Gestión de Riesgos de Seguridad de la Información en Proyectos de Tercerización de Servicios y Soluciones de TI

Rafael Alonso Salamanca Álvarez

Universidad EAN

Facultad de Ingeniería

Programa: Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Bogotá, Colombia

2025

Gestión de Riesgos de Seguridad de la Información en Proyectos de Tercerización de Servicios y Soluciones de TI

Rafael Alonso Salamanca Álvarez

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

Magister en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Director (a):

William Fajardo Moreno, PhD

Modalidad:

Monografía

Universidad EAN

Facultad de Ingeniería

Programa: Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Bogotá, Colombia

2025

Nota de aceptación:

Firma del jurado

Firma del jurado

Firma del director del trabajo de grado

Ciudad, día/mes/año

Resumen

Temática: Estado actual de las buenas prácticas de seguridad de la información que las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, aplican en los proyectos que ejecutan.

Antecedentes: El aumento de la tercerización de proyectos TI , junto con el aumento de las brechas de información, resaltan la importancia de conocer acerca de cómo las compañías de outsourcing de servicios y soluciones TI gestionan los riesgos de brechas de seguridad como parte de su oferta de valor para proteger los activos de la información de sus clientes y favorecer que sus proyectos finalicen de manera exitosa.

Objetivo: Analizar las estrategias implementadas por las compañías de outsourcing de servicios y soluciones TI en Bogotá, Colombia, para dar tratamiento a los riesgos de Seguridad de la información en la gestión de proyectos de servicios y soluciones de TI**.**

Metodología: Se utilizó un enfoque interpretativo o cualitativo, basado en un instrumento debidamente validado para la recolección de datos. La población incluye empresas de outsourcing de servicios y Soluciones TI de Bogotá, Colombia, que reportaron ingresos durante 2022, según el Sistema de Integrado de Información Societaria – SIIS de la Superintendencia de Sociedades. La muestra estuvo compuesta por 22 de estas empresas, seleccionadas bajo la técnica no probabilística por conveniencia.

Resultados: La implementación de buenas prácticas de seguridad de la información que garanticen la confidencialidad, integridad y disponibilidad de los activos de información de los clientes en los proyectos outsourcing de servicios y soluciones TI no es un estándar de industria que caracterice este sector TI**.**

Conclusiones: Aunque algunas compañías adoptan estrategias adecuadas para gestionar los riesgos de brechas de seguridad en los proyectos que ejecutan, esto no es

un factor competitivo que la mayoría de las empresas de este sector apliquen de forma generalizada. La adopción de buenas prácticas de seguridad de la información en proyectos de tercerización de servicios y soluciones TI representa la excepción más que la norma en la protección de los activos de información valiosos para sus clientes.

Palabras clave: Outsourcing de TI, Gestión de Proyectos, tercerización de servicios TI, tercerización de soluciones de TI**,** seguridad de la Información,

Abstract

Topic: Current state of best practices in information security employed by IT Services and Solutions Outsourcing companies in Bogotá, Colombia, in the projects they execute.

Background: The increase in IT project outsourcing, along with the rise in information breaches, highlights the importance of understanding how IT services and solutions outsourcing companies manage security breach risks as part of their value proposition to protect the information assets of their clients and ensure the successful completion of their projects.

Objective: To analyze the strategies implemented by IT services and solutions outsourcing companies in Bogotá, Colombia, to address information security risks in the management of IT services and solutions projects.

Methodology: An interpretive or qualitative approach was used, based on a duly validated instrument for data collection. The population includes IT Services and Solutions Outsourcing companies in Bogotá, Colombia, that reported revenues during 2022, according to the Integrated Societal Information System (SIIS) of the Superintendence of Companies. The sample consisted of 22 of these companies, selected using the non-probabilistic convenience sampling technique.

Main results: The implementation of best practices in information security that ensure the confidentiality, integrity, and availability of clients information assets in IT Services and Solutions Outsourcing projects is not an industry standard characterizing this IT sector.

Conclusions: Although some companies adopt adequate strategies to manage security breach risks in the projects they execute, this is not a competitive factor that most companies in this sector generally apply. The adoption of best practices in information security in IT services and solutions outsourcing projects represents the exception rather than the norm in protecting valuable information assets for their clients.

Keywords: IT outsourcing, project management, IT services outsourcing, IT solutions outsourcing, Information Security

Tabla de Contenidos

Lista de Figuras

Lista de Tablas

1. Introducción

La práctica en la que una empresa emplea a otra organización para realizar parte de su trabajo, en lugar de utilizar a sus propios empleados para realizarlo, es conocida en el mundo de los negocios por la palabra inglesa *outsourcing* y en español como tercerización. En general, la tercerización es una estrategia que las grandes corporaciones norteamericanas iniciaron al principio de los años sesenta del siglo XX subcontratando funciones no medulares para la organización con el objetivo principal de ahorrar costes de personal y administrativos y ha evolucionado para dedicar recursos y conocimiento a aquellas actividades claves y convertirse en un modelo de negocio que deliberadamente desarrolla una cadena de suministro global basada en personal especializado y tecnología avanzada para incrementar la productividad, eficiencia, efectividad y satisfacción de los clientes y consumidores hasta el punto en el que hoy día las compañías de todos los tamaños y sectores tercerizan aquellas funciones y procesos que son vitales para su desarrollo, posicionamiento e, incluso, continuidad en el mercado que sirven, impulsando con esto el desarrollo del sector económico de los servicios. (Charles M. & Benson O. 2023).

La estrategia de tercerizar funciones y procesos clave de las compañías que buscan aprovechar al máximo sus recursos disponibles para crear una organización eficiente y altamente especializada, también ha sido utilizada para el área encargada de la Gestión de las Tecnologías de la Información y Comunicaciones – TICs, convirtiéndose en una práctica de negocio común conocida a nivel mundial bajo la etiqueta de ITO - IT Outsourcing (Tercerización de TI). En su compilación de definiciones y explicaciones de términos relacionados con las TICs, Gartner, empresa consultora y de investigación de las tecnologías de la información a nivel mundial, con sede en Stamford (Connecticut,

Estados Unidos), precisa que la tercerización de TI es el uso de proveedores de servicios de aplicaciones y soluciones de infraestructura para soportar los procesos de negocio de una empresa con el fin de obtener resultados de manera más efectiva pues les permite a las organizaciones contratantes reducir costos, acelerar el tiempo de comercialización y aprovechar la experiencia, los activos y/o la propiedad intelectual de un proveedor externo de soluciones y servicios TI (Gartner. s/f. Definición IT Outsourcing).

A medida que las TICs se convierten en habilitador del negocio bien sea por las amenazas u oportunidades que plantea para las organizaciones tradicionales o bien sea porque la organización nace como un modelo empresarial basado en TICs, la estrategia de tercerizar la gestión y operación de las TICs igualmente gana terreno, pues permite a las organizaciones centrarse en sus competencias principales e impulsar la transformación e innovación digital tan necesaria para los negocios en el entorno económico actual. De acuerdo con Grand View Research, compañía dedicada a la consultoría e investigación de mercados con sede en San Francisco EEUU, en el 2022 el tamaño del mercado mundial de tercerización de servicios relacionados con la gestión de las TICs se valoró en 639,59 mil millones de dólares y se espera que crezca a una tasa anual compuesta del 8,0% hasta el 2030 impulsada por la creciente demanda global de servicios y soluciones enfocados en la gestión de las operaciones de las TICs, en proyectos relacionados con la formulación y optimización de estrategias de TI, en consultoría relacionada con arquitectura empresarial, y en la gobernanza del portafolio de iniciativas relacionados con transformación digital (Grand View Research.2023).

Las tendencias mundiales relacionadas con el desarrollo de la tercerización de servicios y soluciones TICs no son ajenas al entorno colombiano. La Federación Colombiana de la Industria del Software y Tecnologías Informáticas Relacionadas - Fedesoft, organización gremial de las empresas relacionadas con la industria del

software nacional, establece que la estrategia empresarial de tercerizar procesos y funciones de TI, inicia en el país a mediados de los años noventa del siglo XX con un enfoque inicial en la contratación de servicios básicos de soporte técnico y administración de la operación y de infraestructura TI (Fedesoft 2019). Hoy día, en Colombia, el mercado de la tercerización de funciones y procesos de negocio ha evolucionado de manera significativa y distingue tres grandes líneas de servicios: (i) BPO - Business Process Outsourcing, que agrupa los Centros de Servicio (Contact Center and Back Office), los Centros de Servicios Compartidos (GBS-Global Business Services and Service Desk), los servicios relacionados con finanzas, los servicios relacionados con contabilidad y los servicios relacionados con recursos humanos, entre otros; (ii) ITO - Information Technology Outsourcing, en el que se clasifican los servicios relacionados con la gestión y suministro de software, servicios relacionados con la administración y provisión de Centros de Datos (data centers), infraestructura y servicios de nube (cloud); y (iii) KPO - Knowledge Process Outsourcing (KPO) que integra los servicios de telemedicina, investigación de mercados, análisis de información, servicios de educación en línea, entre otros. (Colombia Productiva. 2023).

Debido principalmente al avance y desarrollo acelerado de TICs y su impacto y uso por parte de organizaciones colombianas de todos los tamaños y en todos los sectores económicos, impacto que impulsa la transformación digital, la arquitectura empresarial y a la cada vez mayor necesidad de gobernar de manera efectiva las operaciones de las TICs, de manera creciente, más compañías colombianas recurren a la estrategia de la tercerización de sus áreas y procesos relacionados con las TICs, convirtiéndola en una práctica de negocio actual y común, identificada en el mercado colombiano como tercerización de servicios y soluciones de TI. Las compañías especializadas en proyectos y servicios de TI en Colombia se clasifican en el sector TIC de la economía colombiana,

sector que consolida las actividades económicas relacionadas con las TICs: Manufactura TI, Infraestructura TI, Comercio TI, Telecomunicaciones, Servicios TI y Contenido y media (DANE, 2021).

El sector TIC de Colombia, en su conjunto, muestra una tendencia de crecimiento positivo sostenido en su participación en el PIB del país. De acuerdo con cifras del DANE, este sector registró en 2021 un valor agregado de $18,1 billones y un crecimiento del 26,4%; en 2022, el valor agregado fue de $47,9 billones de pesos y el crecimiento fue del 16,4% con respecto a 2021; y en 2023, su aporte al PIB fue de $49,7 billones de pesos, lo que representa un crecimiento del 3,8% con respecto a 2022. El mercado de los servicios TI participa activamente en estas cifras. Específicamente, el valor agregado de los servicios TI en 2023 fue de $29,3 billones, lo que mostró un crecimiento del 32,8% con respecto al año anterior (DANE, 2024).

La tercerización de sus áreas y procesos relacionados con las TICs explica en gran parte el crecimiento del aporte de valor agregado de los servicios TI el PIB en Colombia. En el país se ha consolidado la tercerización de servicios y soluciones TI como un modelo de negocio, donde compañías especializadas se comprometen a responder por la administración, operación, soporte, mantenimiento, actualización y evolución de los sistemas de información según las necesidades de las organizaciones que las contratan bajo un esquema de proyecto. Esto permite que estas organizaciones contratantes reduzcan costos, aceleren el tiempo de posicionamiento de sus productos y/o servicios en el mercado y aprovechen la experiencia externa, junto con los activos y/o propiedad intelectual relacionada con las TIC de sus contratistas, aportando a su vez al crecimiento y fortalecimiento de la economía del país, como lo demuestran las cifras del Departamento Administrativo Nacional de Estadística (DANE) anteriormente señaladas.

La literatura académica relacionada con el ITO ciertamente recomienda el modelo de negocio de la tercerización de servicios y soluciones TI como una excelente estrategia gerencial madura para desarrollar proyectos relacionados con las TICs dentro de los límites presupuestales, el alcance definido y la calidad requerida sin gastar ni comprometer una cantidad excesiva de recursos de las empresas contratantes, sin embargo, tanto académicos como profesionales involucrados en el gerenciamiento de tales proyectos, advierten que es una maniobra compleja desde el punto de vista de la empresa contratada y que el fracaso de proyectos ITO es muy común, pues aun cuando el 94% de las compañías FORTUNE 500 han tercerizado una función clave de negocio, en el caso de los proyectos relacionados con Sistema de Información y Tecnologías de la Información (IS/IT - Information Systems and Information Technology) los análisis sugieren que al menos uno de cada tres proyectos se consideró un fracaso y muchos proyectos se retrasaron, excedieron el presupuesto y no pudieron cumplir con sus objetivos predefinidos.(Shahzada B. y Otros. 2023).

Uno de los factores que influyen en el fracaso de proyectos ITO tiene que ver con la gestión de la seguridad de la información, tema que debería ser de preocupación no solo de las compañías contratantes sino también de las compañías proveedores y de sus gerentes de proyecto. De acuerdo con un estudio realizado por Yong Wu, investigador académico de la Escuela de Gestión de Ingeniería de la Universidad Donghua en Shangai, China, la filtración de datos mostró un crecimiento explosivo a nivel mundial en el 2020, con más registros filtrados en sólo 12 meses que el total de los últimos 15 años y el análisis de esos eventos de fuga de información, ha permitido identificar la tendencia de que las empresas sean atacadas a través de sus proveedores externos, reiterando que no se debería pasar por alto la desventaja de los riesgos de seguridad de la información en los proyectos ITO (Yong W.& Otros. 2024).

Al implementar una estrategia ITO, la organización contratante facilita que la compañía especializada en proyectos de servicios y soluciones de TI tenga acceso, casi irrestricto, a prácticamente toda su información. En esencia, la tercerización de soluciones y servicios TI supone que el contratante confía en un proveedor externo no solo la gestión y soporte de sus activos tecnológicos, sino que también admite el manejo de sus activos de datos comerciales y de negocio específicos de su organización generados, capturados, procesados y almacenados en esos activos tecnológicos que son administrados por ese tercero. (Piattini M. & Ruiz F. 2021).

En el entorno digital actual, los datos y la información se han convertido en uno de los activos más importantes de las organizaciones, llevando incluso a ser registrados como intangibles en los informes contables de las compañías (Corrado & Otros. 2022) y muchos analistas financieros, contadores, empresarios y académicos coinciden en señalar la necesidad de que las empresas gestionen los datos y la información de la misma manera como gestionarían un activo estratégico organizacional, señalando que, en el caso de los datos y la información, esta gestión incluye la obligación y el coste asociado con su protección y prevención respecto a lase brechas de ciberseguridad. (Collins & Lanz. 2019).

Los activos de datos e información, como cualquier activo organizacional, al verse afectados ya sea por un evento intencional o de descuido, facilitado por la propia organización o por un tercero, eventos conocidos como brechas de seguridad, pueden causar daños económicos muy grandes. Kaspersky (s.f.), compañía internacional dedicada a la seguridad informática con presencia en aproximadamente 195 países del mundo, afirma que una brecha de seguridad puede llegar a costarle a una empresa cuatro millones de dólares, cifra que se estima sobre los datos propios de la compañía. Esta cifra prácticamente coincide con el informe anual publicado en 2020, del Ponemon

Institute en asociación con IBM (s.f.), que realizó un análisis cuantitativo de 524 brechas en 17 geografías y 17 industrias, y estableció que el costo total promedio de una brecha de seguridad de datos es de USD 3,86 millones, señalando que Estados Unidos es el país con mayor valor promedio en costos por brechas de seguridad, USD 8,64 millones (siendo la industria de la Salud la que presenta mayor valor: USD 7,13 millones) e indicando que el tiempo promedio para que una compañía identifique y detenga una brecha de seguridad de la información es de 280 días.

Ante el hecho de que las brechas de seguridad de la información pueden ser un factor que impacta negativamente el éxito de un proyecto ITO y en vista de los costos y tiempo que implica el tratamiento de tales brechas, las empresas proveedores de soluciones y servicios de TI deben asegurarse de aplicar los más altos estándares de seguridad y no exponer la información y/o datos de sus clientes. El INCIBE (Instituto Nacional de Ciberseguridad de España) – (s/f)., empresa pública establecida por el gobierno español para dar soporte en materia de seguridad informática a los ciudadanos, empresas públicas y privadas, así como a las administraciones públicas y sus organismos, y a las instituciones académicas y de investigación del país ibérico, señala que la adecuada protección de los datos y la correcta salvaguarda de la privacidad e integridad de la información, se han convertido en prioridades tanto para las organizaciones como para los consumidores como resultado de la transformación digital y el comercio electrónico y que establecer medidas de seguridad robustas es fundamental para proteger los intereses de los propietarios de negocios y la confianza de sus clientes.

El presente trabajo de investigación tiene como tema el estudio de las estrategias implementadas por las compañías de Outsourcing en Bogotá, Colombia, para dar tratamiento a los riesgos de Seguridad de la información en la gestión de proyectos de Servicios y Soluciones TI y evitar o minimizar los eventos o brechas de seguridad que

afectan los activos de información entregados por sus clientes en la administración, operación, soporte, mantenimiento, actualización y evolución de los sistemas de información y tecnologías de la información.

Para llevar a cabo el estudio de la situación de las estrategias implementadas por las compañías de Outsourcing Servicios y Soluciones TI en Bogotá, Colombia, para dar tratamiento a los riesgos de Seguridad de la información en la gestión de proyectos, se realizó una revisión de la literatura y documentos institucionales para conocer el estado actual del enfoque a este respecto y se aplicó una encuesta a Gerentes de Proyectos de estas compañías.

Este documento registra los resultados del estudio y contiene los siguientes 10 (diez) capítulos:

- Capítulo 1. Introducción: Establece el marco de referencia de la investigación e incluye el tema y contextualización de la investigación, el planteamiento del problema, la formulación de la pregunta de investigación y la estructura del documento.
- Capítulo 2. Objetivos: Define el alcance y la metodología apropiada para responder la pregunta de investigación. Incluye el objetivo general o la meta global de la investigación y sus objetivos específicos.
- Capítulo 3. Justificación: Corresponde al planteamiento de las razones que señalan la relevancia, utilidad y viabilidad de la investigación.
- Capítulo 4. Marco teórico: Reseña los antecedentes, teorías, modelos, otras investigaciones y conceptos que fundamentan el estudio, a partir de la revisión bibliográfica.

- Capítulo 5. Hipótesis: Presenta la explicación posible que da respuesta tentativa a la pregunta de investigación y de los resultados esperados en el desarrollo de este trabajo.
- Capítulo 6. Categorías de análisis: Describe las variables definidas para llevar a cabo las mediciones correspondientes y necesarias para desarrollar los objetivos establecidos y comprobar la hipótesis planteada.
- Capítulo 7. Metodología: Se refiere al enfoque de la investigación, el alcance, las fases que permiten alcanzar cada uno de los objetivos planteados, la población y muestra, los instrumentos y su validación, procedimientos y técnicas aplicadas para recoger y analizar la información.
- Capítulo 8. Trabajo de campo: Describe la labor de investigación realizada, los datos recolectados, el procesamiento de los datos y su presentación en los gráficos de resultados.
- Capítulo 9. Discusión: Presenta la interpretación y análisis de resultados, destacando los principales hallazgos del estudio, su significado y sus limitaciones.
- Capítulo 10. Conclusiones y Trabajo Futuro: Sintetiza los resultados alcanzados, los objetivos correspondientes y las hipótesis comprobadas. Sugiere las investigaciones que se podrían plantear a partir de esta investigación.

1.1. Tema de Investigación.

De acuerdo con las líneas de investigación establecidas por la EAN y considerando el tema de estudio, la presente investigación se clasifica dentro del campo de Emprendimiento y Gerencia y se ubica en el grupo de Dirección & Gestión de Proyectos (EAN, 2022), guardando una relación directa con la Maestría en Sistemas de Información

y Proyectos Tecnológicos, debido a que en su desarrollo se revisaron modelos, metodologías y sistemas de gestión de la seguridad de la información para la gerencia de proyectos de soluciones y servicios TI tercerizados.

1.2. Planteamiento del problema.

En Latinoamérica, la encuesta sobre tendencias de ciber-riesgos y seguridad de la información de Deloitte (2016) que incluyó a 89 empresas de 13 países y 7 industrias entre ellas las Tecnologías de la Información y Comunicaciones, concluyó que 4 de cada 10 empresas sufrieron una brecha de seguridad en los últimos 24 meses. El ESET Security Report (2019), que incluye datos recolectados de empresas de diferentes tamaños (el 30% de más de 1000 empleados y un 15% de por lo menos 500 empleados, con una participación del 50% de PyMEs), de más de 10 tipos de industrias (entidades de gobierno (20%), productos y servicios de tecnología (15%), banca y finanzas (12%), educación (9%) y salud (5%), distribuidas en 13 países de la región (Colombia (18%), Argentina (15%), Guatemala (12%), México (10%) y Chile (10%)) concluye que el 61% de las empresas sufrió por lo menos un incidente de seguridad y que la mitad de estos incidentes está relacionada con el secuestro de información sensible, es decir, que por lo menos 1 de cada 10 empresas encuestadas en toda Latinoamérica sufrió el secuestro de su información y que además, un 20% de las empresas latinoamericanas fueron afectadas por incidentes de acceso indebido a la información y un 15% fue afectada por ataques de Ingeniería Social, que es la mala práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.

