puedan ayudar a proteger las entidades de los ataques cibernéticos." (Entrevista a Jhon Méndez, Jefe Grupo CSIRT de la Policía Nacional, 19/12/23).

De igual forma es importante entender que, el CTI "… Es algo que está en mora de ser usado por todas las empresas y entidades, esto no es solo para las que tienen recursos, es un tema de aplicar un concepto de poder conocer cuáles son las amenazas que existen para un ambiente determinado (…) Es un conocimiento muy poco explorado y muy poco ofrecido. Se ha considerado solo un tema de tecnologías y poco se ha hecho hincapié en el tema del concepto en sí." (Entrevista a Andrés Almanza, creador de la comunidad CISOS.CLUB, 20/11/23).

9.3.1. Planteamiento de la estrategia CTI

Para este planteamiento, hay que definir un proceso, y lo más oportuno sería soportarnos en el modelo tradicional del ciclo de inteligencia, teniendo en cuenta los modelos expuestos anteriormente.

Dado esto se aplicarán las fases de recolección, procesamiento, análisis y difusión planteadas en la ley 1621 de 2013, incluyendo una etapa adicional denominada direccionamiento necesaria para los modelos CTI. Esto teniendo en cuenta que a partir de la experiencia y madurez de las entidades que aplican el ciclo sobre la inteligencia

tradicional servirían como dinamizadores para la aplicación del CTI, con base a lo anterior se tiene lo siguiente:

- **Dirección:** Es la fase en la que se debe establecer la hoja de ruta por parte de la entidad líder de la estrategia, enfocando esfuerzos en la creación de indicadores de gestión, cumplimiento, obligaciones, alianzas, fortalecimiento de las capacidades y herramientas, todo alineado a la definición de objetivos y demás acciones que conlleven a que el proceso de CTI tenga éxito a nivel gubernamental.
- **Recolección:** En esta fase, se debe priorizar la recopilación de datos e información asociados a las amenazas del ciberespacio (vulnerabilidades, IoCs, fugas de información, etc), en el contexto local e internacional con injerencia en las plataformas gubernamentales del país, esta actividad, aunque puede ser desarrollada por medio de herramientas, una buena práctica es generar el conocimiento necesario en el Estado para ser auto suficiente de este tipo de recolección, ya que no sería estratégico tener una inteligencia de amenazas provista por otro Estado.
- **Procesamiento:** Los datos recopilados sin excepción deben ser categorizados, normalizados y estandarizados, entregando al proceso de análisis una escala de importancia, por ejemplo (0-5). Una vez procesados, es imperioso definir un repositorio seguro que permita el acceso a los usuarios finales. En esta fase es importante poner especial cuidado a las actividades de descartar los falsos positivos y aceptar los falsos negativos.
- **Análisis:** A partir del procesamiento de los datos y la información, es necesario realizar un análisis que permitan plantear las acciones y recomendaciones que deben seguir las instituciones para contrarrestar las posibles amenazas que se ciernen sobre las infraestructuras gubernamentales, de igual forma, categorizar el tipo de información dando respuestas a ¿quién?, ¿cómo?, ¿dónde? y ¿por qué?

con el propósito de anticipar posibles afectaciones teniendo un contexto verdadero de la amenaza.

- **Difusión:** La fase que cierra el ciclo, ya que pone a disposición de las partes interesadas la información de inteligencia, considerando que la presentación de los datos debe alinearse a la población objetivo**.** Por lo tanto, el lenguaje debe ser adecuado al uso o receptor de la información en el ámbito estratégico, operativo, táctico o técnico, por medio de un formato estandarizado y entendible.

Con base a lo anterior, culminado el ciclo de CTI cada una de las entidades tiene la opción de tomar decisiones respecto al panorama ofrecido en el contexto de la inteligencia de amenazas, para así minimizar la materialización de riesgos cibernéticos.

Por tal razón, “Una estrategia de CTI puede impactar positivamente la salvaguarda de la información al proporcionar información privilegiada de primer nivel, permitiendo la anticipación y respuesta proactiva a eventos, incidentes y riesgos cibernéticos.” (Entrevista a Julián Giraldo, integrante del Comando Conjunto Cibernético, 16/11/23).

Ante los resultados obtenidos durante la investigación, se tienen otros aspectos que deben ser tenidos en cuenta dentro del planteamiento de la estrategia como son:

- **Capacitación:** aunque el 81% de la población manifestó un aspecto positivo en el entendimiento del CTI, es importante establecer programas de capacitación para llegar a un 100%. Además, de que solo el 39 % se mostró con un aspecto positivo en cuanto a tener personal capacitado en la temática.
- **Implementación del uso de CTI:** se debe llegar a un uso de CTI del 100%, puesto que solo el 58% lo manifestó como un aspecto positivo, sumado a que un 45 % de los que hacen uso de esta capacidad dependen de proveedores de servicio.

- **Compartir información:** el CTI debe conllevar a que las entidades compartan información o suministren datos asociados a indicadores de compromiso, ya que el 69% mostró como aspecto positivo el uso de esta información cuando es suministrada por un tercero afectado por un incidente de seguridad.
- **Producción CTI:** si bien es cierto que solo el 37 % manifestó tener capacidad de producir información de CTI, se debe plantear mecanismos en los que las entidades puedan aportar al proceso de recolección, donde alguna entidad con capacidad pueda continuar con el ciclo CTI, permitiendo aportar a todo el ecosistema de entidades.
- **Herramientas:** solo el 40% manifestó como aspecto positivo contar con herramientas para hacer uso de CTI. Esto hace necesario que la estrategia establezca la forma de proteger a las entidades que no tienen dicha capacidad ya sea por personal capacitado o presupuesto. Es necesario, establecer alianzas estratégicas, de forma que la CTI pueda ser usada y aplicada por todos los actores del ecosistema.

Finalmente, la entrevista a los expertos determina que la entidad a liderar la estrategia debería ser la futura Agencia de Seguridad Digital en caso de llegar a crearse, ya que el 60% de los entrevistados recalca que la responsabilidad debe recaer sobre ella desde el liderazgo en el ámbito estratégico. También se hace mención de que el ColCERT debería liderar esta estrategia, aunque desde el enfoque técnico. En atención a lo anterior, se podría dar una articulación estratégica y técnica en cuanto al liderazgo de la estrategia de CTI, puesto que se requiere de ambos enfoques para tener viabilidad de éxito en la misma.

“Quien maneje está estrategia debe tener la capacidad de lograr un trabajo armónico entre públicos y privados, presidencia con una buena capacidad técnica o la agencia que se pretende crear, pero con las funciones que le permita controlar los ISP.”

(Entrevista a John Guevara, Jefe Grupo Ciberinteligencia de la Policía Nacional, 15/11/23).

9.3.2. Propuesta de un plan de acción para contar con una línea base mínima de cumplimiento de Inteligencia de Amenaza en el Estado

Dado que en las diferentes encuestas realizadas se observa un nivel diferente de madurez en las entidades que hicieron parte de la muestra, y teniendo claro que el camino óptimo para que una estrategia de inteligencia de amenazas funcione adecuadamente, es contar con unos niveles mínimos de apropiación, se definen unas tareas a implementar en los siguientes aspectos, así:

1. Alineación estratégica
2. Alineación organizacional
3. Gestión del talento humano
4. Capacidades técnicas

La estrategia de inteligencia de amenazas está soportada en un ciclo que se compone de las fases de dirección, recolección, procesamiento, análisis y difusión. Sin embargo, para llevar a cabo esta articulación se requiere de implementar los cuatro aspectos definidos anteriormente.

1. Alineación estratégica

- **Modelo de Seguridad y Privacidad de la Información (MSPI)**

En la actualidad el modelo de seguridad y privacidad de la información es de obligatorio cumplimiento para las entidades del Estado. Sin embargo, dentro de la descripción de su normatividad aun no incluye la actualización de los controles establecidos en la nueva versión de la ISO27001/2022.

- ✓ La primera alineación estratégica es que el Ministerio de las Tecnologías de la Información evalué la inclusión del cumplimento normativo del MSPI, así como la actualización de la norma ISO27001/2022, específicamente el cumplimiento al control **(5.7 Inteligencia sobre amenazas)**.

En el MSPI, el control debe contar con el desglose de todas las actividades a realizarse para el desarrollo de una estrategia de CTI en entidades gubernamentales como se plantea en el presente trabajo.

Tiempo de implementación: 4 meses, una vez sea aprobado este plan de acción.