En el caso de Colombia, la XX Encuesta Nacional de Seguridad Informática de Almanza A. & Cano J. (2020), patrocinada por Seguridad Informática, capítulo Colombia, soportada por la Asociación Colombiana de Ingeniero de Sistemas (ACIS), en la cual

participaron 254 encuestados distribuidos en 13 diferentes sectores de la economía, muestra entre el top de hallazgos principales que uno de los aspectos de seguridad de la información que más preocupa al 52% de los participantes es el relacionado con la fuga de información y revela que la principal preocupación del 64% los directivos de TI es la por la falta de capital intelectual para enfrentar los retos de seguridad de la información.

Una de las conclusiones generales de esta encuesta es que la tendencia en materia de incidentes de seguridad en Colombia se mantiene en línea con las tendencias internacionales, de manera que, en este sentido, los errores humanos, el engaño al usuario para robarle información confidencial y en general los ataques de ingeniería social son las principales técnicas para afectar la confidencialidad de la información. En cuanto a costos, los encuestados manifiestan que sus incidentes cuestan menos de $US 50.000, cerca del 13% entre $US 50.000 y $US 100.000, el 10% manifiesta que le cuesta más de $US 150.000 y el resto manifiesta que está en la franja de los $US 100.001 hasta los $US 150.000 dólares. Claramente, debido al tamaño de las empresas y de la economía colombiana estas cifras son representativas.

El término tercerización o subcontratación de servicios y soluciones de TI fue creado en 1980 para describir la creciente tendencia de compañías que estaban transfiriendo tareas operativas relacionadas con sus sistemas de información a proveedores externos como una maniobra estratégica para reducir y controlar costos, obtener acceso a nueva tecnología y/o mejorar el enfoque de la empresa. En la actualidad, es raro encontrar proyectos relacionados con las tecnologías de la información y telecomunicaciones (TICs) de una empresa que se definan y ejecuten utilizando únicamente recursos internos de una compañía. Lo normal hoy día es encontrar que las áreas de gestión de la TICs de una entidad están conformadas por equipos de trabajo tanto internos como externos que utilizan recursos y componentes tecnológicos tanto propios como

alquilados. La tercerización de servicios y soluciones TI es una opción tanto estratégica, como táctica y operativa que utilizan las empresas para gestionar sus sistemas de información y proyectos tecnológicos para lograr ventajas competitivas. (Toro F. 2012).

Aun cuando desde el punto de vista de negocio es atractivo tercerizar los servicios y soluciones de TI por los beneficios que ofrece, la empresa contratante debe tener cuidado de no exponerse a riesgos que puedan poner en evidencia información clave o enfrentar la no disponibilidad de información necesaria para el desarrollo de su actividad y que afecten negativamente misionalidad de la compañía al permitir que competidores puedan sacar ventaja de tal situación. En efecto, la tercerización de servicios y soluciones de TI, además de beneficios, como característica principal puede incrementar el riesgo de pérdida de datos e indisponibilidad de activos de información de la empresa contratante, pues existe la posibilidad de que los estándares éticos y los procedimientos de la compañía subcontratada no sean tan buenos como ella afirma. La filtración de información y/o los incidentes relacionados con seguridad de la información generados por proveedores de servicios y soluciones TI tienen grandes consecuencias en la operación normal del negocio de los clientes y los costos asociados pueden fácilmente superar cualquier ahorro que se derive del contrato de tercerización (Hope J. & Player S. 2012).

Clasificados bajo la categoría de Incidentes de Seguridad de la Cadena de Suministros (INCIBE, 2024) en 2023 se registró un marcado aumento en los ataques a proveedores externos para infiltrarse entre sus clientes. Algunos de los casos más significativos son:

- SolarWinds Corporation, compañía de Austin, Texas, Estados unidos que provee software para sistemas e infraestructura TI implican miles de empresas a nivel mundial demuestra la escala del daño posible a través de las

vulnerabilidades de la cadena de suministro. En este caso a través de este proveedor los atacantes pudieron robar datos, implementar códigos maliciosos o interrumpir la actividad empresarial de agencias gubernamentales en Estados Unidos y corporaciones privadas a nivel mundial. (Cyber Chief Magazine. 2025)

- Las explotaciones de MOVEit y MOVEit Cloud, software para la transferencia seguras de datos y archivos confidenciales, de la empresa Ipswitch Inc, parte de Progress Software, empresa con sede en Burlington, Massachusetts, Estados Unidos, es otro de los casos significativos del 2023. Los atacantes explotaron estas soluciones de gestión e intercambio de archivos para robar datos comerciales confidenciales de más de 500 organizaciones, exponiendo la información personal de más de 34,5 millones de personas. (Cyber Chief Magazine. 2025)
- En septiembre de 2023 un caso que llamó bastante la atención en Colombia por su gran impacto fue el ataque cibernético de ransomware (secuestro digital de información y aplicaciones), que sufrió el proveedor de servicios IFX Network que suministra servicios en tecnología y transferencia de datos y que afectó negativamente a 762 de sus clientes. En Colombia fueron 20 entidades públicas y 78 privadas (Mintic. 2023) que no pudieron operar u operaron de manera parcial por aproximadamente dos semanas.

A continuación, se muestra una representación gráfica del análisis situacional utilizando la técnica de árbol de problemas, con la situación o problema identificado (cuadro de color rojo), por qué está ocurriendo (las causas en los cuadros de color amarillo) y que es lo que esto está ocasionando (los efectos o consecuencias en los cuadros de color azul):

Ilustración 1 - Análisis situacional o árbol del problema

Fuente: Elaboración propia

No hay visibilidad de un registro centralizado de brechas de seguridad en Colombia, ni control ni seguimiento consolidado debido, principalmente, a los aspectos relativos a la reputación de la empresa que sufre un ciberataque y, por lo tanto, no hay datos específicos a mundial, regional, nacional, o a nivel local, que permitan relacionar a las compañías del sector del outsourcing de Servicios y Soluciones TI en Colombia con brechas de seguridad de manera y su comportamiento frente a ellas. Sin embargo, el Boletín Técnico del DANE (Departamento Administrativo Nacional de Estadística) y el MinTIC (Ministerio de las Tecnologías de la Información y las Comunicaciones del 2022 titulado Encuesta de Tecnologías de la Información y las Comunicaciones en Empresas – (ENTIC Empresas) que encuestó a un total de 21.630 empresas de los subsectores de industria (6.328 empresas), comercio (8.936 empresas) y servicios (6.366 empresas) del

país con el fin de conocer información estadística sobre transformación digital, la preparación del sector productivo colombiano para la IA, la capacitación de talento humano de las empresas en la inserción y en el aprovechamiento de las oportunidades y retos que conlleva la 4RI (Cuarta Revolución Industrial) para contribuir con la Política Nacional para la Transformación Digital e Inteligencia Artificial CONPES 3975 de 2019, encontró que 7.419 de las 21.630 empresas (34.30%) habían encargado externamente la implementación de TICs, siendo 3.579 empresas del sector comercio (40.1%), 2.136 empresas del sector industrial (33.8) y 1.704 empresas del sector servicios (26.8%). Este mismo Boletín Técnico reporte que 979 empresas (13.2%) de las 21.630 sufrieron incidentes de seguridad digital relacionados con la suplantación de identidad de clientes y proveedores, siendo 266 empresas del sector industrial (4.2%), 411 del sector comercio (4.6%) y 302 del sector servicios (4.8%). (DANE y MinTIC. 2022).

Frente este panorama conviene conocer las estrategias claves implementadas por las compañías de outsourcing de Servicios y Soluciones TI colombianas para gestionar los riesgos de brechas de seguridad como parte de su oferta de valor, si los gerentes de proyectos de outsourcing de Servicios y Soluciones TI protegen de manera adecuada los activos de información que tienen valor de negocio tanto para el proveedor de los servicios y soluciones de TI como para sus clientes, si los gerentes de proyectos de outsourcing de Servicios y Soluciones TI consideran la gestión de riesgos de seguridad como una de sus áreas de interés para aplicar y si gerentes de proyectos de outsourcing de Servicios y Soluciones TI están preparados para gestionar los riesgos de seguridad de la información.

1.3. Pregunta de investigación.

La pregunta central de esta investigación es: ¿Las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, consideran estrategias adecuadas para gestionar los riesgos de brechas de seguridad como parte de su oferta de valor? y su objetivo principal, es entonces, determinar cuál es la situación de las estrategias implementadas por las compañías de Outsourcing Servicios y Soluciones TI en Bogotá, Colombia, para dar tratamiento a los riesgos de Seguridad de la información en la gestión de proyectos.

2. Objetivos

El objetivo general y los objetivos específicos que orientan el propósito de la investigación son:

2.1. Objetivo general

Analizar las estrategias implementadas por las compañías de outsourcing de Servicios y Soluciones TI en Bogotá, Colombia, para dar tratamiento a los riesgos de Seguridad de la información en la gestión de proyectos de servicios y soluciones de TI.

2.2. Objetivos específicos

- Identificar cómo las compañías de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia protegen los activos de información que tienen valor de negocio para sus clientes en la ejecución de sus proyectos.
- Determinar cuál es el enfoque metodológico que aplican las compañías de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, para la gestión de riesgos de seguridad en sus proyectos.
- Establecer la manera cómo las compañías de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia preparan a sus gerentes de proyectos en la gestión de los riesgos de seguridad de la información.
- Plantear recomendaciones para aportar en el fortalecimiento y mejora de la gestión de los riesgos de seguridad sobre los activos de información utilizados y/o entregados por un cliente a un proveedor de servicios TI en el campo de los proyectos de tercerización de proyectos y soluciones de TI.

3. Justificación

En el escenario actual del ITO en Colombia, es indiscutible la aceptación de la tercerización de servicios y soluciones de TI como una estrategia de apalancamiento en el mundo empresarial, impulsada por el rendimiento que aporta a las organizaciones. Sin embargo, como toda acción de negocio, esta estrategia conlleva aspectos relacionados con los posibles impactos negativos derivados de la gestión de los activos de información involucrados. Los proyectos de TI gestionan activos de información valiosos tanto para el proveedor como para sus clientes, y los riesgos de seguridad de la información asociados pueden materializarse —ya sea de manera accidental, por desconocimiento, negligencia o ataques directos— en filtraciones, manipulaciones o indisponibilidad de datos e información no deseadas. Siendo de por sí grave, en el contexto de la tercerización, esta situación se agudiza, ya que los datos y la información comprometida no pertenecen al proveedor, sino a sus clientes, quienes pueden ser entidades públicas o empresas privadas.

En la práctica, los clientes que deciden emprender proyectos de tercerización de servicios y soluciones TI enfrentan incertidumbre en la administración de los riesgos de sus activos de información por parte de terceros, puesto que una inadecuada gestión de tales riesgos puede generar eventos inesperados y consecuencias negativas. A pesar de la relevancia de esta problemática, los marcos de trabajo y estándares reconocidos en el mercado de TI, relacionados con la gestión de proyectos, no tratan sobre buenas prácticas para abordar los riesgos de seguridad de la información en este tipo de proyectos, existen pocos estudios previos al respecto y hay escasez de información sobre las prácticas actuales de gestión de riesgos de seguridad en proyectos de tercerización en Colombia.

La presente investigación se justifica por el creciente aumento de los proyectos relacionados con la tercerización de servicios y soluciones TI y la importancia de la seguridad de la información como parte del aseguramiento de la cadena de suministro TICs. Es fundamental que los proveedores de servicios y soluciones de TI reconozcan el valor y las amenazas de los activos de información que reciben de sus clientes, y que garanticen la implementación de medidas de seguridad robustas que aseguren el éxito de sus proyectos y una mayor competitividad en el mercado actual a través de una adecuada gestión de riesgos de seguridad sobre los activos de información utilizados y/o entregados por un cliente a un proveedor de servicios y soluciones TI.

Para contribuir con el afianzamiento de la gestión de riesgos de seguridad sobre los activos de información utilizados y/o entregados por un cliente a un proveedor de servicios y soluciones TI, es necesario determinar el estado actual de las estrategias implementadas por las compañías de outsourcing de servicios y soluciones TI. Esto implica investigar cómo protegen los activos de información valiosos para sus clientes, identificar el enfoque metodológico que aplican y establecer cómo preparan a sus gerentes de proyectos para gestionar los riesgos de seguridad de la información en este tipo de proyectos.

Con base en los resultados obtenidos, se plantearán recomendaciones para fortalecer y mejorar la gestión de los riesgos de seguridad sobre los activos de información utilizados y/o entregados por un cliente a un proveedor de servicios TI en el campo de los proyectos de tercerización de servicios y soluciones TI, buscando beneficiar a las empresas y entidades clientes, los proveedores y a la sociedad en general.

El campo de investigación del presente estudio corresponde con Emprendimiento y Gerencia que se encuentra dentro del grupo de investigación de Dirección y Gestión de Proyectos. La línea de investigación está relacionada con Modelos, metodologías y

sistemas en gestión de proyectos pues el tema específico de investigación es el de la gestión de riesgos de seguridad de información en la gestión de proyectos de soluciones y servicios TI. (EAN, 2020).

Respecto a la posibilidad de llevar a cabo el trabajo esta investigación, en la tabla que se muestra continuación, se realizó un análisis cualitativo de los criterios básicos requeridos para su desarrollo:

Tabla 1 – Criterios de factibilidad del proyecto

Criterio	***Factibilidad (siendo 1 menor y 5 mayor)***
Acceso a la información	3
Apoyo e interés de colaboradores o aliados	3
Disponibilidad de recursos requeridos	5
Probabilidad de avance en el tiempo establecido	5
Probabilidad de continuidad o implementación de la propuesta de investigación	5
Promedio	21

Fuente: Plantilla anteproyecto monografía – Universidad EAN

Considerando que la máxima calificación posible es 25 puntos, el resultado de 21 demuestra que existió una alta probabilidad de llevar a cabo la investigación dentro de los limites su alcance, tiempo y costos para lograr los resultados con la calidad requerida.

La calificación con 3 puntos para los criterios de Acceso a la información y Apoyo e interés de los colaboradores aliados se debe a que al ser revisión documental y entrevistas a personal de los equipos de gerencia de proyectos de las compañías de outsourcing de servicios y soluciones TI, generalmente han firmado acuerdos de confidencialidad que solo permiten suministrar información clasificada como pública y que se puede utilizar para fines académicos. De esta manera, la principal limitación de esta investigación en general está relacionada con el acceso completo a las fuentes de información documental y a la falta de cooperación para suministrar información veraz y/o

completa por parte de los entrevistados toda vez que la gestión de seguridad de la información conoce de datos, prácticas y controles considerados sensibles tanto desde el punto de vista de los impactos económicos, como desde el punto de vista de imagen comercial y reputacional de las empresas estudiadas.

La calificación con 5 puntos de los criterios de Disponibilidad de recursos requeridos, Probabilidad de avance en el tiempo establecido y Probabilidad de continuidad o implementación de la propuesta de investigación, se debió a que están relacionados con los recursos técnicos, humanos y financieros a disponibilidad del investigador para aplicar de acuerdo con el avance y resultados parciales obtenidos.

4. Marco Teórico

El desarrollo conceptual que soporta la investigación, que se relaciona con su título y las relaciones entre los conceptos que se plantean es el siguiente:

Un activo de información es cualquier información que una organización valora y que si es perdido, robado, expuesto y/o compartido de manera inapropiada podría llegar a causar graves afectaciones a la organización dueña. Algunos de estas afectaciones son bien conocidas y se pueden encontrar bien documentados, tales como las afectaciones por reputación de la marca respecto a una brecha o fuga de información, multas por incumplimientos en los requerimientos regulatorios relacionados con la seguridad de la información y pago de rescates por secuestro de información sensible o crítica para el negocio. Otros impactos menos conocidos tienen que ver con las pérdidas por eficiencia operativa, pérdidas por retiro de clientes y pérdidas de ventajas competitivas (Wittkop, J. 2016).

Ejemplos de los activos de información que un proveedor de servicios y soluciones TI utiliza y/o recibe de un cliente para producir, entregar y dar soporte a sus proyectos son:

- Datos creados o utilizados por los procesos bien sea en medios digitales, papel y/o en otros medios como imágenes y videos.
- Hardware y software utilizado para el procesamiento, transporte y/o almacenamiento de datos y generación de información.
- Servicios subcontratados a terceros para la transmisión, recepción y/o control de datos e información.
- Plataformas, herramientas y utilidades para el desarrollo, pruebas, instalación, despliegue, soporte y mantenimiento de los sistemas de información.

- Equipos de trabajo, colaboradores y usuarios que manejen datos, información y/o conocimiento específico muy importante para la organización, como secretos industriales, know-how, manejo de información crítica relacionada con planes estratégicos, información de carácter personal asociada a salarios y números de identificación.

Los riesgos relacionados con estos activos de información tienen que ver con tres aspectos básicos (ISO.2018):

- Confidencialidad: Solo aquellos autorizados pueden tener acceso y uso controlado.
- Integridad: Solo aquellos autorizados pueden crear, leer, actualizar y/o borrar datos e información de manera controlada.
- Disponibilidad: La información puede ser accesada y usada en el momento en que se necesite.

En el caso de los proyectos de Servicios y Soluciones TI, muchos de estos activos de información son compartidos o entregados a un tercero debido al alcance de tal servicio o solución y si este tercero no los protege de manera adecuada, se pueden materializar los riesgos relacionados con su confidencialidad, integridad y disponibilidad, afectando negativamente a la organización cliente, situación que no es excepcional. Un estudio realizado en el 2021 por Proofpoint, empresa de ciberseguridad empresarial con sede en Sunnyvale, California, Estados Unidos y la CSA (Cloud Security Alliance) organización sin fines de lucro con sede en Seattle. Estados Unidos, dedicada a promover las mejores prácticas para brindar garantía de seguridad en los servicios de cloud computing (computación en la nube), concluye que aproximadamente el 58% de las empresas que optaron este tipo de servicios fueron afectadas por las brechas de seguridad de sus proveedores o terceros. Cabe señalar que el Cloud computing es la disponibilidad bajo

demanda de recursos de computación como servicios a través de Internet. Esta tecnología evita que las empresas tengan que encargarse de aprovisionar, configurar o gestionar los recursos y permite que paguen a un proveedor tercero únicamente por los recursos IT que usen. Se distinguen tres tipos de modelos de servicios cloud computing: IaaS (Infrastructure as a Service), infraestructura como servicio que ofrece servicios de procesamiento y almacenamiento; PaaS (Platform as a Service) plataforma como servicio que proporciona un entorno de desarrollo y despliegue para crear aplicaciones en la nube; y SaaS (Software as a Service) software como servicio que facilita aplicaciones como servicios. (Google Cloud. s/f).

Los proveedores externos se han convertido en el eslabón más débil de la cadena de suministro de proyectos de servicios y soluciones TI bajo el modelo de ITO. En el mundo global interconectado de hoy, las organizaciones, tanto del sector público como del privado, dependen de proveedores externos para satisfacer las necesidades de su cadena de suministro, ya sea para software, tecnología de la información, servicios, productos o componentes parciales de estos entregables. Esas mismas organizaciones públicas y privadas son proveedores de otras empresas, lo que da lugar a una cadena de suministro compleja, en donde una empresa pierde visibilidad de su cadena total de suministro y limita el control sobre ella, asumiendo los riesgos de seguridad conocidos y desconocidos de los proveedores, con la esperanza de que un enfoque de mercado pueda mejorar la gestión de los riesgos de seguridad en la cadena de suministro y mitigar estos riesgos de la subcontratación ITO (Harrack M. 2021).

PwC - PriceWaterhouseCoopers (2022), firma de servicios profesionales de auditoría, consultoría y asesoramiento legal y fiscal a las principales compañías, instituciones y gobiernos a nivel global y considerada una de la cuatro más grande del mundo en este campo, en su encuesta anual Digital Trust Survey 2022 encontró que tan sólo el 40% de

las compañías afirma conocer a fondo los riesgos de ciberseguridad y de privacidad asociados a sus proveedores terceros (IT third party providers); que el 60% de los entrevistados reconoce no tener un conocimiento profundo de las brechas de seguridad asociadas con estas terceras partes; y que el 20% asegura tener poco o ninguno conocimiento al respecto. Adicionalmente, el informe de PWC señala que menos de la mitad de las empresas encuestadas manifiestan haber abordado activamente las amenazas crecientes de ciberseguridad y privacidad relacionada con sus proveedores y que quienes sí lo han hecho, mitigan tales riesgos auditando o verificando el cumplimiento de sus proveedores (46%); compartiendo información con terceros o ayudándoles de alguna otra manera a mejorar su posición respecto a la ciberseguridad (42%) y abordando los retos relacionados con el coste o el tiempo de la resiliencia ante posibles eventos (40%).

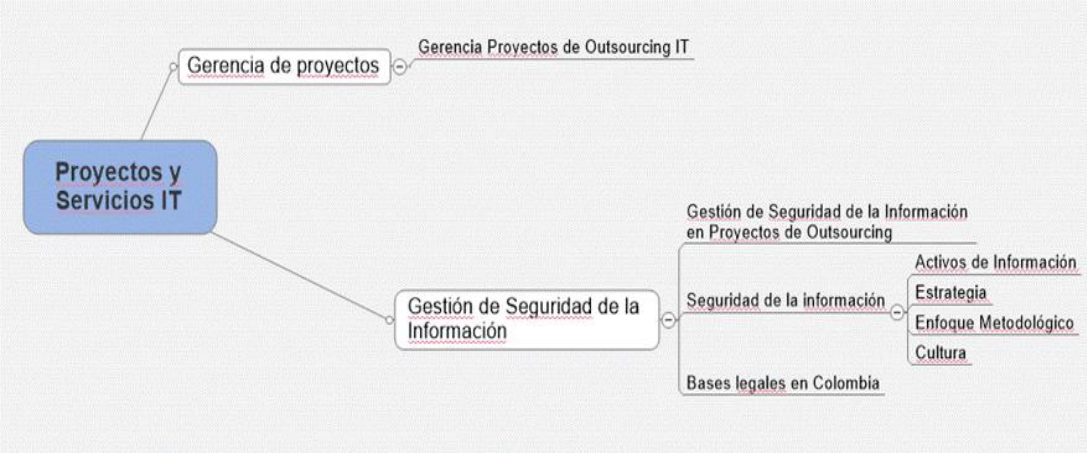
La materialización de riesgos relacionados con la seguridad de la información de los activos de información entregados por clientes a proveedores de proyectos de Servicios y Soluciones TI son incidentes bastante comunes. A nivel mundial, Kapersky (2022) señala que aproximadamente el 33% de las grandes organizaciones incluidas en el ranking Fortune Global 500 sufrieron brechas de seguridad que involucran datos compartidos con proveedores, cuyo impacto financiero ascendió a 1,4 millones de dólares, ligeramente superior al producido por la pérdida física de dispositivos propiedad de la empresa (1,3 millones de dólares), de los ataques de criptominería (1,3 millones de dólares) y el uso inapropiado de recursos de TI por parte de los empleados (1,3 millones).

La debida protección de los activos de información que un proveedor de Servicios y Soluciones TI utiliza y/o recibe de un cliente debería ser un objetivo de alta prioridad para impulsar la entrega exitosa de los beneficios y el valor de negocio de los proyectos que estas empresas se comprometen a realizar y en este contexto la Gerencia de

Proyectos como disciplina profesional que da guía práctica para la planeación y ejecución del trabajo del proyecto para lograr los resultados previstos es un factor crítico de éxito, y los Gerentes de Proyecto como responsables de la gestión y coordinación de los recursos disponibles con el fin de lograr las metas definidas para el proyecto se convierten en los garantes para alcanzar tal objetivo (PMI.2021).

Tal como lo sugiere el método del mapeo, se construyó el siguiente mapa conceptual que contiene los temas y palabras clave del estudio propuesto:

Ilustración 2 - Mapa conceptual del marco teórico



Fuente: Elaboración propia

A partir de este mapa conceptual se desarrolló la estructura del marco teórico en tres grandes capítulos: Antecedentes de la investigación, Bases teóricas y Bases legales de la Seguridad de la Información en Colombia. El capítulo de Bases teóricas a su vez se dividió en los subcapítulos Gerencia de Proyectos, Gerencia de proyectos de Outsourcing TI, Gestión de seguridad de la información y Gestión de Seguridad de la Información en proyectos de Outsourcing TI. El desarrollo de esta estructura se presenta a continuación:

4.1. Antecedentes de la investigación

El propósito de este capítulo es presentar una descripción de artículos de estudio y trabajos de investigación relacionados con la gestión de la seguridad de la información en general, y la gestión de proyectos en particular, organizados desde el más reciente hasta el menos reciente, indicando el autor, el año de la presentación, el título, el objetivo general y una síntesis de sus conclusiones.

Pang G. (2020), plantea que uno de los valores fundamentales del Marco de Referencia Agile, para la gestión de proyectos, es mantener incorporada la calidad. Esto implica que los controles de seguridad deberían, también, estar incrustados en la mentalidad Agile. Así mismo, Pang afirma que la seguridad de la información y la mentalidad Agile no siempre van de la mano en la implementación de este marco para el desarrollo de proyectos dentro de una empresa. Los equipos Agile a menudo consideran que la funcionalidad y el valor comercial son más críticos que el cumplimiento de la seguridad y es claro, entonces, que la madurez de la seguridad de la información y el cumplimento con el marco Agile no está bien alineados.

La conclusión de Pang es que, con la mentalidad adecuada y la voluntad de cambiar la forma en que se abordan la seguridad y los riesgos de TI en los proyectos Agile, será posible administrar la seguridad y los riesgos de TI en un entorno de desarrollo de software dinámico y de ritmo rápido. La adaptación de las prácticas de seguridad dentro del marco Agile permitirá al equipo gestionar el riesgo y equilibrar los requisitos de seguridad de acuerdo con las amenazas identificadas y las demandas de la sociedad.

Fister (2018), expone que las principales brechas de seguridad han generado nuevas regulaciones que a su vez generan una mayor atención de los proyectos relacionados con TI respecto a los temas de seguridad de la información y protección de datos personales. Sostiene que, en lugar de simplemente reaccionar a los nuevos requisitos de

las regulaciones y evitar posibles infracciones, lo que las organizaciones deberían hacer es cambiar a una postura de seguridad enfocada en proteger mejor los datos de los clientes, revisando los pasos en el proceso de planificación de proyectos para todas las iniciativas de TI y los conocimientos de seguridad a sus equipos, pues en la práctica se encuentra que muchos gerentes de proyecto no tienen la formación ni experiencia con la seguridad de la información y tampoco se están incorporando expertos en seguridad de la información a los equipos de proyecto.

Concluye que, en lugar de un enfoque reactivo, las organizaciones, los gerentes de proyecto y los equipos de proyecto deberían adoptar una postura de seguridad proactiva para proteger mejor los datos de los clientes bajo el enfoque de "seguridad por diseño" que forme parte del ciclo de vida del proyecto.

Van Der Heijden Amber, Broasca Cosmin y Serebrenik Alexander (2018), identificaron los desafíos de seguridad encontrados en el desarrollo de software bajo el marco de referencia Agile, a gran escala, desde la perspectiva de los profesionales involucrados en estos equipos de proyecto. Aplicando el método de desarrollo cooperativo para guiar un estudio de caso cualitativo en Rabobank, una organización bancaria multinacional holandesa, realizaron un total de diez entrevistas con miembros en diferentes roles de cinco equipos de desarrollo Agile diferentes. Los resultados muestran que los siguientes desafíos parecen ser exclusivos de Agile a gran escala: alineación de los objetivos de seguridad en un entorno distribuido, desarrollo de una comprensión común de los roles y responsabilidades en las actividades de seguridad, e integración de herramientas de pruebas de seguridad de bajo costo. Estos desafíos reportados parecen ser comunes a la seguridad en el desarrollo de software en general o coinciden con los desafíos reportados para el desarrollo ágil a pequeña escala. Concluyen que los hallazgos informados sugieren la presencia de múltiples desafíos de seguridad que no son

exclusivos de la metodología Agile a gran escala. Sugieren que el trabajo futuro debería centrarse en confirmar estos desafíos e investigar posibles mitigaciones.

Chinyamurindi (2017), realizó un estudio cuyo objetivo fue comprender los puntos de vista y las experiencias de los emprendedores de la industria de la construcción en Sudáfrica. El estudio adoptó un enfoque de investigación cualitativa utilizando entrevistas semiestructuradas para generar narrativas sobre dos temas particulares: (1) cómo se conceptualiza el éxito de la gestión de proyectos y (2) cuál es el papel que la gestión de la información desempeña en esto. Para este estudio se utilizó una muestra de 15 empresarios que trabajan en la industria de la construcción. A partir del análisis de las narrativas de los 15 emprendedores, el éxito de un proyecto se conceptualizó principalmente en torno a tres temas: 1.) el éxito del proyecto consistía en mantener contento al cliente, 2.) El éxito de los proyectos en la industria de la construcción significó cumplir con los objetivos establecidos, especialmente los de naturaleza financiera, y 3.) El éxito del proyecto consistió en canalizar sinergias internas para obtener beneficios externos. Además, los 15 encuestados plantearon un subtema principal en torno al papel de la gestión de la información como una de las bases del éxito del proyecto, estableciendo que es un tema generalmente aceptado o en uso en la toma de decisiones eficaz, sin embargo, ninguno planteó o se refirió al tema de la seguridad de la información y/o estrategias para proteger la información del proyecto.

Baraforta (2017), publicó un estudio cuyo objetivo es analizar las actividades de gestión de riesgos a través de varias normas ISO seleccionadas con el fin de proporcionar la base para mejorar, coordinar e interoperar las actividades de gestión de riesgos en entornos de TI para diversos fines relacionados con la gestión de calidad, gestión de proyectos, gestión de servicios de TI y gestión de seguridad de la información. El método utilizado tomó como base la norma internacional ISO 31000 para la gestión de

riesgos y realizó una comparación con el objetivo de identificar las actividades relacionadas con la gestión de riesgos en la estructura de alto nivel ISO para las normas del sistema de gestión, ISO 9001, ISO 21500, ISO / IEC 20000-1 e ISO / IEC 27001. Lo anterior a razón del gran interés que presentan estas normas para los profesionales en entornos de TI, que se benefician de la integración de actividades basadas en procesos, pero que a su vez ayudan a implementar mecanismos para vincular equipos de trabajo de TI y no TI de la organización, todos con desafíos de gestión de riesgos de seguridad de la información a abordar.

Como resultados se obtuvieron vectores de integración, como la comprensión de la organización y su contexto, el pensamiento basado en el riesgo, el liderazgo y el compromiso, el enfoque de procesos y la estructura PDCA.

Como conclusión proponen un modelo de proceso que integra las actividades de gestión de riesgos en lo modelos de gestión de calidad, gestión de proyectos, gestión de servicios de TI y gestión de seguridad de la información.

Neelov (2017), explica que el uso de la información en la vida diaria se ha vuelto esencial en el siglo XXI y que los proyectos son planeados y ejecutados con base en una abundancia de información que se ha acumulado desde antes del inicio del proyecto. Esta información, que se entrega al equipo al inicio del proyecto, junto a la que se genera durante la propia ejecución del proyecto, se convierten en parte integral de los activos de cualquier proyecto, ya sea la construcción de un condominio de gran altura, la construcción de un submarino nuclear, desarrollar una nueva aplicación, construir un nuevo hospital o fabricar un coche autónomo. Los activos de información del proyecto ayudan a desarrollar el producto, el servicio o el componente sofisticado por el cual el proyecto fue emprendido y es una gran responsabilidad del equipo de proyecto protegerlos del acceso no autorizado y no divulgarlos, sin embargo, el reporte de brechas

o incumplimientos en seguridad de la información a través de fuentes confiables como entidades de control, entidades académicas y/o reportes comerciales o noticiosos demuestran que muchos equipos de proyecto no lo están haciendo muy bien y que por el contrario muestra fallas en la protección de los datos e información que maneja el proyecto.

Concluye que, durante la planificación del proyecto, se debería analizar la exposición a los riesgos de seguridad de la información y se debería planificar para proteger la información como lo recomiendan algunas de las normas internacionales que definen esto como requisitos básicos: ISO 27001, ISO 27018, PCI, SSAE16 y CSA STAR y que son relevantes para las fases de inicio, planificación, ejecución, control y cierre del proyecto. Lamentablemente no siempre se hace de esa manera.

4.2. Bases teóricas

4.2.1. Gerencia de proyectos

Hurtado (2011), afirma que los proyectos son los instrumentos por excelencia para materializar la planeación estratégica empresarial al facilitar convertir las iniciativas de negocio que surgen de la planeación estratégica en productos, servicios y resultados que las áreas operativas pueden entrar a usar cotidianamente.

Seymour & Hussein (2014), afirman que los proyectos y su gestión han existido desde el principio de la humanidad, pero que, formalmente, se considera que la gerencia de proyectos inicia como disciplina con la aparición del Diagrama de Gantt, en 1917 y que es a mediados de 1950 con la metodología PERT (Program Evaluation and Review Technique) y CPM (Critical Path Method), que las organizaciones empiezan a aplicar sistemáticamente estas técnicas y herramientas para la gestión de sus proyectos.

A partir de Diagrama de Gantt, del PERT y del CPM se generan nuevas adaptaciones y modificaciones de técnicas de ingeniería y de administración de negocios que empiezan a ser consideradas como parte fundamental de la gerencia de proyectos. Temas relacionados con la gestión de costos, la gestión del personal del proyecto, gestión de la calidad entre otros, se empiezan a considerar buenas prácticas que los gerentes de proyecto deberían aplicar.

La idea de tener un marco de referencia de buenas prácticas que sirva como base para gerenciar proyectos se empieza a consolidar a través del Project Management Institute (PMI). De acuerdo con la página oficial del Project Management Institute, PMI (s/f), el PMI se fundó en 1969 por 40 voluntarios. Su primer seminario se celebró en Atlanta (Georgia, Estados Unidos), al cual acudieron más de ochenta personas. A finales de 1970, ya tenía alrededor de 2000 miembros. Hoy en día agrupa a más de que 500 000 miembros en casi 100 países y es considera la asociación más grande del mundo relacionada con la práctica de la gestión de proyectos.

El PMI actualiza y publica la Guía de los Fundamentos para la Dirección de Proyectos. Su séptima versión, la más actualizada, fue publicada en julio de 2021. Esta guía agrupa las buenas prácticas para lograr un gerenciamiento eficaz y eficiente de un proyecto. La guía del PMBOK describe 12 principios procesos de dirección de proyectos (Administración, equipo, interesados, valor, pensamiento sistémico, liderazgo, adaptación, calidad, complejidad, riesgo, adaptabilidad y capacidad de recuperación y cambio), 8 dominios de desempeño (Interesados, equipo, enfoque de desarrollo y ciclo de vida, planificación, trabajo del proyecto, entrega, medición, incertidumbre), una guía sobre la adaptación deliberada del enfoque, la gobernanza y los procesos de dirección del proyecto para que resultan más adecuados para el entorno y el trabajo a realizar y una descripción de los modelos, métodos y artefactos de uso común que los equipos de

proyecto pueden usar para producir entregables, organizar el trabajo y permitir la comunicación y colaboración.

Basada en la Guía de los Fundamentos para la Dirección de Proyectos, el PMI administra la certificación Project Management Professional (PMP) que es una certificación reconocida a nivel mundial, la cual valida la formación y experiencia de un experto en la gestión de proyectos. Esta credencial es otorgada a individuos quienes aprueban el examen PMP. Esta certificación es la más conocida y utilizada en Colombia tanto por los clientes como por los proveedores de servicios y soluciones de TI, siendo la más valorada y exigida en el mercado laboral colombiano para los cargos de gerente o director de proyectos.

En el actual entorno de los negocios se habla de los proyectos y de la gestión de proyectos como una forma de materializar estrategias que generen ventajas competitivas para la empresa, bien sea generando nuevos productos, servicios o procesos en una compañía.

De acuerdo con la Guía de los Fundamentos para la Dirección de Proyectos (2021), los proyectos, desde una perspectiva de negocio, impulsan el cambio en una organización: antes de iniciar el proyecto, la organización de define con un estado actual y se espera que al finalizar el proyecto la organización alcance un estado futuro que genera beneficios cuantificables netos que pueden ser tangibles, intangibles o de ambos tipos. Los proyectos son esfuerzos temporales que se llevan a cabo para crear un producto, servicio o resultado único y la gestión o administración de proyectos es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para poder entregar ese producto, servicio o resultado único dentro del marco de tiempo y con los recursos asignados.

Otro marco de referencia para la gestión de proyectos es Prince 2 (Project In Controled Enviroment, versión 2). De acuerdo con el sitio oficial, Axelos (s/f), PRINCE2 es una metodología de gestión de proyectos que desde 1989 se viene usando como un estándar para la gestión de proyectos principalmente en el Reino Unido y en Europa. Inicialmente desarrollada para proyectos TIC, la última versión, PRINCE2 se publicó el 16 de junio de 2009 y se generalizó para la gestión de todo tipo de proyectos.

PRINCE 2 considera 7 temas: la Calidad, el Cambio, la estructura de roles del proyecto (Organización), los planes (Cuánto, Cómo, Cuando), el Riesgo y el Progreso del proyecto, justificado por un Business Case (o necesidad del negocio). El gerente de proyecto deberá revisar estos temas durante el ciclo de vida del proyecto y justificar en todo momento el proyecto frente a la consecución de los beneficios esperados.

AXELOS, basado en PRINCE 2, otorga certificaciones en nivel de Fundamentos Practicante a aquellos profesionales que superan sus exámenes. Estas credenciales validan la educación y la experiencia de un experto en gestión de proyectos.

Desde el punto de vista de estándares internacionales para la gestión de proyectos, se identifican la norma ISO 21500 – Directrices para la Dirección y Gestión de Proyectos y la ISO 10006 de Sistemas de Gestión de la Calidad - Directrices para la Gestión de la Calidad en los Proyectos. A diferencia de las certificaciones PMP y PRINCE ya referenciadas, y como con todas las normas ISO, la 21500 y la 10006 están destinadas para las organizaciones y no para los individuos.

La norma ISO 21500 (ISO.2012) proporciona orientación sobre los conceptos y los procesos relacionados con la dirección y gestión de proyectos que son importantes para, y tienen impacto en el desempeño organizacional de los proyectos. Contiene recomendaciones sobre cómo una organización debería gestionar los procesos, los

tiempos de entrega, la gestión del riesgo o los niveles que hay que alcanzar en el proyecto.

La norma ISO 10006 (ISO.2017) se enfoca en orientar a las organizaciones sobre cómo gestionar la calidad en los procesos de gestión de sus proyectos y reconoce que los proyectos son el eje central del desarrollo de la estrategia de las organizaciones. Al ser tema estratégico, la norma recomienda que la Alta Dirección debe jugar un rol determinante en los proyectos más relevantes de la organización y debe ser consciente de su influencia en el éxito de los mismos con el fin de lograr los objetivos organizacionales propuestos.

4.2.2. Gerencia de proyectos de Outsourcing TI

De acuerdo con Miranda J. (2006), uno de los desarrollos más significativos en la práctica de la gestión de proyectos tiene que ver con el Outsourcing o tercerización. Específicamente en el campo de las Tecnologías de la Información y Comunicaciones, esta práctica nació a principios del 2000, con la idea de reducir los costos directos de los proyectos, subcontratando componentes que no afectan el producto, servicio o componente principal del proyecto, pero siempre conservando el control por parte del contratante. Esta práctica ha evolucionado y se utiliza tanto para componentes específicos, como para el proyecto completo y los servicios y/o soluciones involucradas. Es decir, los negocios entregan la totalidad de la gestión del proyecto a un tercero y participan como un miembro más del equipo de proyecto solo esperando el producto, servicio o componente comprometido.

Davidson (2005) recomienda que, al ser el outsourcing de proyectos una práctica común, para la tercerización la organización contratante y en especial el personal involucrado en los proyectos debería particularmente formarse en el manejo de contratos. Esto por cuanto, aclara, la violación de los términos y condiciones de un acuerdo interno

de la compañía, quizá, termine con un llamado de atención de un superior, pero esa misma violación, puede terminar en una corte judicial, situación que ninguno de los involucrados en un proyecto desea.

Aun cuando es una tendencia de negocios creciente, no todo lo relacionado con la tercerización es positivo. Whelen & Hunger (2007), destacan que el outsourcing de proyectos de servicios y soluciones de TI tiene sus lados negativos. Señalan entre los principales, la reducción de la capacidad de le empresa para aprender nuevas destrezas y desarrollar competencias centrales. Subrayan, además, que uno de los errores que las compañías que subcontratan proyectos de servicios y soluciones de TI deben evitar es seleccionar al proveedor equivocado, en otras palabras, contratar proveedores no confiables. En su caso proponen, entonces, fortalecer las habilidades organizacionales relacionadas con la gestión de proveedores por parte de las empresas que contratan.