Una vez realizada la actividad anterior, se debe medir el nivel de adopción del control por parte de las entidades involucradas hasta que se alcance un nivel satisfactorio.

Tabla 4. Identificador de nivel implementación del control 5.7.

Identificador de nivel implementación del control 5.7 Inteligencia de Amenazas	
Definición	Una vez realizada la actualización de la ISO27001:2022 en el MSPI se debe medir la cantidad de entidades que implementan este control de la norma.
Objetivo	Identificar el nivel de adopción de CTI en las entidades gubernamentales de orden Nacional
Instrumento	Índice de Gobierno Digital
Fórmula	NI_CTI= ((EON_CTI)/(T_EON)) X100
Descripción de las variables	NI_CTI = Nivel de Implementación de CTI (porcentaje) EON_CTI = Entidades del Orden Nacional con CTI (números enteros) T_EON = Total de Entidades del Orden Nacional (números enteros)
Responsable de la medición	MINTIC
Frecuencia de la medición	FR= trimestral

Valoración del indicador	NI_CTI >80% Satisfactorio NI_CTI >50% y <80% Aceptable NI_CTI <50% No Aceptable
Umbral	> 80%

Nota. Elaboración propia.

2. Alineación organizacional

Para tener una alineación organizacional que permita incluir el control de inteligencia de amenazas en las entidades gubernamentales, es necesario incluir como mínimo en los procesos y roles de la entidad lo correspondiente a inteligencia de amenazas, así:

- **Proceso de CTI:** diseñar un procedimiento de inteligencia de amenazas el cual debe contar con un ciclo de cinco (5) fases como se plantea en el **ítem 9.3.1** del presente trabajo, incluyendo las fases de dirección, recolección, procesamiento, análisis y difusión.

- **Roles:** dentro los roles y responsabilidades de seguridad y privacidad de la información de las entidades gubernamentales descritas en el MSPI, se debe incluir una función que relacione la tarea de inteligencia de amenazas.

  - ✓ La función de inteligencia de amenazas deberá ser asumida por un nuevo funcionario o en su defecto por el que actualmente cuente con estas funciones

Tiempo de implementación: 3 meses, una vez completado el punto anterior.

3. Gestión del talento humano

En pro de realizar la implementación de la estrategia de inteligencia de amenazas y teniendo en cuenta la alineación estratégica y organizacional, se hace necesario que las entidades gubernamentales cuenten con el talento humano capacitado en inteligencia amenazas para el desarrollo de los procesos y roles anteriormente expuestos. Si bien es cierto, se obtuvo un 81% de aspecto positivo del concepto, es importante aclarar que una cosa es conocer y otra aplicar, tal y como se observa en las cifras del personal capacitado, donde se evidenció un aspecto negativo del 39% contra 27% de aspecto positivo.

Bajo este entendido, dentro de los conocimientos formales que debe tener el funcionario que cumpla con el rol y responsabilidad como mínimo son, un curso de **Inteligencia de amenazas cibernéticas**, el cual contenga los siguientes temas:

- Ciclo de inteligencia.
- Inteligencia y requisitos sobre amenazas cibernéticas.
- Metodologías de cadenas de ataques.
- El conjunto de habilidades fundamentales: análisis de intrusiones.
- Fuentes de recolección.
- Análisis y Producción de inteligencia.
- Difusión y Atribución.
- Artefactos e indicadores de compromiso.

Tiempo de implementación: 3 meses, una vez completado el anterior.

Estos conocimientos específicos deben ser incluidos en los requisitos del personal que se postule u ostente el rol y responsable de la seguridad y privacidad de la información en las entidades gubernamentales del Estado, lo cual debería ser incluido en

el MSPI para tener un estándar de los requerimientos puntuales de las capacidades del personal en cuanto a CTI.

Nota: Como mínimo las entidades deberían tener una persona con los conocimientos anteriormente expuestos, y el cual debe medirse con el indicador expuesto a continuación:

Tabla 5. Personal capacitado en Inteligencia de Amenazas.

Personal capacitado en Inteligencia de Amenazas	
Definición	Se busca establecer la cantidad de entidades que cuentan con personal capacitado en CTI.
Objetivo	Medir la cantidad de funcionarios con capacidades de CTI que permitan aportar a la estrategia.
Instrumento	Gobierno Digital
Fórmula	NC_CTI = ((FC_CTI)/(TFC_EON)) X100
Descripción de las variables	NC_CTI = Nivel Capacitación CTI (porcentaje) FC_CTI = funcionarios capacitados CTI (números enteros) TFC_EON = Total funcionarios de Capacitación CTI (números enteros)
Responsable de la medición	MINTIC
Frecuencia de la medición	FR= trimestral
Valoración del indicador	NC_CTI >80% Satisfactorio NC_CTI >40 y <80% Aceptable NC_CTI <40% No Aceptable
Umbral	> 80%

Nota. Elaboración propia.

4. Capacidades técnicas

4.1. Listas de distribución: cada una de las entidades como mínimo debe hacer parte de al menos una lista de distribución de alertas cibernéticas sobre amenazas a nivel nacional e internacional.

- **Nacional**

- Lista de distribución **Colcert**

  Página Web: https://www.colcert.gov.co/800/w3-propertyvalue-412601.html

- Lista de distribución Policía Nacional de Colombia

  Página Web: https://cc-csirt.policia.gov.co/

- **Internacional**

- Lista de distribución **CERT US**

  Página Web: https://www.cisa.gov/news-events/cybersecurity-advisories

- Lista de distribución **INCIBE**

  Página Web: https://www.incibe.es/incibe-cert/blog

Es importante tener en cuenta que se requiere fortalecer los entes nacionales de distribución de alertas cibernéticas a nivel gubernamental, por lo tanto, la fase de difusión es fundamental en este punto de la estrategia, ya que el propósito es que se genere información del contexto local a partir de la recolección de información que permita tener mayores insumos para la generación de información de CTI.

4.2. **Ingeniería inversa:** las entidades deberán contar con las capacidades técnicas de análisis de phishing, malware y vulnerabilidades dispuestas en línea como son:

- **Nacional**

  - **Colcert**
  - Página Web: https://www.colcert.gov.co/800/w3-channel.html
  - **CC-CSIRT Policía**

- Página Web: https://cc-csirt.policia.gov.co/

- **Centro Cibernético Policial**
- Página Web: https://caivirtual.policia.gov.co/

- **Internacional**
- **Virustotal**
- Página Web: https://www.virustotal.com/

- **Any Run**
- Página Web: https://any.run/

- **Shodan**
- Página Web: https://www.shodan.io/

Los documentos, Url, archivos o artefactos que en algún momento puedan presentar una amenaza según los parámetros establecidos en un procedimiento de inteligencia de amenazas determinado en el MSPI, deberán ser analizados con estas herramientas, con el fin de entender desde la entidad si es efectivamente una amenaza o un falso positivo. Bajo este aspecto, es importante tener en cuenta que en la actualidad Colombia cuenta con una Sandbox Nacional de acceso al público en general gestionada por el CSIRT-PONAL, la cual podría ser el punto de recolección focalizado de las ciberamenazas que circulan en el país, permitiendo capacidades de CTI propias a nivel gubernamental, para lo cual los entes nacionales relacionados en este punto, podrían

determinar las necesidades de recolección mediante la fase de dirección, al igual que las de procesamiento y análisis.

En el planteamiento de este escenario se puede definir un indicador de medición que permitan conocer el porcentaje de entidades que tienen implementada una Sandbox en el entorno local de cada entidad, con el objetivo de conocer las posibles ciberamenazas que lleguen a la misma y cuyo ciclo interno de CTI apoye a la estrategia nacional con la identificación de IoCs con calidad de los datos.

Tabla 6. Nivel de implementación de Sandbox en las entidades.

Nivel de implementación de Sandbox en las entidades	
Definición	Identificar la cantidad de entidades del orden nacional que tienen desplegada una Sandbox a nivel interno para desarrollar el ciclo CTI
Objetivo	Medir la cantidad del despliegue de Sandbox internas en las entidades
Instrumento	Gobierno Digital
Fórmula	NIS_CTI= ((SEON_CTI)/(T_EON)) X100
Descripción de las variables	NC_CTI = Nivel Implementación Sanbox CTI (porcentaje) SEON_CTI = Sandbox implementadas en Entidades del Orden Nacional CTI (números enteros) T_EON= Total Entidades del Orden Nacional CTI (números enteros)
Responsable de la medición	MINTIC
Frecuencia de la medición	FR= trimestral
Valoración del indicador	NIS_CTI >80% Satisfactorio NIS_CTI >40 y <80% Aceptable NIS_CTI <40% No Aceptable
Umbral	> 80%

Nota. Elaboración propia.

Nota: las herramientas nacionales son gratuitas, las internacionales tienen acceso libre limitado; pero a través del fortalecimiento y generación de capacidades de CTI propias, las entidades deben propender por adquirir estos servicios dispuestos a nivel nacional como parte del cumplimiento de la estrategia o implementar mecanismos

propios para uso general de las entidades del gobierno, de forma que el país sea un referente en capacidades CTI focalizadas y con desarrollo propio.

4.2.1. Búsqueda sobre Dark web

Dentro de esta capacidad gubernamental, se debe implementar la búsqueda con recursos propios o a través de una herramienta tercerizada, en el que se evidencie la exposición de datos de interés de las instituciones del Estado relacionadas con: usuario, contraseñas, vulnerabilidades, entre otros. Las cuales puedan hacer parte del flujo de validación dispuesto en el procedimiento de inteligencia de amenazas, como una afectación a la confidencialidad, disponibilidad e integridad de la información, evidenciando así afectaciones en las infraestructuras tecnológicas de las organizaciones y sus usuarios.

4.3. MISP (Plataforma de intercambio de información sobre malware)

Una MISP es una plataforma de inteligencia de amenazas tipo Open Source que permite compartir, almacenar y correlacionar diferentes indicadores de compromiso (IOCs) ya sea de ataques dirigidos e información de vulnerabilidades, permitiendo compartir de manera oportuna los datos en todas las instancias que se encuentren interconectadas.

De igual forma, cuando las entidades implementen el proceso de CTI, se requiere interconexión a través de plataformas de inteligencia de amenazas como el MISP, por eso es importante medir la cantidad de entidades conectadas a los repositorios donde cada entidad puede aportar información CTI con datos de calidad.

Tabla 7. Interconexión de plataforma MISP.

Interconexión de plataforma MISP	
Definición	En CTI se requiere de compartir información, por lo cual es necesario medir la interconexión de la plataforma MISP
Objetivo	Medir la cantidad de entidades conectadas a través de la plataforma MISP
Instrumento	Plataforma MISP
Fórmula	NCM_CTI= ((EONM_CTI)/(T_EON)) X100
Descripción de las variables	NCM_CTI = Nivel de conexión MISP CTI (porcentaje) EONM_CTI = Entidades del Orden Nacional conectadas a la MISP CTI (números enteros) T_ EON= Total Entidades del Orden Nacional (números enteros)
Responsable de la medición	MINTIC
Frecuencia de la medición	FR= trimestral
Valoración del indicador	NCM_CTI >70% Satisfactorio NCM_CTI >30 y <70% Aceptable NCM_CTI <30% No Aceptable
Umbral	> 70%

Nota. Elaboración propia.

Tiempo de implementación: 3 meses, una vez completado el anterior.

En la actualidad el CSIRT-PONAL hace uso de la Sandbox y la MISP, siendo referente en su uso. Por tal razón, una vez implementado lo planteado en la estrategia, es factible usar estas tecnologías y compartir la información sobre las amenazas que se presenten sobre las plataformas tecnológicas. Esto se describe en el ítem **11.2 Trabajos futuros**.

Finalmente, es importante resaltar que la recolección es una fase que puede ser complementada con las herramientas descritas, sin embargo, es importante medir la calidad de la información de CTI obtenida, por lo cual, se plantea el siguiente indicador

considerando el uso de las plataformas de recolección de información como apoyo al proceso de CTI, así:

Tabla 8. Efectividad en la recolección de Inteligencia de Amenazas.

Efectividad en la recolección de Inteligencia de Amenazas	
Definición	Se requiere conocer la calidad de los datos identificados como amenazas a partir de la recolección de información.
Objetivo	Medir la efectividad en la calidad del dato.
Instrumento	Plataforma de recolección (Sandbox)
Fórmula	ED_CTI= ((AD_CTI)/(TIR_P)) X100
Descripción de las variables	ED_CTI = Efectividad del dato CTI (porcentaje) AD_CTI = Amenazas detectadas CTI (números enteros) TIR_ P= Total de Información Recolectada en la Plataforma (números enteros)
Responsable de la medición	Cada entidad
Frecuencia de la medición	FR= trimestral
Valoración del indicador	ED_CTI >30% Satisfactorio ED_CTI >5 y ED_CTI <30% Aceptable ED_CTI <5% No Aceptable
Umbral	> 30%

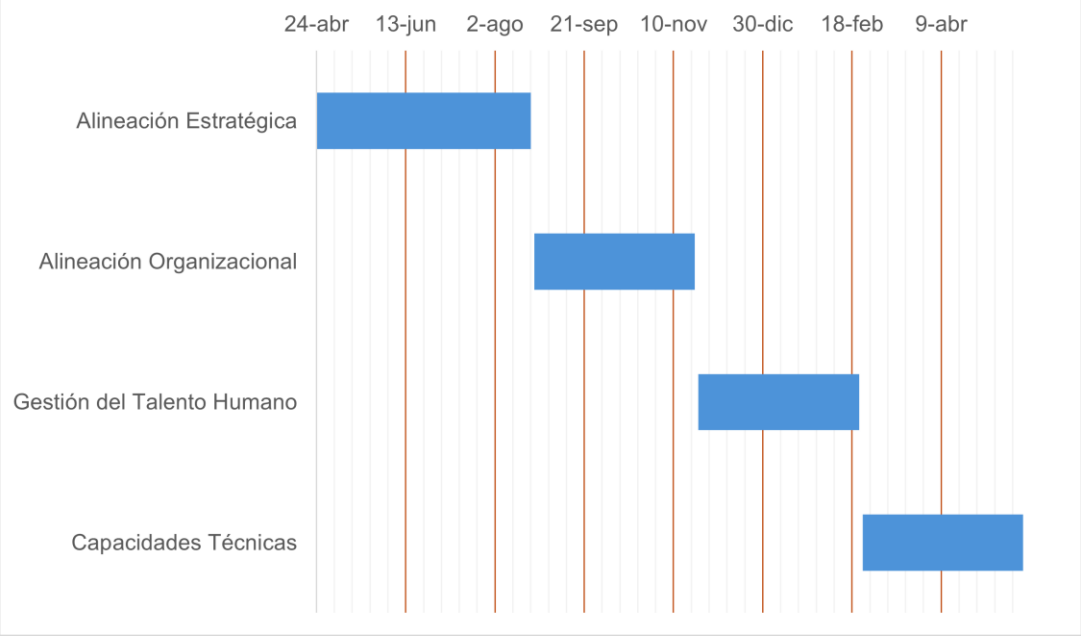
Nota. Elaboración propia.

Nota: Teniendo en cuenta que en la Sandbox pueden subir demasiada información, no toda puede ser útil para generar datos de CTI, por lo cual, el indicador se plantea con un umbral bajo y según la evolución de la estrategia podría tomar un valor mayor. A partir de lo anterior, los IoCs verificados que sean obtenidos a través de la Sandbox deberán ser adjuntados a la MISP, de acuerdo con los parámetros establecidos en el proceso CTI.

4.4. Cronograma estrategia Inteligencia de amenazas

Para la planificación, control y gestión de la estrategia de Inteligencia de Amenazas, se establece un tiempo de 13 meses para garantizar su implementación.

Figura 37. Cronograma estrategia Inteligencia de amenazas.



Nota. Elaboración propia.

10. Discusión

Esta investigación monográfica permitió evidenciar la viabilidad de una estrategia de CTI en las entidades gubernamentales de Colombia para anticipar los eventos, incidentes o materialización de riesgos cibernéticos, con la que se oriente la toma de decisiones de políticas de seguridad digital. Lo anterior es importante, teniendo en cuenta lo manifestado por Paris (Koloveas, Chantzios, Alevizopoulou, Skiadopoulos, & Tryfonopoulos, 2021). En cuanto a que las amenazas cibernéticas han aumentado en cantidad y métodos de sofisticación, debido al surgimiento de nuevas herramientas con las que atacan a sus víctimas.

De igual forma, el planteamiento de la estrategia surge a partir de los resultados de los instrumentos utilizados con funcionarios pertenecientes a las entidades del Estado de orden nacional. La investigación propuesta plantea la necesidad de un mecanismo que amplíe la perspectiva de la atención de incidentes, enfocado en utilizar CTI como defensa ante las amenazas cibernéticas mediante un modelo estándar (Schlette, Caselli, & Pernul, 2021).