Gartner en su definición del modelo Bimodal IT, distingue entre el modelo de gestión TI orientado a sistemas que deben estar centrados en la estabilidad y la eficiencia y el modelo ágil centrado en la evolución rápida de aplicaciones y la alineación estrecha con las unidades de negocio (Gartner.s/f. Definición Bimodal). Ambos modelos coexisten en las compañías, lo que dificulta la gestión en muchas empresas. Refieren que, en este escenario, es el outsourcing de servicios y soluciones de TI la principal herramienta con la que cuentan las organizaciones para superar esta limitación y lograr beneficios relacionados con la eficiencia operacional y de transformación organizacional. Sin embargo, Gartner alerta que las organizaciones no suelen aplicar un sólido proceso de gestión de riesgos cuando seleccionan por primera vez a un proveedor para la prestación de servicios y proyectos y recomiendan que las organizaciones deben incluso monitorizar y revisar las publicaciones de la prensa de la industria, los sitios de comercio del gobierno, los comentarios en Internet e incluso consultar las embajadas en busca de

signos de problemas inminentes y relacionados con los proveedores de servicios y soluciones TI.

Gartner (s/f) igualmente recomienda usar su Cuadrante Mágico (Magic Quadrant) como uno de los primeros pasos para identificar proveedores de tecnologías relacionadas con la información y comunicación específicas. El cuadrante mágico de Gartner ofrece a los compradores de TICs una evaluación comparativa del rendimiento de los proveedores a través de un gráfico de matriz de dos ejes, con el eje vertical representando el conocimiento de mercado y el eje horizontal indicando la habilidad de ejecución, dando como resultado cuatro tipos de proveedores: Proveedores Líderes, Proveedores Visionarios, Proveedores jugadores de nicho y Proveedores retadores o aspirantes. Advierte Gartner que centrarse en los proveedores líderes no siempre es lo mejor opción pues podrían existir buenas razones para considerar a los proveedores aspirantes del mercado o un proveedor jugador de nicho que pudiesen satisfacer de mejor manera las necesidades del comprador, dependiendo, eso sí, de cómo el proveedor seleccionado se alinea con los objetivos comerciales del cliente y el tipo y magnitud de riesgos que ese cliente esté dispuesto a aceptar para alcanzar sus objetivos, lo que obviamente debería incluir los riesgos relacionados con la seguridad de la información.

En este mismo sentido, el Foro Económico Mundial recomienda que todas las organizaciones deberían establecer claramente su apetito y tolerancia al riesgo como un mecanismo para sortear de mejor manera las incertidumbres, optimizar sus procesos de toma de decisiones y mejorar su capacidad de resiliencia ante posibles retos operativos y de mercado. Hace énfasis en la importancia que esta recomendación tiene para las mipymes, principalmente para aquellas que operan como unidades auxiliares (subcontratistas o outsourcer) de empresas más grandes, formando una parte vital del

ecosistema de la cadena de suministro pues su adecuado desempeño y supervivencia garantiza el buen funcionamiento de industrias más grandes y contribuye a la productividad y eficiencia generales de la economía en su conjunto (World Economic Forum. 2023)

Las perspectivas anteriormente expuestas se posicionan desde la situación del contratante. Ahora bien, desde el punto de vista de quien ofrece los servicios y soluciones de TI, es decir, desde la perspectiva del contratista o prestador del servicio, el outsourcing inició con modelos de servicio basados en funciones básicas como el mantenimiento de hardware, software y el help-desk o soporte de usuarios, hasta convertirse en un modelo de negocio que ofrece a sus clientes la promesa de generar valor agregado a través de servicios y soluciones de TI que sirven de catalizadores de los planes de transformación de negocio de los potenciales clientes. Los servicios y soluciones de TI actualmente cubren desde la gestión del portafolio de aplicaciones, fábrica de software y desarrollo de aplicaciones a la medida, centros de servicios de mantenimiento y administración de centros de datos, hasta soluciones de transformación digital de negocios. Los proveedores de servicios y soluciones de TI entienden el outsourcing como una asociación a largo plazo con los clientes para lograr tanto los objetivos de desarrollo y estrategia de negocio propios como de sus clientes, y lo ofertan bajo un esquema de alianza estratégica. (Ruiz, E. 2017).

Los proveedores de servicios y soluciones de TI son por excelencia organizaciones basadas en proyectos. De acuerdo con la Guía de los Fundamentos para la Dirección de Proyectos (PMI.2021), las organizaciones basadas en proyectos son aquellas cuyas operaciones se componen principalmente de proyectos, obtienen sus ingresos principalmente de la ejecución de proyectos para otros en virtud de un contrato y han adoptado la dirección por proyectos para facilitar la ejecución de proyectos para terceros.

En Colombia, de acuerdo con el estudio Caracterización del Sector de Teleinformática, Software y TI en Colombia 2015 del Ministerio de las Tecnologías de la información y las Comunicaciones de Colombia del MinTIC, SENA y Fedesoft (2016), las empresas del Sector Teleinformática, Software y TI se caracterizan por:

- Tener una estructura organizacional de tipo vertical (jerárquica), 47%, seguido por un 38% que identifica su estructura como del tipo horizontal, mientras que el 14% ha implementado una estructura matricial con tendencia a definir su organización con base en proyectos dentro de un enfoque de equipos de trabajo multidisciplinarios.
- Trabajar por procesos, donde los principales procesos identificados se encuentran en su orden: Diseño y Desarrollo, Gerencial/ Estratégico, Gestión de Proyectos, Gestión de Soporte Técnico y Gestión Comercial.
- Desarrollar el proceso de Gestión de Proyectos en fases de planeación, organización, dirección y control sobre proyectos que son aplicadas a proyectos generados por emprendimientos internos para productos/servicios o por requisitos del cliente, para alcanzar los objetivos planteados bajo un acuerdo comercial.
- Emplear personal calificado: El 58% de las personas del nivel táctico en el sector son profesionales, el 19% son técnicos o tecnólogos, el 14% tienen nivel de especialistas, mientras que el 3% tienen nivel elemental y el 4% calificado, por lo que el 2% tienen maestría.
- Altos niveles de capacitación interna no estructurada: El 39% de las empresas afirmaron brindar capacitación y/o entrenamiento a sus empleados por medio de cursos o charlas esporádicas acerca de temas específicos, el 22% brinda entrenamiento esporádico para situaciones específicas o manejo de equipo,

seguido por cursos o charlas de acuerdo a un programa de capacitación con el 21%, y un 18% no brinda capacitación.

- Asignar como responsable de los proyectos, a un director de proyectos o un coordinador de proyectos. Dentro de la estructura organizacional el director de proyectos se clasifica en un nivel táctico, mientras que el coordinador de proyectos se clasifica en el nivel operativo. En general el director de proyectos tiene una maestría en gerencia de proyectos y/o la certificación PMP y el coordinador de proyectos solo tiene la certificación PMP.

No hay referencia que las compañías colombianas que ofrecen productos y servicios de TI consideren la seguridad de la información como uno de los elementos claves de su gestión, pero no por eso se puede dar por sentado que no lo consideren, ni que sean descuidados o desinteresados por ese menester, pues muchas de ellas consideran implementar y certificarse en ISO/IEC 27001 Sistemas de Gestión de Seguridad de la Información.

4.2.3. Gestión de Seguridad de la Información

De acuerdo con Romero M. & Otros (2018), la seguridad se puede concebir como un estado de bienestar por la ausencia de riesgo y la confianza que existe en algo o en alguien. Desde ese punto de vista, definen la seguridad como una ciencia interdisciplinaria para evaluar y gestionar los riesgos a los que se expone una persona, un animal, un ambiente o un bien. De igual manera, establecen que existen diferentes tipos de seguridad y por lo tanto se puede hablar de seguridad ambiental, seguridad económica, seguridad sanitaria y seguridad de la información. Establecen que la seguridad de la información se preocupa por proteger todo aquello que sea información y del medio que la pueda contener y catalogan a la información como “el oro de la seguridad” ya que es lo que una organización debe atesorar y poner a salvo. Concluyen

que la información es el principal activo de una compañía y por lo tanto su seguridad implica cuatro acciones relacionadas con los riesgos que enfrenta: Prevención del Riesgo, Transferencia del Riesgo, Mitigación del Riesgo y Aceptación del Riesgo. En la práctica las organizaciones establecen un proceso que define los parámetros para poder controlar y validar de manera cíclica las actividades relacionadas con la custodia y protección de sus activos de información y los riesgos asociados.

Berrueta (2015) señala que al ser la información uno de los activos más importantes de las compañías, se hace imprescindible que cualquier empresa o institución atienda de manera adecuada la seguridad de su información, bien sea para evitar su pérdida o sustracción, y/o intrusiones para modificarla y/o para consultas no autorizadas. Afirma que muchas organizaciones gastan dinero en dotar sus instalaciones con las mejores medidas de seguridad en el mercado para evitar ataques externos, pero no consideran que el uso de la información que realiza el personal interno de la compañía es una fuente muy importante de brechas de seguridad. Estiman que el 70% de los incidentes de seguridad tienen origen interno mientras que tan solo el 30% restante se debe a factores externos a la compañía y por lo tanto es necesario que las organizaciones presten atención no solo a las amenazas externas respecto a la seguridad de la información, también se hace necesario que presten atención a la filtración de información que sale de la organización bien sea de manera consciente o inconsciente.

De acuerdo con la Norma ISO 27000 (2018):

- La información es un activo que es esencial para las organizaciones y por lo tanto debe ser protegido.
- La seguridad de la información, hace referencia a la protección de la información de una organización independiente de cómo se encuentre almacenada y sea transmitida. En una organización la información puede encontrarse

almacenada en medios digitales, como sistemas electrónicos y/o sistemas ópticos, o se puede encontrar almacenada en medios físicos, como papel, pero también se encuentra en forma de conocimiento de los empleados. La información puede ser transmitida por correo postal, medios electrónicos o por comunicación verbal.

- La gestión de la seguridad de la información considera tres pilares principales: confidencialidad, disponibilidad e integridad. La confidencialidad tiene que ver con que la información no esté disponible para o divulgada a personas, entidades o procesos no autorizados; la disponibilidad tiene que ver con que la información sea accesible y utilizable a pedido de una persona, entidad o proceso autorizados; y finalmente, la integridad tiene que ver con que la información solo pueda ser creada, modificada o eliminada por personas, entidades o procesos autorizados.
- Muchas organizaciones dependen de las tecnologías de la información y comunicaciones para la creación, almacenamiento, transmisión, protección y destrucción de su información.
- La seguridad de la información se logra mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) que incluye el conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgos elegido, sean y las políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados.

En el entorno de negocios actual, donde las organizaciones basan sus modelos de negocio en cadenas productivas que integran la comunicación entre sistemas de información de empresas, socios, clientes y empleados y generan una interacción de

datos en línea y tiempo real y principalmente a través de internet para facilitar la conectividad, se ha venido desarrollando una práctica profesional relacionada con la protección de la confidencialidad, disponibilidad e integridad de las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos digitales conocida como ciberseguridad o seguridad de tecnología de la información o seguridad de la información electrónica (INCIBE. 2022). El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, pasando por el gobierno, el estado y la seguridad nacional. Conceptualmente la seguridad de la información es un concepto más amplio que incluye la ciberseguridad. Mientras que la seguridad de la información incluye la protección de información digital y física, la ciberseguridad se enfoca específicamente en la protección de los datos y la información en el ámbito cibernético que es el espacio virtual en el que se desarrollan las relaciones entre personas y organizaciones a través de computadoras, servidores, dispositivos móviles, aplicaciones de software, sistemas de información y las redes de comunicación por Internet. (Ortega.2024).

En el 2009 con la Ley 1341 que establece como principio orientador la Masificación del Gobierno en Línea (hoy Política de Gobierno Digital) el gobierno colombiano inicia formalmente el camino de la adopción uso y aprovechamiento de las TICs en las entidades del sector público que se materializa en el 2011 con la incorporación gradual los medios electrónicos en los procedimientos administrativos (Ley 1473). En el 2014, como política pública o de estado, el gobierno colombiano toma la decisión de fomentar el uso y aprovechamiento de la TICs en el sector público y en general en todos los sectores productivos del país a través de la transformación digital y para este efecto el Ministerio de las Tecnologías de la Información y Comunicaciones – MinTIC establece el Marco de Referencia de Arquitectura Empresarial-MRAE, que, actualmente en la versión

3, está compuesto por tres modelos: Modelo de Arquitectura Empresarial - MAE, Modelo de Gestión y Gobierno de TI - MGGTI y el modelo de Gestión y Proyecto TI (MinTIC, 2023).

La Política de Gobierno Digital de Colombia (Decreto 767 de 2022) busca modernizar la gestión pública y mejorar la prestación de servicios a través del uso de las TIC, incluyendo la seguridad de la información como un pilar fundamental y entonces, como complemento al MRAE y sus tres modelos, el MinTIC establece el Modelo de Seguridad y Privacidad de la Información – MSPI, que además de estar alineado con el Marco de Referencia de Arquitectura (MRAE), también lo está con el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas. El MSPI es una guía para las entidades públicas que contiene buenas prácticas en la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), tomando como referencia estándares internacionales, como la norma ISO 27001 sobre Sistemas de Gestión de Seguridad de la Información e ISO 31000 sobre Gestión de Riesgos (MinTIC, s/f).

Buscando incentivar el potencial de la transformación digital para superar los desafíos económicos, sociales y ambientales del país la Presidencia de la República, el Departamento Nacional de Planeación (DNP) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) han establecido la Estrategia Nacional Digital (END) de Colombia 2023-2026, con el objetivo de cerrar las brechas de acceso, uso y apropiación de las tecnologías digitales entre hogares, entidades públicas, empresas y territorios. La Estrategia Nacional Digital plantea ocho ejes, 100 acciones y 13 indicadores en el marco de la política pública de transformación digital. Los ocho ejes son: conectividad digital, acceso, uso y aprovechamiento de datos, seguridad y

confianza, habilidades y talento digital, inteligencia artificial, transformación digital y economía y sociedad digital. La END articula a las entidades públicas con el sector privado, el sector TIC y la ciudadanía para cumplir las metas del Plan Nacional de Desarrollo y sus habilitadores son la Política de Gobierno Digital con sus tres modelos para el desarrollo y adopción responsable de Inteligencia Artificial en el país, que capitalice los desarrollos técnicos, institucionales y el MSPI en materia de seguridad digital. (DNP.2024)

Dentro del eje de seguridad y confianza de la Estrategia Nacional Digital - END, el departamento de Planeación Nacional ha expedido los siguientes documentos de políticas públicas (CONPES) que incluyen temas relacionados con la seguridad digital (DNP. s/f):

- CONPES 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa. Este documento CONPES busca fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.
- CONPES 3854. Política Nacional de Seguridad Digital. Este documento CONPES busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país
- CONPES 3995. Política Nacional de Confianza y Seguridad digital. Este documento CONPES busca establecer medidas para desarrollar la confianza

digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

4.2.4. Gestión de Seguridad de la información proyectos de Outsourcing de TI.

El outsourcing de servicios y soluciones TI genera riesgos de seguridad de la información derivados del acceso del proveedor a los datos e información del cliente. El Instituto Nacional de Ciberseguridad de España – INCIBE (s/f) señala que, en el mundo empresarial, hay una tendencia generalizada a considerar como activos de la empresa únicamente los bienes tangibles: mobiliario, maquinaria, servidores, etc. Sin embargo, aclara, no se debe olvidar que existen bienes intangibles como la cartera de clientes, las tarifas, las ofertas que se presentan a los clientes, el conocimiento comercial que permite posicionarse en el mercado o frente a la competencia, los planes estratégicos para el crecimiento del negocio, la propiedad intelectual, entre otros. Todos estos elementos forman parte de la información de cualquier empresa y constituyen uno de los activos más importantes de una organización. Señala que la externalización de servicios TI puede introducir nuevos riesgos para la seguridad de la información, derivados del acceso del proveedor a los datos.

Una medida que mitiga, pero no elimina los riesgos que origina el outsourcing de servicios y soluciones de TI, tiene que ver con la exigencia por parte del cliente de la firma de contratos de confidencialidad o inclusión de este tipo de cláusulas en el contrato de servicio. Esto compromete al prestador del servicio bajo un requisito legal obligatorio a

hacer un buen uso de los datos y la información del cliente que accesa y conoce en virtud del desarrollo del Proyecto respectivo.

Desde el punto de vista del proveedor de servicios, Carpentier (2016) propone que la estrategia de servicio de un proveedor de servicios de TI, debe basarse en el hecho de que un cliente no compra productos, sino que requiere servicios que satisfagan sus necesidades particulares. Esta estrategia debe incluir una garantía relacionada con la gestión de seguridad de la información y que debería estar enfocada en alinear la seguridad de la información con la actividad de su negocio y asegurar que los riesgos relacionados con el manejo de la información del cliente se gestionan eficazmente con el fin de cumplir los requisitos contractuales.

Los delitos informáticos, que ponen en riesgo la seguridad de la información, se han disparado en Colombia en el contexto de la Pandemia COVID19. De acuerdo con el diario colombiano Portafolio (2020) un estudio realizado el programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE) del Tanque de Análisis y Creatividad de las TIC (TicTac) presenta las cifras de denuncias por ciberataques durante la pandemia, (marzo- noviembre) donde se registró un incremento superior al 98%, con más de 32 mil reportes de noticias criminales presentadas ante la Fiscalía General de la Nación, siendo el principal incidente de seguridad de la información la suplantación de sitios web para capturar datos personales con 3800 casos y un crecimiento del 372% comparado con el 2019, seguido con 6.159 casos registrados la violación de datos personales y un crecimiento del 190% como consecuencia de la filtración y robo de datos.

Estos ciberataques afectaron por igual diferentes sectores productivos del país y aún, cuando no hay cifras específicas el sector del outsourcing, es evidente que las empresas de servicios y soluciones de TI no se escapan de esa tendencia.

4.3. Bases Legales de la Seguridad de la Información en Colombia.

En Colombia, a raíz de los cada vez más frecuentes ataques informáticos en que afectan de manera negativa la seguridad de la información en las empresas y personas, se ha venido desarrollado una sólida legislación relacionada con la seguridad informática. Actualmente se cuenta con:

- La Decisión 351 de 1993 de la Comunidad Andina de Naciones - CAN, que reconoce los derechos del autor y da protección sin distinguir el tipo de arte.
- Ley 44 de 1993 que modifica la Ley 23 de 1982 y la ley 29 de 1944 que establece disposiciones para el soporte lógico (Software).
- Ley 527 de 1999 que reglamenta el acceso y uso de mensajes de datos y comercio electrónico y de las firmas digitales. Esta ley trata del uso de información o datos para el comercio electrónico, firmas digitales, mensajes de datos por medio escrito y digital, de la certificación de las personas naturales y jurídicas para realizar transacciones electrónicas y además da reconocimiento legal a los documentos electrónicos como si fueran físicos y pueden ser parte de un proceso legal.
- Ley 545 de 1999 por la cual se aprueba el Tratado de la OMPI -Organización Mundial de la Propiedad Intelectual- sobre Interpretación o Ejecución y Fonogramas (WPPT), adoptado en Ginebra el 20 de diciembre de 1996.
- La Ley 23 de 1982 que regula lo correspondiente a los derechos de autor en Colombia
- Ley 1266 de 2008, con la cual se dictan disposiciones del hábeas data y se regula el manejo de la información que está contenida en las bases de datos especialmente financieras y crediticias.
- Ley 1273 de 2009, conocida como Ley de Delitos Informáticos, añade dos capítulos al código penal colombiano:

  - El Capítulo 1, que trata sobre los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas de informáticos
  - El Capítulo 2, que trata sobre los atentados informáticos y otras infracciones, esta ley está muy atada a la norma ISO 27000, lo que permite al país estar en la vanguardia en la legislación de seguridad Informática.

- Ley 1581 de 2012 que dicta disposiciones sobre la protección de datos personales. Se trata básicamente de reconocer el derecho que tiene toda persona de conocer, actualizar y rectificar los datos que se hayan recogido sobre cada una en bases de datos, así como reconocer el derecho constitucional referido en el artículo 15 de la constitución política de Colombia que se refiere principal al derecho a la intimidad y el artículo 20 que se refiere al derecho de informar y recibir información veraz.
- Ley 1753 de 2015 con la cual se crea el Sistema Nacional de Seguridad y Convivencia Ciudadana, que incluye un componente de ciberseguridad.
- Decreto 1078 de 2015, decreto único reglamentario del sector de las Tecnologías de la Información y las Comunicaciones (TIC), incluye disposiciones sobre seguridad de la información en las entidades públicas y privadas
- Ley 1915 de 2018: Esta ley modifica y adiciona algunas disposiciones de la Ley 23 de 1982 sobre derechos de autor, incluyendo aspectos relacionados con la protección de obras digitales y la gestión de derechos digitales.
- Decreto 338 de 2022 por medio del cual se establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital

5. Hipótesis

Hernández-Sampieri R.& Mendoza C (2018) definen la hipótesis de investigación como la respuesta provisional a la pregunta de investigación y aclaran que en el caso de las hipótesis que corresponden a estudios descriptivos o correlacionales buscan pronosticar una cifra, un dato o un hecho. En línea con esta definición y aclaración, a continuación, se plantea la hipótesis que da respuesta a la pregunta de la presente investigación:

La mayoría de las compañías de outsourcing de Servicios y Soluciones TI no tienen implementadas estrategias claras para gestionar los riesgos de brechas de seguridad de los activos de información de sus clientes como parte de su oferta de valor, lo que implica que los gerentes de proyectos de outsourcing de Servicios y Soluciones TI no protegen de manera adecuada los activos de información que tienen valor de negocio tanto para el proveedor de los servicios y soluciones de TI como para sus clientes, no consideran la gestión de riesgos de seguridad como una de sus áreas de interés para aplicar y no están preparados para gestionar los riesgos de seguridad de la información.