Desde otro enfoque, la investigación estableció que CTI se convierte en una necesidad dada por la ISO 27001 en la versión 2022 como lo plateó (Ta-Seen, 2023). A partir de lo anterior, el MSPI de MinTIC es una herramienta gubernamental basada en esta normatividad, que cuando sea actualizada deberá tener en cuenta la adición del control 5.7 que se enfoca en la inteligencia de amenazas, mediante la cual las organizaciones obtendrán información de amenazas que se ciernen sobre su infraestructura.

Por otra parte, se logra evidenciar que la normatividad existente no es suficiente con relación a la temática planteada en la investigación, pues el análisis plantea que el

CTI es un término que no se encuentra plasmado a nivel documental en el sector gubernamental colombiano. El referente más cercano a nivel documental son los Estados Unidos. Este país promulgó la Ley de Intercambio de Información de Ciberseguridad de 2015, en el que se exigió establecer capacidades y procedimientos que permitieran el intercambio oportuno de indicadores de compromiso (Jasper, 2017).

Además de lo anterior, se destaca el hecho que plantea la creación de una agencia encargada de las políticas de seguridad, para lo cual, esta entidad debería tener en cuenta el intercambio de información con el objetivo de tener un panorama del contexto de las ciberamenazas locales e internacionales, estableciendo un lenguaje y procedimiento estándar que permita la protección ante ataques cibernéticos (Gao, Li, Peng, Fang, & Yu, 2022). Por lo anterior, es importante que en las mesas de trabajo sean planteados los conceptos y beneficios del CTI para la protección de infraestructuras tecnológicas, desplegando las acciones que considere necesarias para su definición e implementación.

Es importante recalcar que, el panorama de la ciberseguridad ha cambiado durante los últimos años y mientras la tecnología evoluciona y se adapta a los nuevos escenarios, surgen nuevos vectores de ataque sofisticados. Estas amenazas cuentan con características que permiten realizar ataques complejos, complicando la detección y mitigación de estos, sobrepasando así las capacidades de defensa existentes. Por tal razón, es importante que las entidades implementen enfoques proactivos, pasando de los mecanismos de defensa tradicionales a los anticipativos. (de Melo e Silva, de Oliveira Albuquerque, García Villalba, & Costa Gondim, 2020).

Finalmente, la hipótesis planteada en este estudio, consistente en que la implementación de una estrategia de amenazas cibernéticas anticipa la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos en las entidades gubernamentales de Colombia, es aplicable al contexto nacional dado que es de interés

para el sector, con el cual es posible conocer el panorama de amenazas que convergen en el ciberespacio y que pueden llegar a convertirse en un hecho relevante que afecte el normal desarrollo de las operaciones de las instituciones. Esto aplica tanto para entidades públicas y privadas, por lo que la información obtenida a través de CTI debe ser de calidad y de carácter cooperativo, implementando los cambios legislativos que correspondan (Schaberreiter, y otros, 2019).

11. Conclusiones y trabajos futuros

1.1. Conclusiones

Considerando la investigación realizada sobre una estrategia CTI en las entidades gubernamentales en Colombia, se logró evidenciar que aún no se ha implementado el mecanismo y que a nivel normativo no se ha referido la temática. De igual forma, el MSPI aún no incorpora este control, por lo cual, no existe un ciclo CTI definido, ni los conceptos asociados que determinen los lineamientos a seguir por parte de las entidades gubernamentales.

Se encontró que se materializaron muchos riesgos cibernéticos en las entidades gubernamentales, generando impactos negativos en sus procesos y que trascendieron a la ciudadanía. Además, la investigación nos permitió validar que el mayor riesgo existente sobre las entidades se derivada de vectores de ataque originados por malware y phishing principalmente, lo que deja ver un panorama importante sobre la atención de las ciberamenazas.

Finalmente, se logró determinar que es necesaria una estrategia de CTI que minimice el riesgo y oriente adecuadamente la toma de decisiones, soportada en el actual ciclo de inteligencia dada su madurez, confiabilidad y efectividad demostrada en la anticipación y prevención de riesgos tradicionales, lo que, sin grandes ajustes solo en el direccionamiento puede traslaparse a los entornos digitales (CTI).

1.2. Trabajo futuro

A partir de los conocimientos adquiridos en el desarrollo del ejercicio académico de la maestría, se puede desarrollar un proyecto que impacte considerablemente múltiples sectores, dependiendo de la relevancia que cada uno le dé a la ciberseguridad

y a la forma en que se pueden anticipar los eventos, incidentes o materialización de riesgos cibernéticos.

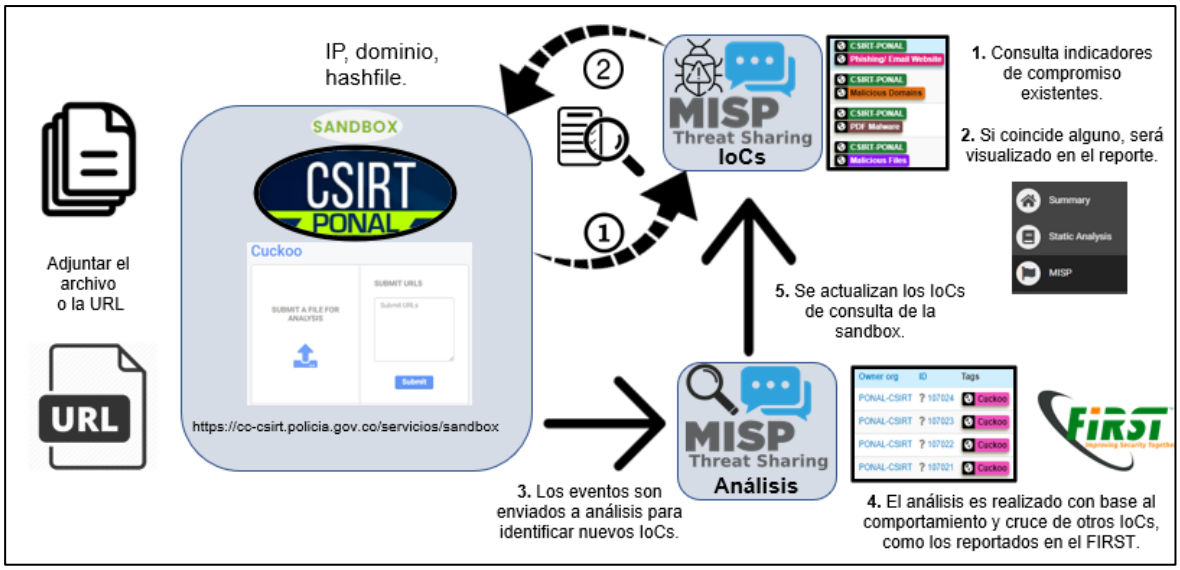
El uso de la tecnología se refiere a herramientas y técnicas implementadas para construir un sistema o una aplicación, haciendo uso de lenguajes de programación, modelos de bases de datos, infraestructura, entre otros. Esto básicamente se traduce en que existe un modelo de negocio en el que existe competencia y por ende también unos proveedores y clientes, lo que se deriva en procesos contractuales de carácter individual para la adquisición de una capacidad de CTI a nivel gubernamental.

Con el proyecto en proceso, lo que se busca es generar una estrategia de CTI que permita orientar por medio de la anticipación los procesos de ciberseguridad en las entidades del Estado para prevenir la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos. Sin embargo, es importante tener claro que, generalmente, CTI suele desarrollarse en el ámbito privado de acuerdo con las metodologías usadas por quien brinde el servicio. Por tal razón, al generar un mecanismo de uso común a las organizaciones, que puede llegar a tener un alcance en lo público y privado, se podrían enfocar los esfuerzos a combatir el actuar delictivo de los cibercriminales que sacan provecho de las falencias actuales de las organizaciones.

En un primer paso y aplicando la recolección como una de las fases comunes de los modelos de CTI, se puede llegar a implementar una herramienta en la que las entidades del estado colombiano aporten diferentes insumos de las campañas maliciosas que se presentan en el contexto del ciberespacio y que de una u otra forma trascienden a la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos. Esto de forma posterior a la planeación y dirección de lo que se quiere hacer se convierte en un

paso fundamental para desarrollar las demás fases que se definan, como puede ser el análisis, tratamiento y difusión (ver Figura 37).

Figura 38. *Modelo herramienta para la fase de recolección CTI.*



Nota. Fuente propia.