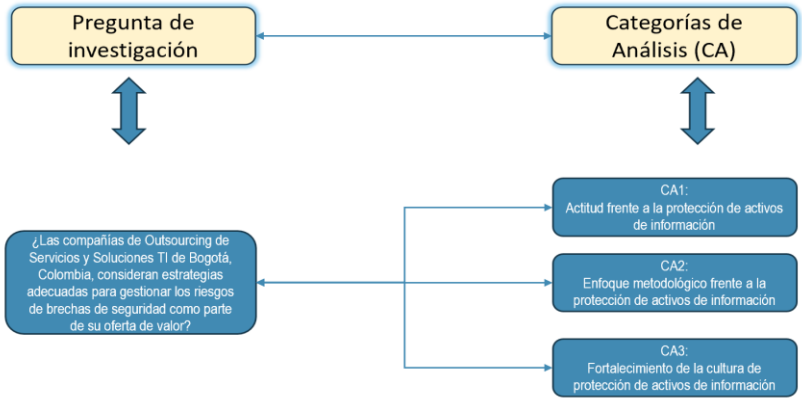
6. Categorías de análisis

Las categorías de análisis corresponden a las propiedades del objeto de estudio que se manifiestan a través de conductas observables, generalmente denominadas indicadores, que caracterizan y/o explican fenómenos sociales bajo observación (Malvaceda E. & Otros. 2023). Las categorías de análisis se utilizan para ordenar el trabajo de recolección y análisis de datos con el fin de responder la pregunta de investigación y cumplir con los objetivos planteados para el estudio que se esté llevando a cabo (Salazar M. 2013).

Considerando las anteriores conceptualizaciones, para el presente estudio se definieron tres categorías de análisis para establecer si las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, consideran estrategias adecuadas para gestionar los riesgos de brechas de seguridad como parte de su oferta de valor: i) actitud frente a la protección de activos de información, ii) enfoque metodológico frente a la protección de activos de información, y iii) fortalecimiento de la cultura de protección de activos de información.

El siguiente diagrama muestra la relación entre la pregunta de investigación y las categorías de análisis propuestas para esta investigación:

Ilustración 3 – Relacionamiento pregunta investigación y categorías análisis



Elaboración propia

Para mostrar la relación entre los objetivos específicos del estudio con cada categoría de análisis, se elaboró la siguiente tabla:

Tabla 2 – Objetivos de investigación y las Categorías de Análisis

Objetivo específico	Categorías de análisis			
	Nombre	Definición Conceptual	Definición Operacional	Indicador
Identificar cómo las compañías de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia protegen los activos de información que tienen valor de negocio para sus	**CA1: Actitud frente a la protección de activos de información**	Definición estratégica de la organización que orienta los procesos y controles de protección de activos de	Observación directa	Declaración en la promesa de valor a los clientes

Objetivo específico	Categorías de análisis			
	Nombre	Definición Conceptual	Definición Operacional	Indicador
clientes en la ejecución de sus proyectos		información del cliente		
Determinar cuál es el enfoque metodológico que aplican las compañías de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, para la gestión de riesgos de seguridad en sus proyectos	**CA2: Enfoque metodológico frente a la protección de activos de información**	Implementación de marcos de referencia reconocidos para la protección de activos de información	Observación directa	Modelos de Sistemas de Gestión de Seguridad de la Información certificados de manera independiente
Establecer la manera cómo las compañías de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia preparan a sus gerentes de proyectos en la gestión de los riesgos de seguridad de la información	**CA3: Fortalecimiento de la cultura de protección de activos de información**	Desarrollo profesional desde la empresa	Observación directa	Acciones de sensibilización de protección de activos de información desarrolladas internamente por la compañía

Fuente: Elaboración propia

7. Metodología

La definición del enfoque metodológico y el alcance de la investigación, la población y muestra, el instrumento de medición y su validación y los procedimientos y técnicas para la recolección y análisis de la información se presentan a continuación.

7.1. Enfoque y alcance de la investigación

El enfoque metodológico básico de la presente investigación fue el interpretativo o cualitativo. Uno de los objetivos de investigación que demandan metodologías cualitativas es reconocer las prácticas sociales (Galeano, M. 2004) y en este caso se trata de estudiar la postura y acciones de las compañías de outsourcing de servicios y soluciones TI y sus equipos de proyecto de gestión de proyectos respecto a la seguridad de los activos de información de sus clientes.

Respecto a la naturaleza de la investigación, el presente trabajo adoptó el método descriptivo que, de acuerdo con Hernández- Sampieri R. & Otros (2006), es la

investigación que se limita a describir fenómenos, situaciones, contextos y eventos, mediante los cuales se pretende especificar las propiedades, características o los perfiles de personas, grupos, comunidades o cualquier otro tipo de sujeto bajo estudio.

Al ser un estudio cualitativo descriptivo de la problemática relacionada con las estrategias implementadas por las compañías de outsourcing de Servicios y Soluciones TI en Bogotá, Colombia, para dar tratamiento a los riesgos de Seguridad de la información en la gestión de proyectos, los resultados se relacionan con la manera cómo estás compañías protegen los activos de información que tienen valor de negocio para sus clientes, identificar cuál es el enfoque metodológico que aplican y establecer la manera cómo las compañías de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia y preparan a sus gerentes de proyectos para gestionar los riesgos de seguridad de la información. En ningún momento estos resultados conducen, de ninguna manera, a determinar las causas que originan esta problemática.

Así pues, el diseño de la investigación se enfoca en establecer una descripción lo más completa posible de la problemática a partir de la observación de la configuración de las estrategias y los métodos de seguridad de la información que aplican las compañías que proveen servicios y soluciones de TI de Bogotá, Colombia, y de la manera como estas organizaciones preparan a sus gerentes de proyectos en la aplicación de tales estrategias. Por lo tanto, esta investigación no pregunta ni responde por la causalidad de la situación observada, es decir, el por qué ocurre lo que se observa. Simplemente, trata de obtener una imagen esclarecedora del estado de la situación.

Como parte fundamental de la metodología de trabajo, se realizó una serie de consultas a profundidad de otros trabajos, libros, artículos y páginas de internet a fin de recolectar suficiente información para cumplir con los objetivos planteados. En el trabajo de investigación de campo se recopiló información acerca de la gestión de proyectos y la

gestión de la seguridad información y de manera similar se realizó la investigación de los marcos de trabajo utilizados a fin de permitir una mejor comprensión del tema y la problemática planteada.

7.2. Población y muestra

De acuerdo con Hernández-Sampieri, R. & Mendoza, C (2018), la población debe situarse en torno a sus atributos de contenido, tiempo y lugar y definir sus características con el propósito de establecer los parámetros muestrales que delimitarán la muestra del estudio. Para el presente estudio, la población corresponde a las empresas de outsourcing de servicios y soluciones (contenido) de Bogotá, Colombia (lugar) que reportaron ingresos durante 2022 (tiempo) según el Sistema de Integrado de Información Societaria – SIIS de la Superintendencia de Sociedades.

Respecto las características y dinámica de estas compañías, el estudio Caracterización del Sector de Teleinformática, Software y TI en Colombia 2015 del Ministerio de las Tecnologías de la información y las Comunicaciones de Colombia del MinTIC, SENA y Fedesoft (2016) y el estudio Observatorio de Competitividad de FEDESOFT (Fedesoft.2019), a partir de encuestas y estadísticas generadas en diferentes fuentes públicas de información tales como CC - Cámaras de Comercio, DANE- Departamento Administrativo Nacional de Estadística, DNDA – Dirección Nacional de Derechos de Autor, Superintendencia de Sociedades y fuentes de información privadas especializadas en la comercialización de datos comerciales y financieros, como es el caso de EMIS (Emerging Markets Information System), INFORMA COLOMBIA y DATOS.COM, permiten establecer que las empresas del sector de outsourcing de servicios y soluciones TI de Bogotá, Colombia con experiencia en el desarrollo de soluciones y prestación de servicios TI, atienden diferentes verticales de mercado como Fintech, Salud, Agroindustria, Oil&Gas, Energía y Telecomunicaciones,

Logística, Gobierno, Marketing Digital, Realidad Virtual y Aumentada, Negocios y Big Data, entre otros y presentan una naturaleza muy heterogénea ya sea por la oferta de servicios, el número de empleados, las líneas de negocios, el valor de activos, las certificaciones, el tiempo de antigüedad, etc., sin embargo, en su gran mayoría en cuanto a su modelo de gestión se caracterizan por:

- Corresponder a micro, pequeñas y medianas empresas, pues su tamaño se concentra en hasta 50 empleados, siendo muy pocas las que tienen de 51 a 200 empleados y muy escasas aquellas que superan los 200 empleados y por nivel de ventas el 50% corresponden a micro empresas, el 31% a pequeñas, el 13% a medianas y tan solo el 6% corresponden a grandes empresas.
- Presentar estructuras organizacionales tipo vertical clásica con un fuerte enfoque en áreas departamentales, de las cuales se destaca el área operativa y el área comercial como áreas misionales y el área administrativa desempeñando funciones de apoyo.
- Operar bajo una cadena de valor tradicional basada en la interrelación de tres tipos básicos de procesos (estratégicos, misionales y de apoyo) muy alineados con la estructura organizacional, que interactúan con el propósito de lograr la satisfacción de las partes interesadas, entre los que se identifican principalmente:
    - Procesos estratégicos: Gestión Estratégica y Gestión Financiera.
    - Procesos misionales se encuentran transversalmente Gestión Comercial, Gestión de Servicio al Cliente y Gestión de Proyectos; Análisis de Negocios, Diseño y Desarrollo, Gestión de Operaciones, Gestión Soporte Técnico, Gestión Bases de Datos y Aseguramiento de Calidad.

- Procesos de apoyo: Gestión Administrativa, Gestión del Talento Humano, Gestión de equipos e informática/ infraestructura.

- Considerar relevante la adopción de modelos de Gestión de Calidad, principalmente de calidad en TI y modelos de Gestión de Seguridad de la Información, pero el 44% no los implementa, el 20% está en proceso de implementación y el 36% ya lo implementado y certificó. Entre las certificaciones de Gestión de la Calidad más implementadas se encuentran CMMI nivel 3, ITMARK e ISO 9001. Entre las que se encuentran en implementación están: CMMI nivel 3, ITMARK, ITIL e ISO/IEC 27001 sistemas de gestión de seguridad de la información.
- Operativamente las empresas del sector de outsourcing de servicios y soluciones TI de Bogotá, Colombia, en términos generales, desarrollan el outsourcing bajo la modalidad de proyectos soluciones y proyectos de operaciones de servicios. Para este efecto conforman equipos de proyecto, que bajo la dirección de un Gerente o Líder de Proyecto se encargan del desarrollo de las soluciones TI y la prestación de servicios dentro del alcance contractual acordado con sus clientes.

La muestra fue no probabilística y con el fin de minimizar y controlar los riesgos de sesgos en este tipo de muestra, para el presente estudio se consideró:

- La utilización de la técnica de muestreo no probabilístico por conveniencia. (Boza & Otros. 2021). Se consultó en el Sistema Integrado de Información Societaria - SIIS de la Superintendencia de Sociedades (https://siis.ia.supersociedades.gov.co/#/) y se identificaron 22 compañías que, de acuerdo con su naturaleza, objeto social, oferta de servicios y domicilio

registrado en Bogotá reportaron ingresos durante al corte de diciembre 31 de 2022.

- La definición de criterios de representatividad cualitativa basadas en características conductuales o teóricas para seleccionar las fuentes de información administrativa (Sanjuán L. 2019) que propicien la validez de sus repuestas (Flores F. & Mora R. 2023). En el caso del presente estudio las características para definir las fuentes de información administrativa son: (i) desempeñar el rol de Gerente y/o Líder de proyecto y (ii) tener o haber tenido vinculación laboral con las empresas seleccionadas De esta manera las fuentes de información administrativa para el presente estudio corresponden a los Gerentes y/o líderes de los equipos de proyecto que han estado o están vinculados a las 22 empresas de outsourcing de servicios y soluciones de Bogotá, Colombia identificadas y por lo tanto pueden proporcionar la información más relevante y significativa durante el proceso investigativo. Cabe señalar que, en los estudios sociales, administrativos y económicos cualitativos, existe una tendencia generalizada y rápida hacia el uso de fuentes administrativas basadas en criterios de representatividad cualitativa, ya sea para complementar fuentes tradicionales de datos obtenidos a través de censos y encuestas, compensar la ausencia o deficiencias de los datos recogidos por medios tradicionales o para reemplazar las fuentes tradicionales de captura de datos, esto debido a las ventajas de esta tendencia general, incluida una reducción de la carga para los encuestados, una producción más rápida de estadísticas y la consiguiente reducción de costes (United Nations.2023).
- La cantidad de 30 entrevistas como la cantidad requerida para el presente estudio. Esta cantidad de entrevistas se basa en el trabajo práctico de

investigación del sociólogo francés Daniel Bertuax de 1993, que establece en 30 el número de casos necesarios para lograr el punto de saturación en muestras cualitativas precisando que una menor cantidad de unidades de muestra tiende a dar una visión incompleta y una mayor cantidad tiende a la saturación del conocimiento o a la repetibilidad donde los nuevos casos no introducen correcciones ni complementan y solo repiten el conocimiento de la realidad estudiada. (Mejía J. 2000). Esta cantidad mínima se fue cristalizando durante el desarrollo de los tres momentos del trabajo de campo: general (contacto inicial con el grupo semilla), específico (respuesta a la encuesta)) y de referenciación (nuevos participantes).

- La utilización de la técnica de muestreo intencional de red también conocida de bola de nieve o de cadena y que ayuda en la identificación de casos de interés de personas que conocen a otras personas que pueden ser fuentes de información útiles para el estudio y tiene mejor adaptación a los estudios de investigación cualitativa con fuentes de información ocultas o difíciles de censar (hard-to-reach) bien sea por tener acceso limitado a la tecnología, bajos niveles de alfabetización, barreras culturales o preocupaciones de privacidad que los hacen menos propensos a participar en encuestas, entrevistas o grupos focales, y se adapta muy bien a una selección mediante participantes semilla (Polgar & Thomas. 2021). Para la presente investigación no se identificó un directorio y/o base de datos que de manera oficial registre y/o mantenga un censo de los Gerentes de Proyecto y/o Lideres dedicados al campo de las TICs y que posibilite la selección de la muestra de forma probabilística, así que el grupo semilla corresponde a los 22 Gerentes y/o Líderes de proyecto encontrados en LinkedIn y en el formulario de la encuesta online se incluyó la solicitud de

referenciación de la red de contactos que el encuestado considere que están dispuestos a participar del estudio asegurando mantener total reserva de los datos compartidos. Idealmente, si cada uno de los Gerentes de Proyecto propone un referenciado que cumpla las características de fuente de información se le invitaría y si responde, sus datos serían considerados y se tendrían 44 encuestas. Aun cuando se supere el punto de saturación, esto no tendría mayor significancia para el estudio, pero mantendría el nivel de confianza de los participantes tanto en el estudio como en el perfil del investigador.

- La utilización de las redes sociales virtuales (RRSS) y en general de una estrategia metodológica que integra el uso de nuevas tecnologías de información para estudiar la empresarialidad étnica y posibilitan acceder a unidades de observación que no se hubieran detectado por vías institucionales tradicionales como listados, registros administrativos, archivos y/o censos y que por lo tanto son difícilmente accesibles (hard-to-reach) (Baltar F. & Gorjup M.2012). Específicamente, para el presente estudio se eligió la utilización de LinkedIn por ser una red social orientada al uso empresarial, a los negocios y al empleo y en donde cada perfil libremente revela su experiencia laboral. A partir de esta red se ubicaron los 22 participantes iniciales, que cumplieran los dos criterios como fuentes de información administrativa: Cargo Gerente y/o líder de equipos de proyecto de las 22 empresas identificadas, y como grupo semilla, a través del servicio de mensajería propio de la red InMail, que cumple la función de sistema de correo, se les envió un mensaje individual invitándolos a participar a través de un enlace al cuestionario online y se le pidió que referenciaran a otras Gerentes y/o Líderes de Proyecto que consideran podrían estar interesados en participar, asegurándoles que sus datos personales y los de sus

referenciados no serían recolectados por lo que de ninguna manera sus respuestas individuales podrían ser conocidas.

- La aplicación de una estrategia de participación basada en condiciones de privacidad de los datos identificables, es decir de confidencialidad y no divulgación de datos personales y datos corporativa y anonimización de la información (CEPAL. s/f) que, para la presente investigación incluye: (i) recopilar información personal mínima de nombre, cargo y empresa para el reclutamiento de fuentes de información administrativa (ii) Retirar los datos de nombre y empresa después de la recolección de información (iii) Usar únicamente la red LinkedIn y sus facilidades de mensajería, y (iv) tratamiento masivo de los datos. Se considera esta estrategia un factor importante por cuanto se estudia un tema sensible como es el de las estrategias para tratar los riesgos de seguridad de la información en el que los gerentes y/o líderes de proyecto no hablan abiertamente, o si hablan sobre las estrategias implementadas por las compañías de outsourcing de Servicios y Soluciones TI en Bogotá, Colombia, para dar tratamiento a los riesgos de Seguridad de la información en la gestión de proyectos de servicios y soluciones de TI, podrían incurrir en incumplimiento de acuerdos de la cláusula de confidencialidad de sus contratos de vinculación laboral o prestación de servicios.

7.3. Instrumentos

De acuerdo con Arias F. (2012), la técnica de investigación es el procedimiento formal para obtener los datos e información, mientras que el instrumento de recolección de datos es cualquier recurso físico, en papel o digital que se utiliza para registrar y almacenar información siendo ejemplos de instrumentos de recolección de datos el cuestionario, una libreta de apuntes, programas de computador, cámaras fotográficas,

cámaras de video y grabadoras de audio. En esta misma línea de pensamiento, Fabregues S. (2016) define que el cuestionario es la técnica o el instrumento empleado para la recolección de datos mientras que la metodología de las encuestas es el conjunto de pasos organizados o la técnica para su diseño, administración y recogida de datos.

Para la presente investigación se utilizó el cuestionario como el instrumento para la recogida de datos durante el trabajo de campo que se llevó a cabo con la metodología o técnica de encuestas.

A continuación, se plantea una tabla que relaciona el diseño y la técnica e instrumento de recolección de datos de la presente investigación:

Tabla 3 – Diseño, técnica e instrumento de la investigación

Diseño	Técnica	Instrumento
Investigación de campo	Encuesta escrita	Cuestionario

Fuente: Adaptado de Arias F. (2012)

El cuestionario utilizado tiene 9 preguntas dicotómicas e incluyó una justificación de la elección que facilitó su estandarización y análisis para establecer las conclusiones y generalizaciones correspondientes. La siguiente tabla muestra la relación de las categorías de análisis, los indicadores y los tipos preguntas:

Tabla 4 – Relación categorías de análisis, indicadores y tipos preguntas

Categoría de Análisis	Indicador	Preguntas
CA1: Actitud frente a la protección de activos de información	Declaración en la promesa de valor a los clientes	1 a 3 sobre Gobierno, riesgo y conformidad de los activos de los clientes
CA2: Enfoque metodológico frente a la protección de	Modelos de Sistemas de Gestión de Seguridad de la Información certificados de manera independiente	4 a 6 sobre Estrategia para la seguridad de la información de los activos de los clientes

activos de información		
CA3: Fortalecimiento de la cultura de protección de activos de información	Acciones de sensibilización de protección de activos de información desarrolladas internamente por la compañía	7 a 9 sobre Uso y apropiación de los principios organizacionales respecto a la protección de los activos de información de los clientes.

Fuente: Elaboración propia

En el anexo A se presenta el cuestionario aplicado para la recolección de datos e información. En este cuestionario no se recolectan datos de identificación personal con el fin de garantizar la protección de los datos personales de los participantes. De igual manera tampoco se filmaron, grabaron ni se registraron imágenes de los entrevistados. En todo caso siempre se buscó proteger a los participantes de cualquier daño originado por la pérdida de su privacidad.

Respecto a la validez del contenido del cuestionario, se utilizó el método de coeficiente V de Aiken (Aiken L.1985). Para el cálculo de este coeficiente se eligieron 5 (cinco) evaluadores que califican Claridad, es decir que la pregunta está correctamente redactada y sea fácil de comprender; Pertinencia, es decir que la pregunta permita medir con precisión la variable identificada; y Relevancia, es decir que se evidencie un enfoque teórico adecuado en la redacción de la pregunta. La calificación tomó los valores 0 y 1. Posteriormente se promedian las calificaciones de los evaluadores y el resultado de las preguntas que se acerque a 1 revela una valoración positiva. Las que se alejen sugieren revisar o eliminar los ítems. La fórmula de cálculo utilizada es la siguiente:

$$V = \frac{P}{E * (C-1)}$$

Donde:
V = Coeficiente de Aiken
P = Promedio de las calificaciones de los evaluadores
E = Número de evaluadores (5 en este caso)
C = Número de valores de la escala de valoración (2 en este caso)

Los evaluadores seleccionados fueron cinco (5) expertos tanto con conocimiento como con experiencia práctica y su tarea fue la evaluación de la claridad, pertinencia y relevancia de las preguntas propuestas (Supó J.2013.). Esto evaluadores fueron:

- Evaluador #1: Miembro del Comité Técnico sobre Seguridad de la información y Ciberseguridad de la Asociación Española de Normalización y Certificación - AENOR . Ingeniería de sistemas. Certificado como Gerente de Proyectos del Project Management Institute - PMI. Auditor Líder de certificación en sistemas de gestión de seguridad de la información y sistemas de gestión de servicios por más de 15 años. Consultor, conferencista y tutor.
- Evaluador #2: Miembro del comité IT Governance de ISACA. Ingeniería de Sistemas. Especialista en Gobierno de TI, riesgos, seguridad de la información (ciberseguridad). Certificado CISM (Certified Information Security Manager). Consultor, conferencista y trainer en cursos de certificación de ISACA.
- Evaluador #3: Decanatura de Ingeniería de Sistemas y vicerrectoría. Ingeniería de sistemas y Executive MBA. Docente en pregrado y posgrado en Gerencia de Proyectos, gobierno de TI, arquitectura empresarial, y business process management. Investigador reconocido por el Ministerio de Ciencia, Tecnología e Innovación.
- Evaluador #4: Miembro del equipo de Mentoría del Project Management Institute - PMI. Magister en Ingeniería Ambiental. Gerente de proyectos PMI. Consultora en

proyectos del sector energético y agricultura sostenible. Conferencista e investigadora.

- Evaluador #5: Maestría en Educación y Entornos Virtuales de Aprendizaje, Especialista en Gerencia Informática y Líder Programa Administración y Dirección de Empresas. Reconocido por el Ministerio de Ciencia, Tecnología e Innovación – MINCIENCIAS, como Investigador del SNCT en la categoría Integrante Vinculado con Maestría.

A los evaluadores se les proporcionó el formato de evaluación que contiene las preguntas propuestas y las instrucciones para su validación. Adicionalmente se les entrego el título de la investigación, su objetivo, las características de la población y la muestra. Las evaluaciones de cada experto se consolidaron para el cálculo del coeficiente V de Aiken. La siguiente tabla muestra los resultados del coeficiente V de Aiken:

Tabla 5 – Resultado coeficiente V de Aiken

		A. Actitud frente a la protección de activos de información	EVALUADOR1	EVALUADOR2	EVALUADOR3	EVALUADOR4	EVALUADOR5	V DE AIKEN
Preguntas	1	¿La compañía cuenta con una política de uso de activos de información pertenecientes a los clientes aprobada por la alta Dirección que contemple los escenarios de riesgos a los cuales están expuestos tales activos de información?	1,00	1,00	1,00	1,00	1,00	1,00
	2	¿La compañía tiene formalizada y en operación una estructura organizacional que define los roles y responsabilidades frente a la seguridad de la información de los activos de información pertenecientes a los clientes?	1,00	0,67	1,00	1,00	1,00	0,93
	3	¿Los requisitos legales, regulatorios, y/o estatutarios relacionados con los activos de información del cliente son definidos de forma explícita?	1,00	0,67	1,00	1,00	1,00	0,93
		B. Enfoque metodológico frente a la protección de activos de información	**EVALUADOR1**	**EVALUADOR2**	**EVALUADOR3**	**EVALUADOR4**	**EVALUADOR5**	**V DE AIKEN**
Preguntas	1	¿La compañía posee certificaciones de estándares de seguridad u otras certificaciones relacionadas?	1,00	1,00	1,00	1,00	0,67	0,93
	2	¿La compañía define un plan de gestión de la seguridad específico para cada proyecto/servicio prestado que establezca los requisitos de seguridad de los activos de información del cliente y el enfoque para cumplirlos?	0,67	1,00	1,00	1,00	1,00	0,93
	3	¿Qué mecanismos ha implementado la compañía para la identificación, detección y bloqueo de fuga de información confidencial y crítica de los clientes?	1,00	1,00	1,00	1,00	0,67	0,93
		C. Fortalecimiento de la cultura de protección de activos de información	**EVALUADOR1**	**EVALUADOR2**	**EVALUADOR3**	**EVALUADOR4**	**EVALUADOR5**	**V DE AIKEN**
Preguntas	1	¿Existen programas definidos para que los equipos de proyecto/servicio tengan una concientización y entrenamiento referente a los aspectos relevantes en seguridad de la información y uso adecuado de los activos de información de los clientes?	1,00	1,00	1,00	1,00	0,67	0,93
	2	¿Se ha definido e implementado un proceso disciplinario formal, que incluya las acciones a tomar ante aquel personal que haya provocado alguna brecha de seguridad respecto a los activos de información de los clientes?	0,67	1,00	1,00	1,00	1,00	0,93
	3	¿Con cuales certificaciones cuenta sus gerentes de proyecto/servicio en cuanto buenas prácticas en seguridad de la información?	1,00	1,00	1,00	1,00	1,00	1,00

Fuente: Elaboración a partir de la plantilla suministrada por la UEAN

De acuerdo con los resultados consolidados de la valoración de los expertos, no se eliminaron preguntas y se realizó la siguiente revisión en cuanto a la redacción de aquellas con calificación menor a 1:

- Pregunta A2: No se modificó por cuanto es claro que los roles y responsabilidades organizacionalmente de definen dentro de una estructura, en este caso relacionadas con la seguridad de la información perteneciente a los clientes.
- Pregunta A3: No se modificó por cuanto es relevante que todos los requisitos queden formalmente definidos para facilitar su control, auditoría y trazabilidad, bien sea en el contrato, anexos técnicos o cualquier otro documento relacionado.
- Pregunta B1: Se modificó la redacción para incluir cuales son las certificaciones a nivel de compañía a las que se refiere la pregunta.
- Pregunta B2: No se modificó por cuanto su pertinencia radica en el hecho de que cada proyecto tiene un alcance y tiempo de servicio o solución diferente haciendo que los activos de la información del cliente también sean diferentes de manera que un plan general sería poco práctico.
- Pregunta B3: Se modificó la redacción para cambiar mecanismo por controles.
- Pregunta C1: Se modificó la redacción para precisar que se trata de programas de concientización y entrenamiento.
- Pregunta C3: Se modificó la redacción para precisar que se trata de las certificaciones en seguridad que posee el gerente/líder de proyecto que contesta la encuesta. No corresponde a ninguna observación de los evaluadores.

7.4. Técnicas para el análisis de la información

De acuerdo con Abarca & Otros (2013), el procedimiento o serie de pasos que ordenan la actividad científica corresponden con el método, mientras que las técnicas

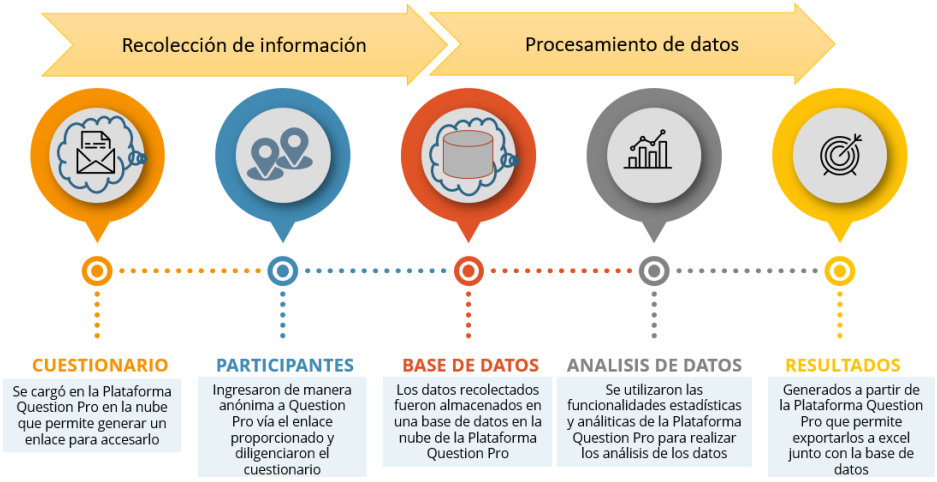
son el conjunto de reglas y operaciones para el manejo de los instrumentos que le facilitan al investigador la aplicación del método. En este contexto, Gil J. (2016) plantea que una vez realizado el diseño metodológico de la investigación que incluye la definición del instrumento de recolección de datos e información, el procedimiento que continua tiene que ver con los pasos relacionados con el trabajo de campo para obtener, registrar y almacenar los datos e información, proceder con su procesamiento, generar el informe del resultado y con base en ese informe de resultados establecer las conclusiones de la investigación.

Para obtener y registrar los datos de la investigación en un trabajo de campo se utilizan tres técnicas básicas: la observación, la encuesta y la entrevista. La observación se refiere a la captura de manera espontánea de cosas o hechos realizados por el investigador a través de sus propios sentidos, en la encuesta la obtención de datos se realiza a través de un formulario previamente suministrado por el investigador y en la entrevista el investigador obtiene los datos a través de conversaciones dirigidas (Hernández A. & Otros. 2018). De estas tres técnicas básicas para obtener datos e información, la encuesta es aquella que permite obtener datos e información cuantitativa y cualitativamente de forma sistemática y estandarizada a través del instrumento llamado cuestionario (Quispe A. 2013). El almacenamiento y procesamiento de los datos recolectados en el trabajo de campo de una investigación hacen referencia al tratamiento electrónico de los datos con la construcción de una base de datos a partir de las categorías de análisis previamente definidas. (Borda M.2016).

En el caso de la presente investigación para la recolección de información se utilizó la técnica de la encuesta a través del instrumento cuestionario validado y en cuanto a las técnicas de procesamiento de datos se utilizó una base de datos que facilitó la tabulación, exploración y descripción en gráficos y tablas resumidas para poder

interpretarlos. La siguiente ilustración muestra el flujo de los datos y las técnicas utilizadas:

Ilustración 4 – Flujo de datos y las técnicas utilizadas



Fuente: Elaboración propia

En el caso de la presente investigación, para garantizar la confiabilidad y seguridad de los datos el cuestionario fue cargado como un formulario en la plataforma QuestionPro. Esta plataforma esta alojada en la nube y permitió recolectar las respuestas a través de email, mensajes SMS consolidando una base de datos en la plataforma en la nube ONE Drive. El análisis estadístico de los datos se realizó utilizando las funcionalidades analíticas de QuestionPro y junto con la base de datos fueron exportados a Excel.

8. Trabajo de Campo

Teniendo presente que el enfoque metodológico de la investigación es cualitativo descriptivo basado en un instrumento debidamente validado para la recolección de datos de empresas del sector de outsourcing de servicios y soluciones TI de Bogotá y sus equipos de gestión de proyectos para estudiar su postura y acciones respecto a la seguridad de los activos de información de sus clientes, el trabajo de campo inicio identificando los datos de contacto de gerentes y líderes de proyecto de las 22 empresas que de acuerdo con su naturaleza, objeto social, oferta de servicios y domicilio registrado en Bogotá reportaron ingresos durante al corte de diciembre 31 de 2022 según el SIIS. Sistema Integrado de Información Societaria de la Superintendencia de Sociedades.

Con los datos de contacto de gerentes y/o líderes de proyecto se estableció la base de datos inicial del grupo semilla para el estudio con los 22 Gerentes y/o Lideres de Proyecto de las 22 empresas identificadas. Con esta base de datos inicial, se procedió con la definición de la invitación a participar en la investigación (Anexo B), la cual fue enviada por medio de InMail de LinkedIn desde el perfil del investigador como un mensaje personal a cada uno de los participantes identificados iniciales, explicando el propósito del estudio, la importancia de su colaboración y compartiendo el enlace para el correspondiente diligenciamiento del instrumento. A medida que los participantes iniciales referenciaban nuevos participantes la base de datos inicial se actualizaba para validación y envío, si procedía, de nuevas invitaciones.

Presupuestando que cada una de las 22 fuentes de información del grupo semilla, referenciara al menos un contacto de su red que estuviese interesado en participar y que correspondieran a la misma empresa u otras empresas con servicios similares se

esperaba realizar 44 encuestas y/o completar la cantidad mínima de 30 entrevistas requeridas en las muestras cualitativas como tamaño de la muestra o de punto de saturación. Finalmente, se consolidaron 32 respuestas al instrumento de recolección de información de la siguiente manera:

- De las 22 fuentes iniciales contactadas 19 contestaron (86,36%) y se recibieron 19 contactos referenciados.
- De estos 19 contactos referenciados 15 (73,68%) cumplieron las condiciones para ser fuentes de información y por lo tanto se les envió el mensaje personal con la invitación. Dos (2) referenciados ya estaban incluidos y los otros dos (2) no cumplían.
- De los 15 nuevos contactos, 11 contestaron (73,30%) y referenciaron 9 contactos,
- De estos 9 nuevos contactos referenciados (6) cumplieron las condiciones para ser fuentes de información y por lo tanto se les envió el mensaje personal con la invitación. Cuatro (4) contactos referenciados ya estaba incluidos. Uno (1) no cumplía.
- De estos 6 contactos referenciados, 2 contestaron (33,33%) y referenciaron 4 contactos.
- De estos 4 contactos referenciados 1 no cumplía y tres ya estaban incluidos.
- Validando que no se tenían más fuentes de información referenciadas por contactar y que se había superado las 30 encuestas definidas como punto de saturación, se consideró la finalización del trabajo de campo, pues se alcanzó el estado en el que las nuevas entrevistas a Gerentes y/o líderes de los equipos de proyecto que estuvieron o están vinculados a las 22 empresas de outsourcing de servicios y soluciones de Bogotá, Colombia identificadas, no aportan nueva información a la investigación.

8.1. Procesamiento estadístico de datos

Una vez consolidados los datos recolectados se procedió a transformarlos en información utilizable para interpretar la postura y acciones de las empresas del sector de outsourcing de servicios y soluciones TI de Bogotá y sus equipos de gestión de proyectos respecto a la seguridad de los activos de información de sus clientes. Al tratarse de una investigación cualitativa, esta transformación se realizó a través de ilustraciones y tablas relacionadas con cada una de las categorías de análisis planteadas: Actitud frente a la protección de activos de información, Enfoque metodológico frente a la protección de activos de información y Fortalecimiento de la cultura de protección de activos de información. Como herramienta de ayuda se utilizó el software estadístico XLSTAT versión libre.

8.1.1. Actitud frente a la protección de activos de información

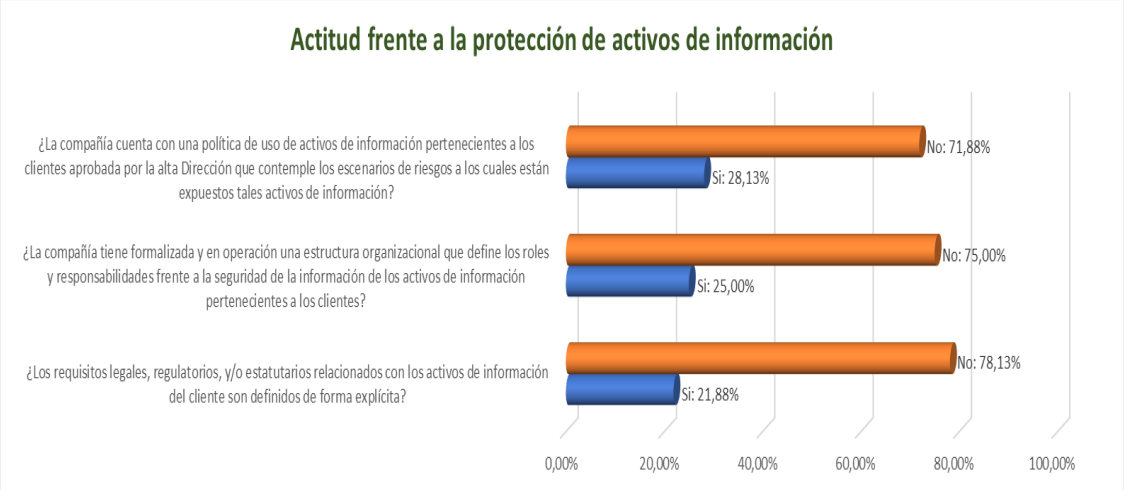
Las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, exhiben ciertas actitudes o rasgos y comportamientos colectivos que reflejan su cultura, valores y formas de operar y revelan su disposición para ofrecer a sus clientes servicios y soluciones que garanticen la confidencialidad, integridad y disponibilidad de los activos de información que los clientes les comparten o entregan debido al alcance de tal servicio o solución.

La actitud empresarial habla de la postura la organización en su conjunto frente a los retos que representan las exigencias y cambios del entorno para la sostenibilidad de la compañía e influye en cómo la empresa es percibida tanto internamente por los empleados como externamente por clientes, proveedores y el público en general. Las actitudes empresariales se pueden entender como características que describen la personalidad o la identidad de una empresa y se reconoce por los modos de organizarse,

relacionarse y posicionarse y mantenerse en el negocio (Tovar J. & Perez A. & Rodriguez A.2017).

A continuación, aparecen los resultados con respecto a la actitud de las compañías de outsourcing de servicios y soluciones TI de Bogotá, Colombia frente a la protección de activos de información de sus clientes:

Ilustración 5 – Actitud frente a la protección de activos de información



Fuente: Elaboración propia

De acuerdo con estos resultados:

- El 71,88% de las compañías de outsourcing de servicios y soluciones TI que hacen parte del estudio, no cuentan con una política de uso de activos de información pertenecientes a los clientes aprobada por la Alta Dirección que incluya los escenarios de riesgo a los cuales están expuestos tales activos de información. Solamente el 28,13% de estas compañías cuentan con esa política.
- El 75% de las compañías de outsourcing de servicios y soluciones TI que hacen parte del estudio, no cuentan con una estructura organizacional que defina los roles y responsabilidades frente a la seguridad de la información de los activos de

información pertenecientes a los clientes. Solamente el 25% de estas compañías han definido tal estructura organizacional.

- El 78,13% de las compañías de outsourcing de servicios y soluciones TI que hacen parte del estudio, no tienen definidos de forma explícita los requisitos legales, regulatorios y/o estatutarios relacionados con los activos de información pertenecientes a los clientes. Solamente el 21.88% de estas compañías han especificado tales requisitos.

8.1.2. Enfoque metodológico frente a la protección de activos de información

Existen diversos marcos de referencia, estándares y metodologías que tratan el concepto de seguridad de la información y que establecen lineamientos para proteger los activos de información. Las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, pueden utilizar estos marcos de referencia, estándares y metodologías de manera separada o en conjunto para definir un enfoque metodológico que mejor se ajuste a su escenario de negocio para proteger los activos de información. Entre los marcos de referencia, estándares y metodologías más conocidos para la gestión de la seguridad de la información están la familia de normas ISO 27000, PCI (Payment Card Industry Data Security Standard), NIST CSF (Instituto Nacional de estándares y tecnología – Marco de ciberseguridad), HITRUST CSF (Marco de Seguridad de Ciberseguridad de la Alianza de Confianza de información de salud), CSA (Cloud Control Matrix, ISF – Information Security Forum), COBIT e ITIL. (Taherdoost, H. .2022).