Uno de los factores claves en la inteligencia de amenazas es la recolección de información, pero la difusión en todos los niveles puede conllevar al éxito de una estrategia de CTI. Por lo tanto, definir las acciones y cómo se realizarán en cada una de las fases es fundamental para poder orientar la toma de decisiones en el ámbito de la ciberseguridad, siendo este un avance que futuros investigadores pueden retomar para medir sus resultados y así evaluar la eficacia de este tipo de estrategias, pudiendo plantear mejoras y desarrollar nuevas investigaciones, por lo que otros pueden continuar con los avances realizados en el presente proyecto.

12. Referencias

Función Pública. (24 de 07 de 2000). *Ley 599*. Obtenido de https://www.funcionpublica.gov.co/: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

ACIC, A. C. (2017). *Australian Criminal.* Obtenido de afp.gov.au: https://www.afp.gov.au/sites/default/files/PDF/ACIM-strategy-2017-20.pdf

Aggarwal, D., & Gautam, S. (2017). Threat Intelligence: Let‟s Make Internet Secure. *College of Computing Sciences and Information Technology (CCSIT)*. Obtenido de https://icac.tmu.ac.in/wp-content/uploads/2020/11/A8.pdf

Akbanov, M., Vassilakis, V., & Logothetis, M. (21 de 03 de 2019). *Ransomware detection and mitigation using software-defined networking: The case of WannaCry.* Obtenido de sciencedirect.com: https://www.sciencedirect.com/science/article/abs/pii/S0045790618323164?via%3Dihub

Almanza, A. (01 de 07 de 2022). XXII Encuesta Nacional de Seguridad Informática. Resiliencia un aspecto clave en la ciberseguridad. (55), 163. doi:10.29236/sistemas.n163a4

Banco de la República de Colombia. (02 de 08 de 2023). *Informe de Política Monetaria - Julio de 2023*. Obtenido de banrep.gov.co: https://www.banrep.gov.co/es/publicaciones-investigaciones/informe-politica-monetaria/julio-2023

Betancourt, A. (30 de 11 de 2022). *Sanitas y Colsanitas continúan sin servicios digitales tras ataque cibernético*. Obtenido de enter.co: https://www.enter.co/colombia/sanitas-y-colsanitas-continuan-sin-servicios-digitales-tras-ataque-cibernetico/

Bianco, D. (17 de 01 de 2014). *Enterprise Detection & Response*. Obtenido de http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Bonilla Mora, A. (14 de 09 de 2023). ¿Hay procesos judiciales en riesgo por ataque cibernético? Judicatura responde. *El Tiempo*, págs. https://www.eltiempo.com/justicia/cortes/hay-procesos-judiciales-en-riesgo-por-ataque-cibernetico-judicatura-responde-806156.

BreachForums. (17 de 01 de 2023). *Colombia - Users of social assitance programs Sisben (25 Millon Records) (08 2021).*

Brodersen, J. (21 de 09 de 2023). *IFX Networks: un ciberataque a una multinacional afecta a pymes y grandes empresas argentinas*. Obtenido de https://www.clarin.com/tecnologia/ifx-networks-ciberataque-multinacional-afecta-pymes-grandes-empresas-argentinas_0_73JfZR8VLr.html

Cámara de Representantes. (25 de 07 de 2023). *https://www.camara.gov.co/*. Obtenido de Agencia Nacional de Seguridad Digital y Asuntos: https://www.camara.gov.co/agencia-nacional-de-seguridad-digital-y-asuntos-espaciales

Cardash, S., Cilluffo, F., & Ottis, R. (22 de 08 de 2013). *Estonia's Cyber Defence League: A Model for the.* Obtenido de tandfonline.com: https://www.tandfonline.com/doi/abs/10.1080/1057610X.2013.813273

Centro Cibernético Policial. (11 de 2023). *Balance Cibercriminalidad*. Obtenido de https://caivirtual.policia.gov.co/sites/default/files/observatorio/Bolet%C3%ADn%20Centro%20Cibern%C3%A9tico%20Semana%2048%20de%202023.pdf

Chismon, D., & Ruks, M. (2015). *Threat Intelligence: Collecting, Analysing, Evaluating.* (M. InfoSecurity, Ed.) Obtenido de https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf

CIA, C. (2001). *The Intelligence Cycle.* Obtenido de https://irp.fas.org/cia/product/facttell/intcycle.htm

Cisos. (02 de 2023). *Reportes de Industria.* Obtenido de cisos.co: https://cisos.co/reportes-de-industria

CNI, C. N. (2021). *El Ciclo de Inteligencia.* Obtenido de cni.es: https://www.cni.es/la-inteligencia

Colombia, C. d. (2022). *Centro de Capacidades para la ciberseguridad de Colombia.* Obtenido de https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.4793144

Congreso de la República. (05 de 01 de 2009). *Ley 1273 de 2009*. Obtenido de secretariasenado.gov.co: http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CONPES. (s.f.). *Consejo Nacional de Política Económica y Social de Colombia.* Obtenido de Cepal.org: https://observatorioplanificacion.cepal.org/es/instituciones/consejo-nacional-de-politica-economica-y-social-conpes-de-colombia

Dahj, J. N. (04 de 2022). *Mastering Cyber Intelligence* (1 ed.). Birmingham: Packt Publishing. Recuperado el 27 de 03 de 2023

DANE. (15 de 08 de 2023). *En el segundo trimestre de 2023 el producto interno bruto de Colombia crece 0,3%.* Obtenido de dane.gov.co: https://www.dane.gov.co/files/operaciones/PIB/cp-PIB-IItrim2023.pdf

de Melo e Silva, A., de Oliveira Albuquerque, R., García Villalba, L. J., & Costa Gondim, J. J. (23 de 06 de 2020). A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence. *Future Internet, 12*(6). doi:10.3390/fi12060108

Departamento Administrativo de Presidencia. (8 de 03 de 2022). *Decreto 338 del 2022*. Obtenido de dapre.presidencia.gov.co: https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20338%20DEL%208%20DE%20MARZO%20DE%202022.pdf

Departamento Nacional de Planeación. (14 de 07 de 2011). *Lineamientos De Política Para Ciberseguridad Y Ciberdefensa.* Obtenido de colaboracion.dnp.gov.co: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Departamento Nacional de Planeación. (11 de 04 de 2016). Obtenido de CONPES 3854: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación. (01 de 07 de 2020). *CONPES 3995.* Obtenido de colaboracion.dnp.gov.co: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Díaz Acevedo, M., & Cremades Guisado, Á. (07 de 2023). La evolución de la estrategia de ciberseguridad de Colombia 2011-2021. (U. Nebrija, Ed.) *https://www.researchgate.net/*, 48. doi:10.13140/RG.2.2.22241.58723

Directiva Presidencial 02. (24 de 02 de 2022). *Directiva Presidencial N° 02 de 2022*. Obtenido de dapre.presidencia.gov.co:

https://dapre.presidencia.gov.co/normativa/normativa/DIRECTIVA%20PRESIDENCIAL%2002%20DEL%2024%20DE%20FEBRERO%20DE%202022.pdf

El Colombiano. (15 de 12 de 2022). *Ciberataque a EPM empieza a afectar a usuarios de servicios prepago de luz y agua*. Obtenido de https://www.elcolombiano.com/antioquia/ciberataque-a-epm-dejo-sin-agua-y-luz-a-usuarios-de-servicios-prepago-BN19634225

ENISA. (2019). ENISA Threat Landscape Report 2018. (L. Marinos, & M. Lourenço, Edits.) doi:DOI 10.2824/622757

ENISA. (2022). *ENISA Threat Landscape 2022.* European Union Agency for Cybersecurity. doi:10.2824/764318

FBI, F. (s.f.). *Active Collaboration.* Obtenido de https://www.fbi.gov/image-repository/intelligence-cycle-graphic.jpg/image_view_fullscreen

Federación de Científicos de América. (1 de 03 de 1996). *Preparing for the 21st Century.* Obtenido de https://irp.fas.org/offdocs/report.html

Federal Bureau Of Investigation. (02 de 08 de 2017). *Intelligence Branch.* Obtenido de FBI: https://www.fbi.gov/about/leadership-and-structure/intelligence-branch

Fiduagraria. (23 de 05 de 2023). *Comunicado Oficial*. Obtenido de fiduagraria.gov.co: https://www.fiduagraria.gov.co/index.php/nuestra-compania/noticias/comunicado-oficial.html

First. (2015). *Methods and Methodology.* Obtenido de https://www.first.org/global/sigs/cti/curriculum/methods-methodology