En términos generales, la mayoría de los marcos de referencia, estándares y metodologías para la gestión de la seguridad de la información sugieren que la organización debería considerar los aspectos de seguridad de la información tanto en sus

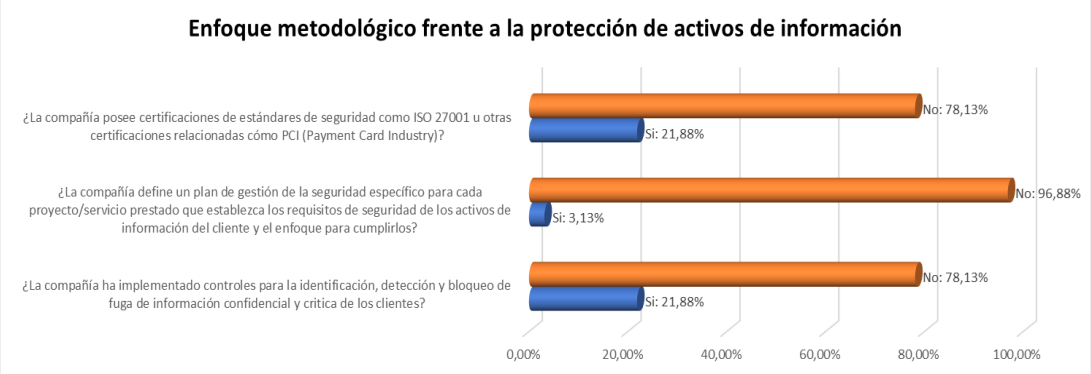
funciones y procesos internos como también en los servicios o productos que entregan a sus clientes y recomiendan, igualmente, tener presente los requisitos de seguridad de la información en proyectos. Una manera típica de demostrar que una compañía de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, cumple con alguno de estos marcos de referencia, estándares y/o metodologías es a través de una certificación de cumplimiento que de manera independiente valida que la compañía cumple con una normativa específica y que los requisitos de tal normativa están correctamente implementados. (Chauhan. M & Shiaeles S. 2023). La certificación empresarial más reconocida es la certificación ISO 27001 que refleja el compromiso de una empresa con prácticas de seguridad de la información óptimas y genera confianza en sus clientes y otras partes interesadas (AENOR s/f).

Las organizaciones que operan por proyectos para terceros, donde cada proyecto tiene su propio alcance, con un equipo y presupuesto propios y objetivos particulares, proyectos que no tienen que están relacionados entre sí, pero cuyos resultados en su conjunto ayudan alcanzar objetivos estratégicos del negocio. como es el caso de las empresas de outsourcing de servicios y soluciones TICs de Bogotá, Colombia, deberían incorporar, como buena práctica, un plan global de gestión de sus proyectos que incluya todos los aspectos del proyecto en particular o desarrollar planes individuales para cada uno de esos aspectos. Los planes son los medios a través de los cuáles se describe cómo se implementarán las políticas, procedimientos y pautas aplicables para lograr los objetivos de un proyecto y el enfoque para cumplirlos (Project Management Institute.2021) . En el caso de las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, los planes de seguridad de la información deberían describir cómo se implementarán las políticas, procedimientos y pautas de seguridad de la información y el enfoque para proteger de manera adecuada los activos de información

que les comparten o entregan sus clientes debido al alcance de tal servicio o solución, incluido los controles para identificar, detectar y bloquear posibles fugas de información confidencial y crítica de sus clientes.

A continuación, se muestra los resultados obtenidos respecto al enfoque metodológico de las compañías de outsourcing de servicios y soluciones TI de Bogotá frente a la protección de activos de información de sus clientes:

Ilustración 6 – Enfoque metodológico frente a la protección de activos de información



Fuente: Elaboración propia

De acuerdo con estos resultados:

- El 78.13% de las compañías de outsourcing de servicios y soluciones TI que hacen parte del estudio, no han obtenido una certificación en estándares de seguridad como ISO 27001 u otras certificaciones relacionadas cómo PCI (Payment Card Industry). Solamente el 21.88% de estas compañías han obtenido este tipo de certificaciones de seguridad de la información.
- El 96,88% de las compañías de outsourcing de servicios y soluciones TI que hacen parte del estudio, no han definido un plan de gestión de la seguridad específico para cada proyecto/servicio prestado que establezca los requisitos de seguridad de los

activos de información del cliente y el enfoque para cumplirlos. Solamente el 3,13% de estas compañías han definido este tipo planes de gestión de seguridad de la información.

- El 78,13% de las compañías de outsourcing de servicios y soluciones TI que hacen parte del estudio, no han implementado controles para la identificación, detección y bloqueo de fuga de información confidencial y crítica de sus clientes. Solamente el 21.88% de estas compañías han implementado tales controles.

8.1.3. Fortalecimiento de la cultura de protección de activos de información.

La cultura de protección de los activos de información se refiere a los hábitos, comportamientos y actitudes tanto individuales como colectivas de los empleados de las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, respecto a la protección de tales activos. Incluye las acciones diarias que animan a los gerentes y equipos de proyecto a conocer las amenazas y riesgos de seguridad de la información y adoptar en sus actividades diarias los controles y mecanismos para enfrentarlos y, en consecuencia, tomar decisiones reflexivas respecto a la confidencialidad, integridad y disponibilidad de los activos de información durante el ciclo de vida del proyecto. La cultura de seguridad está determinada por el liderazgo, entrenamiento y concientización que determinan cómo se espera que las personas piensen y aborden la seguridad en una organización (NCSC-National Cyber Security Center, s/f).

La cultura de protección de activos de información es una faceta de la cultura corporativa, que incentiva a los gerentes y equipos de proyecto de las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia a tomar decisiones y cumplir con sus tareas diarias garantizando la seguridad de la información. Una cultura de seguridad involucra más que solamente concientización pues requiere seguimiento y

reforzamiento de los comportameintos considerados apropiados en cuanto a la protección de los activos de información entregados y/o compartidos por los clientes. En este contexto, todos los miembros de un equipo de proyecto, incluyendo el gerente del proyecto, deben considerarse responsables de proteger los activos de información y necesitan tener claro un proceso disciplinario que defina que supone un incumplimiento de las políticas organizacionales en cuanto al manejo de los activos de información entregados o compartidos por los clientes y las consecuencias correctiva o negativas derivadas de tal incumplimiento. De igual manera, las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia podrían considerar dentro de su proceso disciplinario medidas positivas que premien el buen desempeño y cumplimiento de las responsabilidades relacionadas con la protección de los activos de información entregados y/o compartidos por los clientes como dos buenas prácticas para r incentivar y revisar la cultura de protección de los activos de información.

A continuación, se muestra los resultados obtenidos respecto Fortalecimiento de la cultura de protección de activos de información de las compañías de outsourcing de servicios y soluciones TI de Bogotá frente a la protección de activos de información de sus clientes:

Ilustración 7 – Fortalecimiento de la cultura de protección de activos de información

Fuente: Elaboración propia

De acuerdo con estos resultados:

- El 71.88% de las compañías de outsourcing de servicios y soluciones TI que hacen parte del estudio, no tienen programas de concientización y entrenamiento definidos para los equipos de proyecto/servicio que incluyan aspectos relevantes en seguridad de la información y uso adecuado de los activos de información de los clientes. Solamente el 28.13% de estas compañías han obtenido este tipo de programas.
- El 75.00% de las compañías de outsourcing de servicios y soluciones TI que hacen parte del estudio, no han definido e implementado un proceso disciplinario formal que incluya las acciones a tomar ante aquel personal que hay provocado alguna brecha de seguridad respecto a los activos de información de los clientes. Solamente el 25.00% de estas compañías han definido un proceso disciplinario formal relacionado con seguridad de la información.
- El 93.75% de las compañías de outsourcing de servicios y soluciones TI que hacen parte del estudio, cuentan con gerentes/líderes de proyecto certificados en buenas prácticas de seguridad de la información. Solamente el 6,25% no cuentan con gerentes/líderes de proyecto certificados en este tipo de prácticas.

8.2. Análisis de resultados

A continuación, se realiza la comparación de la hipótesis planteada frente a los indicadores de las categorías de análisis calculados como promedio de los resultados del procesamiento estadístico de datos obtenidos luego del trabajo de campo:

Tabla 6 – Relación categorías de análisis, indicadores y tipos preguntas

Hipótesis	Categoría de análisis	Indicador	
		Nombre	Valor
Las compañías de outsourcing de Servicios y Soluciones TI no tienen implementadas estrategias claras para gestionar los riesgos de brechas de seguridad de los activos de información de sus clientes como parte de su oferta de valor, lo que implica que los gerentes de proyectos de outsourcing de Servicios y Soluciones TI no protegen de manera adecuada los activos de información que tienen valor de negocio tanto para el proveedor de los servicios y soluciones de TI como para sus clientes, no consideren la gestión de riesgos de seguridad como una de sus áreas de interés para aplicar y no están preparados para gestionar los riesgos de seguridad de la información	CA1: Actitud frente a la protección de activos de información	Declaración en la promesa de valor a los clientes	25,00%
	CA2: Enfoque metodológico frente a la protección de activos de información	Modelos de Sistemas de Gestión de Seguridad de la Información certificados de manera independiente	15,63%
	CA3: Acciones de sensibilización de protección de activos de información desarrolladas internamente por la compañía	Acciones de sensibilización de protección de activos de información desarrolladas internamente por la compañía	19,79%

Fuente: Elaboración propia

De acuerdo con estos indicadores, se puede afirmar que en promedio:

- El 25% de las compañías de compañías de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, cuentan con los elementos necesarios para confirmar su actitud o mentalidad que se caracteriza por su disposición a asumir de manera reflexiva la protección de los activos de información de sus clientes, actitud que se manifiesta a traces de una política de uso de activos de información pertenecientes a los clientes aprobada por la alta Dirección que contempla los escenarios de riesgos a los cuales están expuestos tales activos de información, una estructura organizacional formalizada y en operación que define los roles y responsabilidades frente a la seguridad de la información de los activos de información pertenecientes

a los clientes y la definición de forma explícita de los requisitos legales, regulatorios, y/o estatutarios relacionados con los activos de información del cliente.

- El 16.63% de las compañías de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia poseen certificaciones de estándares de seguridad como ISO 27001 u otras certificaciones relacionadas cómo PCI (Payment Card Industry), definen un plan de gestión de la seguridad específico para cada proyecto/servicio prestado que establece los requisitos de seguridad de los activos de información del cliente y el enfoque para cumplirlos y han implementado controles para la identificación, detección y bloqueo de fuga de información confidencial y critica de los clientes.
- El 19,79% de las compañías de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia implementan programas de concientización y entrenamiento definidos para que sus equipos de proyecto/servicio que incluyen aspectos relevantes en seguridad de la información y uso adecuado de los activos de información de los clientes, han definido e implementado un proceso disciplinario formal, que incluye las acciones a tomar ante aquel personal que haya provocado alguna brecha de seguridad respecto a los activos de información de los clientes y cuentan con gerentes/líderes de proyecto/servicio, certificados en buenas prácticas en seguridad de la información.

De las encuestas también se obtuvieron como resultado comentarios que permiten deducir el por qué estas cifras son tan bajas:

Actitud frente a la protección de activos de información

- La gerencia considera que el tiempo que los gerentes/líderes y los equipos de proyecto dedican a la constitución de políticas y procedimientos e identificación de riesgos relacionados con seguridad de la información de los activos de información

de los clientes son muy largos y costosos y afectan de manera negativa los tiempos de entrega del proyecto y por lo tanto es necesario evitarlos.

- La gerencia considera que no es necesaria una estructura organizacional con roles y responsabilidades frente a la seguridad de la información de los activos de los clientes. Esto eleva los costos de operación de la compañía . Es responsabilidad del gerente/líder y del equipo de proyectos.
- Si los requisitos legales, regulatorios, y/o estatutarios relacionados con los activos de información del cliente no están definidos de forma explícita en el contrato y sus anexos no es necesario que el gerente/líder y el equipo de proyecto se preocupen y dediquen tiempo y recursos a esta definición. Si se incluyen puede aumentar el alcance con el mismo presupuesto del proyecto.

Enfoque metodológico frente a la protección de activos de información

- La compañía no invierte y tampoco destina presupuesto de gastos para certificarse en estándares de seguridad. Es el costo, es claro que hay que realizar una inversión y la compañía no tiene presupuesto para estas certificaciones. Cuando se requieren, la compañía busca un socio que las tenga.
- La compañía no tiene una metodología de gerencia de proyectos. No se define un plan de gestión de la seguridad específico para ningún proyecto/servicio.
- La compañía no tiene medidas de seguridad. La compañía no invierte en hardware de seguridad. Los únicos controles son las instrucciones de la gerencia. Se actúa de manera reactiva.

Fortalecimiento de la cultura de protección de activos de información

- La compañía no tiene programas de capacitación. Si el cliente no pide estas capacitaciones para el personal del proyecto la compañía no las da.

- No tenemos claro que acciones tomar cuando se presenten fallas de seguridad. Todo es reactivo y se define en el momento que suceda.
- La compañía no lo pide. El cliente no lo solicita. Como gerente/líder de proyecto/servicio, no es prioridad obtener una certificación en seguridad de la información.

8.3. Propuesta de solución a la problemática

Las compañías de Servicios y Soluciones TI de Bogotá, Colombia, tienen la oportunidad de maximizar sus beneficios de negocio priorizando la seguridad de la información de los activos de información de sus clientes dentro de su oferta de valor como una estrategia de negocio y la gerencia de proyectos como habilitador de tal estrategia puede brindarles las capacidades para lograrlo (Ortegón A. & Otros.2018). Como proveedores de TI (IT third party providers), las compañías de Servicios y Soluciones TI de Bogotá, Colombia deberían integrar la ciberseguridad y la seguridad de la información de los activos de sus clientes como un estándar de facto (Simunic D. & Pavic I. 2020), es decir, como un componente básico que se da por descontado en sus servicios y soluciones y que hace parte fundamental de su cultura organizacional, su presupuesto operativo y una práctica normal entre sus Gerentes/Líderes y equipos de proyecto.

Toda compañía de Servicios y Soluciones TI de Bogotá, Colombia debería contar con un enfoque y un plan maestro que defina el retorno de la inversión en la protección de los activos de información de sus clientes y que ayude a sus Gerentes/Líderes y equipos de proyecto a gestionar de manera positiva la protección de tales activos, ya que por más dinero que inviertan en la seguridad de la información de sus servicios y soluciones, nunca alcanzarán niveles de seguridad satisfactorios para sus clientes salvo que implementan un instrumento que les permita medir y gestionar de manera eficiente el

valor de las inversiones frente al valor de tales activos y la materialización de los riesgos asociados y no podrán hacerlo a menos que desarrollen la capacidad organizacional para proteger tales activos. Las capacidades organizacionales o las destrezas que desarrolla una organización, son activos intangibles, insustituibles, difíciles de imitar, valiosas, escasas e intransferibles y fomentan actitudes positivas como el compromiso y la motivación y se manifiestan en la forma de cooperar, interactuar y tomar decisiones tanto de los empleados como de los equipos de trabajo (Acosta J. & Otros.2017).

Una capacidad organizacional es la habilidad que tiene una empresa para utilizar de manera óptima sus recursos para lograr sus objetivos de negocio. Es la alta dirección de una organización quién determina cuáles son las capacidades de negocio que son requeridas por la empresa para entregar valor a sus clientes y obtener beneficios y se materializan en unidades o funciones del negocio y en servicios del negocio que son gobernados de manera explícita a través de directrices, resultados esperados y una estructura organizacional (The Open Group.2022). La estructura organizacional corresponde al diseño de la empresa y la manera como se distribuyen procesos, actividades tareas, roles, responsabilidades y toma de decisiones para que se alcancen los propósitos de la organización buscando la adaptación al entorno y la diferenciación en el mercado que sirven (Blanco A. & Otros. 2019).

Estos mismos elementos de gobierno son referenciados por la ISO (ISO: 2022) para un Sistema de Seguridad de la Información cuando establece en sus requisitos que la alta dirección de una organización deberá demostrar su liderazgo y compromiso con la seguridad de la información garantizando que se establezcan la política de seguridad de la información (directriz), los objetivos de seguridad de la información (resultados que se esperan) y asegurándose que las funciones, responsabilidades y autoridades de los roles

relevantes para la seguridad de la información sean designados y comunicados dentro de la organización (estructura organizacional).

En este caso, se propone que las compañías de outsourcing de Servicios y Soluciones TI en Bogotá, Colombia, desarrollen la capacidad organizacional relacionada con el fortalecimiento y mejora de la gestión de los riesgos de seguridad de los activos de información compartidos y/o entregados por sus clientes a sus equipos de proyecto dentro del alcance de tales servicios y soluciones. Los principales factores a tener en cuenta para desarrollar esta capacidad organizacional ya son ampliamente conocidos y al adoptar estas recomendaciones, los empresarios del sector del outsourcing de Servicios y Soluciones TI pueden proteger sus negocios y la reputación de sus clientes y sus activos de información:

- Cultura de seguridad
    - Las compañías de outsourcing de Servicios y Soluciones TI deberían ser conscientes de que forman parte una cadena de suministro y considerar los riesgos de seguridad de la información de los activos de los clientes y cómo mitigarlos.
    - Desde la alta gerencia de las compañías de outsourcing de Servicios y Soluciones TI se debería fomentar una cultura de seguridad que incluya a toda la organización y en especial para los equipos de proyecto respecto a los activos de información de los clientes.
    - Como parte del entrenamiento continuo, las compañías de outsourcing de Servicios y Soluciones TI deberían organizar talleres y cursos regulares para los equipos de proyecto sobre buenas prácticas de seguridad de la información, últimas amenazas y sobre cómo identificar y reportar posibles incidentes que afecten los activos de información de los clientes

- Las compañías de outsourcing de Servicios y Soluciones TI deberían realizar simulacros de ataques cibernéticos a los activos de información recibidos de los clientes para evaluar la preparación de los equipos de proyecto de outsourcing de Servicios y Soluciones TI para identificar áreas de mejora.

- Metodología de Gestión de Proyectos
  - Como un componente básico de la metodología de gestión de proyectos de las compañías de outsourcing de Servicios y Soluciones TI, se debería considerar específicamente un área de interés que incluya políticas, normativas, procedimientos y controles de seguridad relacionados con los activos de información de los clientes.
  - Los equipos de proyectos de outsourcing de Servicios y Soluciones TI deberían ampliar el análisis de riesgos e incluir la categoría de seguridad de la información para que de manera regular se identifiquen las vulnerabilidades y amenazas más importantes relacionadas con los activos de información de los clientes.
  - Las compañías de outsourcing de Servicios y Soluciones TI deberían establecer como buena práctica para la gestión de proyectos, un plan de gestión de seguridad de los activos de información de los clientes que las opciones de tratamiento de riesgos y respuesta a incidentes.
- Cumplimiento Normativo:
  - La alta gerencia de las compañías de outsourcing de Servicios y Soluciones TI deberían estar al tanto de las regulaciones de seguridad de la información aplicables a su industria y región y asegurar que sus equipos de proyecto las cumplan

- La alta gerencia de las compañías de outsourcing de Servicios y Soluciones TI deberían asegurar que se realicen auditorías regulares para garantizar el cumplimiento de requisitos normativos y del cliente, así como de los aspectos metodológicos relacionados con la adecuada protección de los activos de información de sus clientes.
- Los organismos gubernamentales, las asociaciones de industria, las compañías de outsourcing de Servicios y Soluciones TI, los equipos de proyecto y en general todos los actores públicos y privados que integran o son partes interesadas en esta cadena de suministro deberían colaborar e intercambiar información sobre amenazas y vulnerabilidades del sector y buscar articular y coordinar respuestas a los riesgos de seguridad de la información asociados que la industria ITO en Colombia.

9. Discusión

A continuación, se presenta la comparación de resultados, se señalan las limitaciones que enfrento la presente investigación, se realiza la verificación de la hipótesis y finalmente se evalúa el método de investigación utilizado.

9.1. Comparación de resultados

De acuerdo con el análisis de resultados, se procede a exponer la comparación de los resultados obtenidos en esta investigación con los antecedentes previos y las bases teóricas:

- Respecto a la actitud de las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, que hacen pare del estudio, frente a la protección de los activos de información de sus clientes, se obtuvo que el 75.00% no confirman su disposición a asumir de manera reflexiva esta protección pues no cuentan con una política aprobada por la Alta Dirección, no cuentan con una estructura organizacional que defina los roles y responsabilidades ni tienen definidos de forma explícita los requisitos legales, regulatorios y/o estatutarios relacionados con los activos de información pertenecientes a los clientes. Carpentier (2016) propone que la estrategia de servicio de un proveedor de servicios de TI, debe basarse en el hecho de que un cliente no compra productos, sino que requiere servicios que satisfagan las necesidades particulares de tales clientes y que esta estrategia debe incluir una garantía relacionada con la gestión de seguridad de la información enfocada en alinear la seguridad de la información con la actividad de negocio del cliente y asegurar que los riesgos relacionados con el manejo de la información de los cliente se gestionan eficazmente con el fin de cumplir los requisitos

contractuales. Evidentemente los resultados obtenidos no están en línea con esta propuesta.