FIRST. (s.f.). *Methods and Methodology.* Obtenido de first.org: https://www.first.org/global/sigs/cti/curriculum/methods-methodology

Función Pública. (18 de 10 de 2012). *Ley 1581*. Obtenido de funcionpublica.gov.co: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Función Pública. (17 de 04 de 2013). *Ley 1621*. Obtenido de funcionpublica.gov.co: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706

Función Pública. (08 de 03 de 2022). *Decreto 338 de 2022*. Obtenido de Ministerio de Tecnologías de la Información Comunicaciones: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Función pública. (16 de 05 de 2022). *Decreto 767 de 2022*. Obtenido de https://www.funcionpublica.gov.co/: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186766

Función Pública. (14 de 11 de 2023). Obtenido de https://www.funcionpublica.gov.co/web/sie/entidades-del-estado

Gao, Y., Li, X., Peng, H., Fang, B., & Yu, P. (1 de 02 de 2022). HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. *IEEE Transactions on Knowledge and Data Engineering, 34*(2), 708-722. doi:10.1109/TKDE.2020.2987019

García R., J. (23 de 03 de 2023). *https://www.eltiempo.com/*. Obtenido de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/tumbaron-agencia-de-ciberseguridad-del-plan-nacional-de-desarrollo-752893

García, C. (27 de 03 de 2023). *Publican miles de documentos robados al Sistema Integrado de Emergencias y Seguridad de Medellín*. Obtenido de

Muchohacker.lol: https://muchohacker.lol/2023/03/publican-miles-de-documentos-robados-al-sistema-integrado-de-emergencias-y-seguridad-de-medellin/
García, Camilo Andrés. (26 de 05 de 2023). *Fiduagraria, nueva víctima de Lockbit en Colombia*. Obtenido de muchohacker.lol: https://muchohacker.lol/2023/05/fiduagraria-nueva-victima-de-lockbit-en-colombia/
García, Camilo Andrés. (23 de 01 de 2023). *Sacan a la venta lo que serían 25 millones de datos que podrían pertenecer a usuarios del Sisbén*. Obtenido de Muchohacker.lol: https://muchohacker.lol/2023/01/sacan-a-la-venta-lo-que-serian-25-millones-de-datos-que-podrian-pertenecer-a-usuarios-del-sisben/
Gobierno Digital. (2023). Obtenido de https://gobiernodigital.mintic.gov.co/
Gobierno Digital. (2023). *Política de Gobierno Digital.* Obtenido de gobiernodigital.mintic.gov.co: https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/
Hernández-Sampieri, R., & Mendoza-Torres, C. P. (2018). *Metodología de la investigación Las rutas cuantitativa, cualitativa y mixta* (Vol. 10). México, México: Mc Graw Hill Education.
Hodigital. (03 de 2019). *Cyber Threat Intelligence in Government: A Guide for Decision Makers and Analysts.* Obtenido de Home Office Digital, Data and Technology: https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf
IFXNetworks. (18 de 09 de 2023). *Comunicado de Prensa Oficial IFX Networks N°2*. Obtenido de https://ifxnetworks.com: https://ifxnetworks.com/embed/
Inteligencia, C. N. (2021). *El Ciclo de Inteligencia*. Obtenido de https://www.cni.es/la-inteligencia
International Business Machines. (07 de 2023). *Cost of a Data Breach Report 2023*. Obtenido de https://www.ibm.com/downloads/cas/E3G5JMBP
Jasper, S. (2017). U.S. Cyber Threat Intelligence Sharing Frameworks. *Taylor \& Francis Group, LLC*. doi:http://dx.doi.org/10.1080/08850607.2016.1230701
Koloveas, P., Chantzios, T., Alevizopoulou, S., Skiadopoulos, S., & Tryfonopoulos, C. (30 de 03 de 2021). inTIME: A Machine Learning-Based Framework for Gathering and Leveraging Web Data to Cyber-Threat Intelligence. *Electronics, 10*(7), 34. doi:https://doi.org/10.3390/electronics10070818
Lesme Díaz, L. (07 de 06 de 2023). *Colombia destinará $ 10.000 millones a la creación de un centro de ciberseguridad*. Obtenido de eltiempo.com: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-tendra-centro-ciberseguridad-segun-mauricio-lizcano-mintic-775700
Ley 1273. (05 de 01 de 2009). *Congreso de la República*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
Ley Estatutaria 1621 de 2013. (s.f.). Obtenido de Ley 1621 de 2013 - Gestor Normativo: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706
Loishyn, A., Hohoniants, S., Tkach, M., Tyshchenko, M., Tarasenko, N., & Kyvliuk, V. (27 de 08 de 2021). *Development of the Concept of Cybersecurity of the Organization.* Obtenido de www.temjournal.com: https://www.temjournal.com/content/103/TEMJournalAugust2021_1447_1453.pdf
Lumu Technologies. (2022). *Alerta para organizaciones colombianas: Cómo enfrentar la dura realidad del estado de ransomware en el país*. Obtenido de lumu.io:

https://lumu.io/wp-content/uploads/2022/12/lumu-alerta-para-organizaciones-colombianas.pdf

Marinos, L., & Lourenco, M. (01 de 2018). ENISA Threat Landscape 2018. doi:10.2824/967192

Martínez Viqueira, L. (2016). El Ciclo de Inteligencia Complejo. 625 - 639. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=5998270

Meli Tsofou, C. (17 de 07 de 2020). *Cyber Threat Intelligence: A Proposal of a Threat Intelligence Cycle from an Enterprise perspective.* Tesis Master, Erasmus Mundus. Obtenido de Departamento de Estudios de Seguridad. Universidad Charles, Facultad de Ciencias Sociales: https://dspace.cuni.cz/bitstream/handle/20.500.11956/177249/120368692.pdf?sequence=1

Minambiente, M. (19 de 06 de 2013). *Ley 1672*. Obtenido de Gestión Integral de Residuos de Aparatos Eléctricos y Electrónicos – RAEE: https://www.minambiente.gov.co/wp-content/uploads/2021/06/ley-1672-2013.pdf

MinTic. (octubre de 2021). *Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas.* Obtenido de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237907_maestro_mspi.pdf

MINTIC. (10 de 03 de 2021). *Resolución 00500*. Obtenido de Ministerio de Tecnologías de la Información y las Comunicaciones: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

MinTIC. (11 de 03 de 2022). *Resolución N° 000746.* Obtenido de mintic.gov.co: https://www.mintic.gov.co/portal/715/articles-208143_recurso_1.pdf

MinTIC. (07 de 06 de 2023). *“Manizales será la capital mundial de la ciberseguridad”: Mauricio Lizcano, Ministro TIC*. Obtenido de mintic.gov.co: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/276750:Manizales-sera-la-capital-mundial-de-la-ciberseguridad-Mauricio-Lizcano-Ministro-TIC

MinTIC. (16 de 08 de 2023). *abre 200.000 cupos para formación digital especializada con empresas líderes en tecnología*. Obtenido de mintic.gov.co: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/277584:MinTIC-abre-200-000-cupos-para-formacion-digital-especializada-con-empresas-lideres-en-tecnologia

MinTIC. (19 de 05 de 2023). *MinTIC anunció $1.500 millones para el centro BIOS*. Obtenido de mintic.gov.co: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/276286:MinTIC-anuncio-1-500-millones-para-el-centro-BIOS

MINTIC, M. (06 de 11 de 2016). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.* Obtenido de mintic.gov.co: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

MinTIC. (26 de 06 de 2023). *Google, MinTIC y Colnodo entregarán 4.000 becas para apoyar la formación en ciberseguridad de jóvenes en Colombia*. Obtenido de mintic.gov.co: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/276647:Google-MinTIC-y-Colnodo-entregaran-4-000-becas-para-apoyar-la-formacion-en-ciberseguridad-de-jovenes-en-Colombia

MIPG - Función Pública;. (2022). *Resultados Medición del Desempeño Institucional 2022* . Obtenido de funcionpublica.gov.co: https://www.funcionpublica.gov.co/web/mipg/resultados-medicion

Mouthón, L. (2022). *Ciberataque al Invima afecta al comercio exterior*. Obtenido de https://www.elheraldo.co/economia/ciberataque-al-invima-afecta-al-comercio-exterior-888540

Mucho Hacker. (08 de 03 de 2023). *Ataque a Mintic: Habrían vulnerado entidad que tiene a su cargo la ciberseguridad del país*. Obtenido de muchohacker.lol: https://muchohacker.lol/2023/03/ataque-a-mintic-habrian-vulnerado-entidad-que-tiene-a-su-cargo-la-ciberseguridad-del-pais/

Nan, S., Ming, D., Jiaojiao, J., Weikang, X., Xiaoxing, M., Yonghang, T., & Jun, Z. (2023). Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Communications Surveys & Tutorials, 25*(3), 1748-1774. doi:10.1109/COMST.2023.3273282

Nato Standard. (02 de 2016). *Allied Joint Doctrine For Intelligence, Counterintelligence And Security.* (N. S. (NSO), Ed.) Obtenido de https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP2.pdf

Nava Chan, A. (2022). *El ciberespacio como nueva expresión de poder en las relaciones internacionales: el caso del ciberataque NotPetya a Ucrania en 2017.* Tesis de Licenciatura, Benemérita Universidad Autónoma de Puebla, México. doi:https://hdl.handle.net/20.500.12371/18383

NCSI, N. (2022). *Índice Nacional de Seguridad Cibernética en Colombia*. Obtenido de ncsi.ega.ee: https://ncsi.ega.ee/country/co/

NIST. (16 de 03 de 2017). *El Instituto Nacional de Estándares y Tecnología*. Obtenido de https://nvd.nist.gov/vuln/detail/CVE-2017-0144

North Atlantic Treaty Organization. (22 de 06 de 2023). *Joint Intelligence, Surveillance and Reconnaissance*. Obtenido de https://www.nato.int/cps/en/natohq/topics_111830.htm

Nsit. (10 de 01 de 2022). *10 reconocidas instituciones de Colombia hackeadas en el 2022*. Obtenido de https://www.nsit.com.co/10-reconocidas-instituciones-de-colombia-hackeadas-en-el-2022/

OCDE. (2015). *Gestión de riesgos de seguridad digital para la prosperidad económica y social.* La Organización para la Cooperación y el Desarrollo Económicos. doi:10.1787/9789264245471-en

Oosthoek, K., & Doerr, C. (14 de 07 de 2020). Cyber Threat Intelligence: A Product Without a Process? *International Journal of Intelligence and CounterIntelligence, 34*(2), 300-315. doi:https://doi.org/10.1080/08850607.2020.1780062

Phythian, M. (2013). *Understanding the Intelligence Cycle.* Usa. Obtenido de https://www.defence.lk/upload/ebooks/Mark%20Phythian-Understanding%20the%20Intelligence%20Cycle-Routledge%20(2013).pdf

Planeación, D. N. (06 de 02 de 2023). *Bases del Plan Nacional de Desarrollo 2022 - 2026.* Obtenido de senado.gov.co: https://senado.gov.co/index.php/documentos/senado-prensa/6893-2023-02-06-bases-pnd-2023/file

Planque, D. (2017). *Cyber Threat Intelligence From confusion to clarity; An investigation into Cyber Threat Intelligence.* Tesis de máster ejecutivo, Universidad Leiden ,

Gobernanza y Asuntos Globales. Recuperado el 27 de 03 de 2023, de https://studenttheses.universiteitleiden.nl/handle/1887/64551

Portafolio. (01 de 11 de 2022). *Persiste la inconformidad de los gremios por la reforma tributaria*. Obtenido de portafolio.co: https://www.portafolio.co/economia/reforma-tributaria/reforma-tributaria-gremios-siguen-inconformes-con-el-proyecto-573472

Portafolio. (16 de 09 de 2023). Obtenido de Servicios que siguen funcionando a pesar de ciberataque a IFX Networks: https://www.portafolio.co/tecnologia/ciberataque-a-ifx-networks-servicios-que-siguen-funcionando-en-las-entidades-del-estado-de-colombia-589123

Redpacket Security. (27 de 03 de 2023). *Medusa Locker Ransomware Victim: Fiduagraria*. Obtenido de redpacketsecurity.com.

Sakib, S. (2022). *Cyber Threat Intelligence.* Bangladesh. doi:10.31224/2289

Schaberreiter, T., Kupfersberger, V., Rantos, K., Spyros, A., Papanikolaou, A., Ilioudis, C., & Quirchmayr, G. (26 de 08 de 2019). ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security. *Association for Computing Machinery*(83), Pages 1–10. doi:https://doi.org/10.1145/3339252.3342112

Schlette, D., Caselli, M., & Pernul, G. (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *IEEE Communications Surveys & Tutorials, 23*(4), 2525-2556. doi:10.1109/COMST.2021.3117338

Secretaría de Seguridad y Convivencia. (02 de 02 de 2023). *Twitter.com*. Obtenido de https://twitter.com/seguridadmed/status/1621143433577644038

Semana. (02 de 04 de 2023). *Los detalles secretos del grave hackeo que sufrió la Universidad Nacional*. Obtenido de https://www.semana.com/: https://www.semana.com/nacion/articulo/asi-fue-el-hackeo-del-que-fue-victima-la-universidad-nacional/202335/

Semana. (15 de 08 de 2023). *“Es necesario cuidar la economía y sus empresas”: la alerta de José Manuel Restrepo, exministro de Hacienda*. Obtenido de semana.com: https://www.semana.com/economia/macroeconomia/articulo/es-necesario-cuidar-la-economia-y-sus-empresas-la-alerta-de-jose-manuel-restrepo-exministro-de-hacienda/202337/

Senado de la República. (23 de 05 de 2023). *https://leyes.senado.gov.co/*. Obtenido de Por medio de la cual se crea la Agencia Nacional de Seguridad Digital y de dictan otras disposiciones: https://leyes.senado.gov.co/proyectos/index.php/proyectos-ley/cuatrenio-2022-2026/2022-2023/article/346-por-medio-de-la-cual-se-crea-la-agencia-nacional-de-seguridad-digital-y-se-dictan-otras-disposiciones

Skopik, F. (2018). *Collaborative Cyber hreat Intelligence* (1 ed.). New York: Auerbach Publications. doi:https://doi.org/10.4324/9781315397900

Soto Setzke, D., Riasanow, T., Böhm, M., & Krcmar, H. (12 de 03 de 2021). Pathways to Digital Service Innovation: The Role of Digital Transformation Strategies in Established Organizations. *Springer*, 21. doi:https://doi.org/10.1007/s10796-021-10112-0

Strom, B., Andy, A., Miller, D., Nickels, K., Pennington, A., & Thomas, C. (03 de 2020). *MITRE ATT&CK: Design and Philosophy.* Obtenido de attack.mitre.org: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Sülü, M., & Daş, R. (07 de 2022). Graph Visualization of Cyber Threat Intelligence Data for Analysis of Cyber Attacks. *Balkan Journal of Electrical & Computer Engineering, 10*(3), 300 - 305. Recuperado el 27 de 03 de 2023

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (05 de 05 de 2023). Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. *IEEE Communications Surveys & Tutorials, 25*(3), 1748-1774. doi:10.1109/COMST.2023.3273282

Ta-Seen, J. (2023). *ISO 27001: Information Security Management Systems.* Tesis. doi:10.13140/RG.2.2.36267.52005

Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (16 de 01 de 2021). *A review of threat modelling approaches for APT-style attacks.* Obtenido de cell.com: https://www.cell.com/heliyon/fulltext/S2405-8440(21)00074-8?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2405844021000748%3Fshowall%3Dtrue#%20

TicTac. (11 de 2022). *Ciberseguridad en redes de telecomunicaciones móviles.* Obtenido de ccit.org.co: https://www.ccit.org.co/wp-content/uploads/ciberseguridad-en-redes-de-tel-2022-2.pdf

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *computers & security, 72*, 212-233. Obtenido de https://www.sciencedirect.com/science/article/pii/S0167404817301839

Villalón Huerta, A., Ripoll Ripoll, I., & Marco Gisbert, H. (29 de 01 de 2022). Key Requirements for the Detection and Sharing of Behavioral Indicators of Compromise. *Electronics, 11*(3), 416. doi:https://doi.org/10.3390/electronics11030416

Virustotal. (2023). *virustotal*. Obtenido de https://www.virustotal.com/

Wagner, T., Mahbub, K., Palomar, E., & Abdallah, A. (06 de 08 de 2019). *Cyber threat intelligence sharing: Survey and research directions.* Obtenido de sciencedirect.com: https://www.sciencedirect.com/science/article/pii/S016740481830467X?via%3Dihub

WIPO, W. (2022). *Global Innovation Index 2022 : What is the Future of Innovation-driven Growth?* (15th edition. ed.). (S. Dutta, B. Lanvin, L. Rivera León, & S. Wunsch-Vincent, Edits.) Geneva, Switzerland. doi:https://doi.org/10.34667/tind.46596

A. Anexo. Encuesta

NIVEL DE APROPIACIÓN DEL CTI

La presente encuesta tiene como fin fundamental identificar el nivel de apropiación del CTI (Inteligencia de amenazas cibernéticas) en entidades gubernamentales de Colombia. La información suministrada será usada con fines académicos en un trabajo de grado de la Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos de la Universidad EAN.

1	**Totalmente en desacuerdo**
2	**En desacuerdo**
3	**Ni de acuerdo, ni en desacuerdo**
4	**De acuerdo**
5	**Totalmente de acuerdo**

1. Tipo de entidad en la que labora:
    - Entidad del estado del orden Nacional
    - Entidad del estado del orden Territorial
    - Sector Privado
2. ¿Conoce el concepto de CTI?
    - Totalmente en desacuerdo
    - En desacuerdo
    - Ni de acuerdo, ni en desacuerdo
    - De acuerdo
    - Totalmente de acuerdo
3. ¿Actualmente la entidad hace uso de recursos CTI?
    - Totalmente en desacuerdo

- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- Totalmente de acuerdo

4. ¿Qué tipos de recursos CTI usan en la entidad?
    a. Consulta en fuentes abiertas
    b. De un proveedor de servicios
    c. Otros ¿Cuáles?
    d. Ninguno
5. Si la anterior pregunta fue Otros, mencione ¿Cuáles?
6. ¿Con qué frecuencia se revisan las actualizaciones de los recursos de CTI?
    a. Diariamente
    b. Semanalmente
    c. Mensualmente
    d. Nunca
7. ¿Qué información obtiene de los recursos de CTI?
    a. Reportes, noticias o similares
    b. Información de vulnerabilidades
    c. Indicadores de compromiso
    d. Otros ¿Cuáles?
    e. Ninguno
8. Si la anterior pregunta su respuesta fue Otros, menciones ¿Cuáles?
9. ¿Cuál es la utilidad del CTI?
    a. Conocimiento general para evitar eventos, incidentes o la materialización de riesgos cibernéticos
    b. Modelamiento de amenazas

c. Informes a la alta gerencia

d. Ninguno

10. Teniendo en cuenta la pregunta anterior, ¿Cuál es el uso que se le da a la información de inteligencia de amenazas?

    a. Uso de nivel táctico

    b. Uso de nivel operativo

    c. Uso de nivel estratégico

    d. Uso en todos los niveles

    e. Ninguno

11. ¿Cómo obtiene la información de los recursos CTI?

    a. Vía correo

    b. Actualizaciones automáticas en las herramientas de seguridad

    c. Recursos en línea

    d. Otros (¿Cuáles?)

    e. Ninguno

12. Si la anterior pregunta su respuesta fue Otros, mencione ¿Cuáles?

13. Cuando se pública información de interés de CTI asociado a otros ciberataques, ¿hace uso de este recurso?

    - Totalmente en desacuerdo
    - En desacuerdo
    - Ni de acuerdo, ni en desacuerdo
    - De acuerdo
    - Totalmente de acuerdo

14. ¿Qué tipo de CTI puede ser útil para la entidad?
    a. Reportes de vulnerabilidades
    b. Indicadores de compromiso
    c. Metodologías de ataques
    d. Otros (¿Cuáles?)
    e. Ninguno
15. Si la anterior pregunta su respuesta fue Otros, mencione ¿Cuáles?
16. ¿Cuenta con la capacidad de producir información de CTI?
    - Totalmente en desacuerdo
    - En desacuerdo
    - Ni de acuerdo, ni en desacuerdo
    - De acuerdo
    - Totalmente de acuerdo
17. ¿Tiene personal capacitado en CTI?
    - Totalmente en desacuerdo
    - En desacuerdo
    - Ni de acuerdo, ni en desacuerdo
    - De acuerdo
    - Totalmente de acuerdo
18. ¿Considera que una estrategia de CTI puede ayudar a anticipar la ocurrencia de eventos, incidentes o materialización de riesgos cibernéticos en las entidades gubernamentales?
    - Totalmente en desacuerdo
    - En desacuerdo
    - Ni de acuerdo, ni en desacuerdo
    - De acuerdo

- Totalmente de acuerdo

19. ¿Considera que se tiene una base adecuada de conocimiento sobre CTI en la entidad?
    - Totalmente en desacuerdo
    - En desacuerdo
    - Ni de acuerdo, ni en desacuerdo
    - De acuerdo
    - Totalmente de acuerdo
20. ¿Cuenta con las herramientas de seguridad suficientes para hacer uso de CTI?
    - Totalmente en desacuerdo
    - En desacuerdo
    - Ni de acuerdo, ni en desacuerdo
    - De acuerdo
    - Totalmente de acuerdo
21. ¿Han ocurrido eventos, incidentes o materialización de riesgos cibernéticos en su entidad?
    - Sí
    - No
    - Desconoce sobre incidentes ocurridos en la entidad
22. Si su respuesta anterior fue si, mencione cuales:
    - Phishing
    - Ransomware
    - Malware
    - Fuga de datos

- Explotación de vulnerabilidades
- Otros

La encuesta de **NIVEL DE APROPIACIÓN DEL CTI**, puede ser verificada en el siguiente enlace: https://forms.office.com/r/VVDJPKEjf8?origin=lprLink

B. Anexo. Entrevista

NIVEL DE APROPIACIÓN DEL CTI EN EXPERTOS

La presente entrevista tiene como fin fundamental identificar el nivel de apropiación del CTI (Inteligencia de amenazas cibernéticas) en entidades gubernamentales de Colombia. La información suministrada será usa con fines académicos en un trabajo de grado de la Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos de la Universidad EAN.

1. Tipo de entidad en la que labora:
    - Entidad del estado del orden Nacional
    - Entidad del estado del orden Territorial
    - Sector Privado
2. Nombre, entidad en la que labora y funciones que desempeña o ha desempeñado en el ámbito de la ciberseguridad en las entidades gubernamentales de Colombia.
3. ¿Considera que las políticas gubernamentales para salvaguardar la confidencialidad, integridad y disponibilidad de la información en las entidades del sector gobierno son suficientes? Justifique la respuesta.
4. Ante la ocurrencia de diversos eventos, incidentes o la materialización de riesgos cibernéticos (delitos informáticos) ocurridos en diferentes entidades, ¿considera que se desplegaron las acciones necesarias para evitar que dichos eventos ocurran nuevamente en otras dependencias del sector?
5. ¿Conoce el término CTI? ¿considera que su aplicación puede ayudar a la anticipación de eventos, incidentes o la materialización de riesgos cibernéticos

(delitos informáticos) en las entidades del sector gobierno? Justifique su respuesta.

6. ¿Cree que por medio de una estrategia CTI se puede impactar favorablemente la salvaguarda de la información, al obtener información privilegiada de primer nivel que permita la anticipación de eventos, incidentes o la materialización de riesgos cibernéticos (delitos informáticos)?
7. ¿Considera que el conocimiento de CTI en el sector dedicado a la seguridad de la información en el país es amplio o, por el contrario, los controles en la actualidad se enfocan en respuestas reactivas y no anticipativas?
8. Si en algún momento llegara información de CTI del entorno colombiano, ¿estaría dispuesto a aplicarla en las herramientas de seguridad informática de su organización?
9. Con base en las infraestructuras actuales de TI, ¿considera que una estrategia de CTI puede ayudar a fortalecer la ciberseguridad de las entidades?
10. ¿Considera que las entidades tienen una buena gestión de infraestructura para aplicar CTI?
11. ¿Cree que la información con la que cuenta actualmente el Estado colombiano para proteger sus infraestructuras tecnológicas (críticas) ante la materialización de riesgos cibernéticos es suficiente y tiene buenos estándares de calidad?
12. ¿Considera relevante para la definición, implementación, puesta en marcha y seguimiento de una estrategia de CTI, la entidad que debería estar a cargo de esta? Elija cual sería la entidad más idónea y porqué (Presidencia - DAPRE, Mintic-Colcert, Agencia Nacional de Seguridad - ANSD, Mindefensa, Otra).
13. ¿Autoriza que la información suministrada en el presente formulario pueda ser usada en la tesis de grado?
    - Sí

- No

La encuesta de **NIVEL DE APROPIACIÓN DEL CTI EXPERTOS**, puede ser verificada en el siguiente enlace: https://forms.office.com/r/fym1iq3xvC?origin=lprLink