De manera similar, el estudio de Caracterización del Sector de Teleinformática, Software y TI en Colombia 2015 del Ministerio de las Tecnologías de la información y las Comunicaciones de Colombia del MinTIC, SENA y Fedesoft (2016), no encontró referencias de que las compañías colombianas que ofrecen productos y servicios de TI consideraran la seguridad de la información como uno de los elementos clave de su gestión. Este resultado concuerda con los de la presente investigación pues la mayoría de las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, no cuentan ni con una política, ni con una estructura organizacional, ni con definiciones explícitas de los requisitos legales, regulatorios y/o estatutarios relacionados con los activos de información pertenecientes a los clientes, todos elementos básicos de un sistema de gestión relacionado con la seguridad de la información (ISO. 2022).

- Respecto al enfoque metodológico frente a la protección de activos de información, el resultado de la presente investigación arroja que 83,37% de las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, que hacen pare del estudio, no han identificado, definido e implementado un conjunto de principios y prácticas que sirvan como guía para el desarrollo de sus proyectos/servicios, pues no cuentan con alguna certificación en estándares de seguridad, no han definido un plan de gestión de la seguridad específico para cada proyecto/servicio prestado y tampoco han implementado controles para la identificación, detección y bloqueo de fugas de información confidencial y crítica de sus clientes. Baraforta (2017) propuso un modelo general que integra las actividades de gestión de riesgos con los modelos de gestión de calidad, gestión de proyectos, gestión de servicios de TI y gestión de seguridad de la información con el fin de proveer vectores de integración, como la comprensión de la

organización y su contexto, el pensamiento basado en el riesgo, el liderazgo y el compromiso, el enfoque de procesos y la estructura PDCA basado en prácticas y estándares de mercado y que sirviera de marco metodológico para las organizaciones integren las actividades de gestión de riesgos en los modelos de gestión de calidad, gestión de proyectos, gestión de servicios de TI y gestión de seguridad de la información. Evidentemente, los resultados obtenidos no están en línea con este modelo integrador basados en la gestión de riesgos.

De forma similar, Neelov (2017) encuentra que no siempre durante la planificación de un proyecto, se analiza la exposición a los riesgos de seguridad de la información y, por tanto, no se definen las medidas y controles para gestionarlos, lo que evidencia una falta de cumplimiento de estándares y normas y de cierto rigor metodológico. Este resultado concuerda con los de la presente investigación, pues la mayoría de las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, no han obtenido una certificación en estándares de seguridad, no definen un plan de gestión de la seguridad específico para cada proyecto/servicio prestado que establezca los requisitos de seguridad de los activos de información del cliente y el enfoque para cumplirlos, y no han implementado controles para la identificación, detección y bloqueo de fugas de información confidencial y crítica de sus clientes como elementos básicos de su enfoque metodológico de gestión de seguridad de la información en proyectos ITO.

Cabe señalar que el estudio Transformación con sentido digital 2022: Un nuevo ritmo en la madurez digital de Latinoamérica, de la firma de consultoría y auditoría Ernest & Young, citado por la Asociación Colombiana de Ingeniería de Sistemas – ACIS, encontró que tan solo el 29% de las empresas encuestadas contempla un programa de calidad que defina y priorice todos los dominios de información y monitoree permanentemente el estado de la información crítica, así como las acciones de remediación para mantenerla

en niveles óptimos, lo que esta en línea con los resultados de la presente investigación. (ACIS.2023)

- Respecto al fortalecimiento de la cultura de protección de activos de información, el 80.21% de las compañías de outsourcing de servicios y soluciones TI de Bogotá, Colombia, que hacen pare del estudio, no promueven acciones que estimulen, afiancen y refuercen que sus equipos de trabajo estén informados y sean proactivos en la adopción de medidas para prevenir riesgos y proteger los activos de información de los clientes, pues no implementan programas de concientización y entrenamiento definidos para sus equipos de proyecto/servicio, no han definido e implementado un proceso disciplinario formal, ni cuentan con gerentes/líderes de proyecto/servicio, certificados en buenas prácticas en seguridad de la información. Fister (2018), recomienda que, en lugar de un enfoque reactivo, las organizaciones, los gerentes de proyecto y los equipos de proyecto deberían adoptar una postura de seguridad proactiva para proteger mejor los datos de los clientes durante el ciclo de vida del proyecto/servicio. Evidentemente, los resultados obtenidos no están en línea con esta recomendación.

  De forma similar, Fister (2018) encontró que, en la práctica, se encuentra que muchos gerentes de proyecto no tienen la formación ni la experiencia en seguridad de la información y tampoco se están incorporando expertos que aporten esos conocimientos y experticia en seguridad de la información a los equipos de proyecto. Este resultado coincide con los de la presente investigación, pues la mayoría de las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, no implementan programas de concientización y entrenamiento en seguridad de la información para sus equipos de proyecto/servicio, no han definido e implementado un proceso disciplinario formal, ni cuentan con gerentes/líderes de proyecto/servicio, certificados en buenas

prácticas en seguridad de la información como elementos básicos de refuerzo de su cultura de protección de activos de información de sus clientes.

9.2. Limitaciones

Los retos no anticipados que surgieron durante el desarrollo de la presente investigación y las características que condicionan o restringen las generalizaciones de sus resultados son:

- Enfoque y alcance de la investigación: Se trata de un estudio cualitativo descriptivo, por lo que es necesario ser cuidadosos con la generalización de sus resultados. Es importante subrayar las limitaciones en la generalización al mercado del outsourcing de servicios y soluciones TI del país dado que los resultados están limitados en términos de su aplicabilidad a las compañías de Outsourcing de Servicios y Soluciones TI de Bogotá, Colombia.
- Acceso a las fuentes de información: El principal impedimento de la presente investigación tiene que ver con el acceso e identificación de las fuentes de información, pues al tratar temas sensibles como las brechas de seguridad originadas en proyectos ejecutados por proveedores de servicios y soluciones TI, y las estrategias para tratar los riesgos de seguridad de la información en este tipo de proyectos, se identificaron pocos estudios previos y una alta sensibilidad de los gerentes de proyecto que participaron respecto mantener su anonimato:
    - No hay visibilidad de un registro centralizado de brechas de seguridad en Colombia. En este caso, se utilizó como una fuente alterna de información el Boletín Técnico del DANE (Departamento Administrativo Nacional de Estadística) y el MinTIC (Ministerio de las Tecnologías de la Información y las Comunicaciones del 2022 titulado ¨Encuesta de Tecnologías de la Información y las Comunicaciones en Empresas – (ENTIC Empresas)¨.

- Los gerentes y/o líderes de proyecto no hablan abiertamente sobre las estrategias implementadas por las compañías de outsourcing de Servicios y Soluciones TI en Bogotá, Colombia, para dar tratamiento a los riesgos de Seguridad de la información en la gestión de proyectos de servicios y soluciones de TI. Si lo hacen, podrían incurrir en incumplimiento de acuerdos de la cláusula de confidencialidad de sus contratos de vinculación laboral o prestación de servicios. Frente a esta dificultad, la alternativa utilizada fue garantizar las condiciones de privacidad de los datos identificables y la total confidencialidad y no divulgación de datos personales y corporativos de los participantes.

- Población y muestra: La población se limita a las empresas de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, y la muestra considera 22 de estas empresas seleccionadas bajo la técnica de muestreo no probabilístico por conveniencia.
    - No se logró identificar un directorio y/o base de datos que de manera oficial registre y/o mantenga un censo de los Gerentes de Proyecto y/o Lideres dedicados al campo de las TICs y que posibilitara la selección de la muestra de forma probabilística, por lo que el grupo semilla para iniciar la investigación correspondió a 22 Gerentes y/o Líderes de proyecto encontrados en LinkedIn. En el formulario de la encuesta en línea se incluyó la solicitud de referenciación de la red de contactos que el encuestado consideró que están dispuestos a participar del estudio, asegurando mantener total reserva de los datos compartidos.

- Finalmente se logró registrar 32 participantes de un ideal de 44, superando el punto de saturación de 30 participantes. por lo que puede considerarse un estudio piloto.

- Sesgos en la información: Los datos suministrados por las fuentes de información, 32 participantes gerentes y/o líderes de proyecto, no pudieron ser verificados independientemente.

9.3. Verificación de la hipótesis.

Para la verificación de la hipótesis se realizó el siguiente procedimiento de contraste de hipótesis:

1. Definición de la hipótesis nula y la hipótesis alternativa
    - Hipótesis nula H0: P = 100%
        - La mayoría de las compañías de outsourcing de Servicios y Soluciones TI no tienen implementadas estrategias claras para gestionar los riesgos de brechas de seguridad de los activos de información de sus clientes como parte de su oferta de valor, lo que implica que los gerentes de proyectos de outsourcing de Servicios y Soluciones TI no protegen de manera adecuada los activos de información que tienen valor de negocio tanto para el proveedor de los servicios y soluciones de TI como para sus clientes, no consideran la gestión de riesgos de seguridad como una de sus áreas de interés para aplicar y no están preparados para gestionar los riesgos de seguridad de la información.
    - Hipótesis alternativa (Ha): Ha: P < 100%
        - La implementación de estrategias claras para gestionar los riesgos de seguridad de los activos de información de sus clientes como

parte de su oferta de valor de 22 de las compañías de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, es deficiente. Esto implica que los gerentes de proyectos de outsourcing de Servicios y Soluciones TI no protegen adecuadamente los activos de información que tienen valor de negocio tanto para el proveedor de los servicios y soluciones de TI como para sus clientes. Además, no consideran la gestión de riesgos de seguridad como una de sus áreas de interés, y no están preparados para gestionar los riesgos de seguridad de la información de dichos activos.

2. Determinación del nivel de significancia

   $\alpha = 0.05$

   - 5% es la probabilidad de rechazar la hipótesis nula cuando es verdadera.

3. Determinación del nivel de confianza

   - $1 - \alpha = 0.95$ es el Nivel de confianza, es decir, la probabilidad de no cometer el error de rechazar la hipótesis nula cuando es verdadera.

4. Resultado de la prueba

   A continuación, se presenta el resultado generado por el software estadístico XLSTAT:

   Tabla 7 – Resultado de la prueba

XLSTAT 2024.3.0.1423 - Pruebas t y z para una muestra - Comienzo: 04/16/2024 a las 10:47:19 / Final: 04/16/2024 a las 10:47:20

Datos: Libro = Basedatos Info_registrada / Hoja = Hoja1 / Rango = 'Hoja1'!$A$1:$A$3 / 2 filas y 1 columna
Media teórica: 0
Nivel de significación (%): 5

Estadísticos descriptivos:

Variable	Observaciones	Obs. con datos perdidos	Obs. sin datos perdidos	Mínimo	Máximo	Media	Desv. típica
SI	2	0	2	0,242	0,273	0,258	0,021

Prueba de normalidad:

Prueba de Shapiro-Wilk (SI):

W	1
alfa	0,05

Interpretación de la prueba:
H0: Los residuos siguen una distribución Normal.
Ha: Los residuos no siguen una distribución Normal.

Prueba t para una muestra / Prueba bilateral:

Intervalo de confianza para la media al 95%:
[0,065; 0,450]

Diferencia	0,258
t (Valor obse	17
|t| (Valor crí	12,706
GL	1
valor-p (bila	**0,037**
alfa	0,05

Interpretación de la prueba:
H0: La media es igual a 0.
Ha: La media es diferente de 0.
Puesto que el valor-p computado es menor que el nivel de significación alfa=0,05, se debe rechazar la hipótesis nula H0, y aceptar la hipótesis alternativa Ha.

Prueba t para una muestra / Prueba bilateral:

Intervalo de confianza para la media al 95%:
[0,065; 0,450]

Diferencia	0,258
t (Valor obse	17
|t| (Valor crí	12,706
GL	1
valor-p (bila	0,037
alfa	0,05

Interpretación de la prueba:

H0: La media es igual a 0.
Ha: La media es diferente de 0.
Puesto que el valor-p computado es menor que el nivel de significación alfa=0,05, se debe rechazar la hipótesis nula H0, y aceptar la hipótesis alternativa Ha.

Fuente: Resultados del software XLSTAT

La verificación estadística de los resultados de la investigación realizada determina que, si bien algunas compañías de Servicios y Soluciones TI de Bogotá, Colombia, consideran estrategias adecuadas para gestionar los riesgos de brechas de seguridad como parte de su oferta de valor, tales como actitudes, enfoques metodológicos y fortalecimiento de la cultura de protección de los activos de información que los clientes les comparten o entregan debido al alcance de tal servicio o solución, esto no constituye un punto de referencia que sirva de factor competitivo ni de incentivo que impulse a las

22 empresas de servicios y soluciones TI de Bogotá, Colombia, incluidas en el estudio a cumplir con las expectativas de una adecuada protección de los activos de información que sus clientes les confían.

Con base en los resultados obtenidos, se puede afirmar que la disposición para ofrecer servicios y soluciones de TI que garanticen la confidencialidad, integridad y disponibilidad de los activos de información de los clientes no es un estándar de industria para estas 22 compañías que garantice la uniformidad, la calidad y la seguridad en este sector TI.

A continuación, se muestran la hipótesis inicial o nula y la hipótesis alternativa que es la aceptada:

Tabla 8 – Hipótesis Inicial o Nula e Hipótesis alternativa aceptada

Hipótesis Inicial	Hipótesis ajustada
La mayoría compañías de outsourcing de Servicios y Soluciones TI no tienen implementadas estrategias claras para gestionar los riesgos de brechas de seguridad de los activos de información de sus clientes como parte de su oferta de valor, lo que implica que los gerentes de proyectos de outsourcing de Servicios y Soluciones TI no protegen de manera adecuada los activos de información que tienen valor de negocio tanto para el proveedor de los servicios y soluciones de TI como para sus clientes, no consideran la gestión de riesgos de seguridad como una de sus áreas de interés para aplicar y no están preparados para gestionar los riesgos de seguridad de la información	La implementación de estrategias claras para gestionar los riesgos de seguridad de los activos de información de sus clientes como parte de su oferta de valor de 22 de las compañías de outsourcing de Servicios y Soluciones TI de Bogotá, Colombia, es deficiente. Esto implica que los gerentes de proyectos de outsourcing de Servicios y Soluciones TI no protegen adecuadamente los activos de información que tienen valor de negocio tanto para el proveedor de los servicios y soluciones de TI como para sus clientes. Además, no consideran la gestión de riesgos de seguridad como una de sus áreas de interés, y no están preparados para gestionar los riesgos de seguridad de la información de dichos activos.

Fuente: Elaboración propia

10. Conclusiones y Trabajo Futuro

La motivación de este trabajo de investigación nace de la necesidad de confirmar un asunto de gran importancia en el ámbito de la industria ITO, como es el de la debida protección de los activos de información de los clientes por parte de los proveedores de Servicios y Soluciones TI. Una vez definida la metodología, desarrollado el trabajo de campo y realizado la discusión de los resultados, considerando la realidad de las compañías de servicios y soluciones TI de Bogotá, Colombia, en la actualidad, donde todas dependen de la gestión de proyectos para llevar a cabo la gestión empresarial, a continuación, se presentan las conclusiones y se plantean las líneas de acción para trabajos futuros.

10.1. Conclusiones

La presente investigación, encaminada a analizar las estrategias implementadas por 22 de las compañías de outsourcing de Servicios y Soluciones TI en Bogotá, Colombia, para dar tratamiento a los riesgos de seguridad de la información en la gestión de proyectos de servicios y soluciones de TI, estableció que, si bien algunas compañías consideran estrategias adecuadas para gestionar los riesgos de brechas de seguridad en los proyectos que ejecutan como parte de su oferta de valor, esto no es un factor competitivo que la mayoría de las empresas de este tipo aplique de forma generalizada, lo que evidentemente constituye la excepción más que la regla en la protección de los activos de información que tienen valor de negocio para sus clientes.

Frente a la estrategia de establecer una política de uso de activos de información pertenecientes a los clientes, aprobada por la Alta Dirección y apoyada por una estructura organizacional con roles y responsabilidades definidos en cuanto a la seguridad de la información de dichos activos, y la definición explícita de los requisitos legales, regulatorios y/o estatutarios relacionados con los activos de información

pertenecientes a los clientes que deben cumplir, se identificó que tan solo el 25% de las compañías de outsourcing de servicios y soluciones TI de Bogotá, Colombia, lo realiza, evidenciando el compromiso gerencial y el alineamiento con los objetivos de negocio.

Con relación a la estrategia de utilizar modelos de Sistemas de Gestión de Seguridad de la Información certificados de manera independiente para la gestión de riesgos de seguridad en sus proyectos, que ejecutan las compañías de outsourcing de servicios y soluciones TI de Bogotá, Colombia, se determinó que tan solo el 15.63% adoptan este tipo de guías y estándares que aportan buenas prácticas y el uso de impulsores de negocios que permiten definir y madurar la gestión de riesgos dentro de la organización. Respecto a la estrategia de preparar a sus gerentes de proyectos en la gestión de los riesgos de seguridad de la información, a través de acciones de sensibilización sobre la protección de activos de información desarrolladas internamente por las compañías de outsourcing de servicios y soluciones TI de Bogotá, Colombia, se estableció que el 19.79% de las compañías de outsourcing de servicios y soluciones TI de Bogotá, Colombia, ejecutan este tipo de estrategia para lograr que sus colaboradores se sientan comprometidos y entusiasmados con los objetivos empresariales.

Lo más en el análisis de las estrategias implementadas por las 22 compañías de outsourcing de servicios y soluciones TI en Bogotá, Colombia, para dar tratamiento a los riesgos de seguridad de la información en la gestión de proyectos de servicios y soluciones de TI fue abordar el estudio desde la vista del proveedor. Esto se debe a que la mayoría de los antecedentes investigativos están enfocados desde la visión del cliente. Por otra parte, lo que más ayudó a realizar este análisis fue que se enfocó en dos áreas fundamentales de la gestión TIC actual: gestión de proyectos y gestión de seguridad de la información. Esto permitió explorar el panorama desde un punto de vista de dirección y gobierno, y no desde un punto de vista técnico. Finalmente, cabe señalar que lo que más

dificultó la realización de este análisis fue la aplicación del instrumento, puesto que, precisamente por cuestiones de seguridad de la información, los gerentes de proyecto encuestados limitaban su participación al tratarse de revelar las estrategias que aplican sus compañías para la seguridad de la información en los proyectos a su cargo.

10.2. Trabajo futuro

A nivel mundial, en su último informe sobre Gobernanza de Seguridad de los Datos (DSG – Data Security Governance), Gartner predice que, para 2026, el 40% de las organizaciones utilizarán DSG con una alta tendencia a la tercerización para respaldar los resultados del negocio y las inversiones en seguridad de datos, frente a menos del 15% actual (Gartner, 2023). En Colombia, el panorama del outsourcing de Tecnología de la Información (ITO) es bastante prometedor, y como mercado ha mostrado un crecimiento significativo en los últimos años, llevando a que el Ministerio de Comercio, Industria y Turismo haya fijado como visión país posicionar a Colombia en 2032 como uno de los 25 principales proveedores de servicios de alto valor agregado, con ventas de USD 16.473 millones, generando más de 580.000 empleos y exportaciones de USD 2.500 millones (Colombia Productiva, s/f).

Frente a las anteriores perspectivas de crecimiento y desarrollo del Outsourcing de Tecnología de la Información (ITO), esta investigación puede continuar en las siguientes líneas de acción:

10.2.1. Académico

- Proponer modelos de formación cruzada de seguridad de la información a estudiantes de gerencia de proyectos y de gestión de proyectos a estudiantes de seguridad de la información, con énfasis en Outsourcing de Tecnología de la Información (ITO).

- Definir e incluir casos de estudio basados en Outsourcing de Tecnología de la Información (ITO) para análisis tanto de estudiantes de gerencia de proyectos como de estudiantes de seguridad de la información.

10.2.2. Gestión empresarial

- Extender el estudio para cubrir todas las empresas de outsourcing de Servicios y Soluciones TI a nivel de todo el territorio colombiano, o al menos todas las empresas de este tipo domiciliadas en Bogotá, con el fin de obtener un panorama general de las estrategias implementadas por las compañías de outsourcing de Servicios y Soluciones TI en Colombia, o en Bogotá, según sea el caso, para dar tratamiento a los riesgos de Seguridad de la información en la gestión de proyectos de servicios y soluciones de TI.
- Realizar un estudio en profundidad para determinar por qué la seguridad de la información no es considerada un factor determinante para el éxito de los proyectos que desarrollan las empresas de Outsourcing de Servicios y Soluciones TI a nivel de Bogotá, Colombia.

10.2.3. Regulación

- Identificar factores y métricas en el seguimiento de la gestión de proyectos ITO contratados por la administración pública y/o privada y su relación con la protección de los activos de información de las entidades del Estado colombiano.
- Definir un modelo de gestión de proyectos ITO que incluya la gestión de seguridad de la información como un área de interés, contribuyendo a la integralidad de la triada institucional Estado-Empresa-Academia.

10.2.4. Institucionalidad

- Evaluar el impacto que ha tenido el despliegue de la Estrategia Nacional de Ciberseguridad en el sector ITO en general y en los proyectos de tercerización de servicios y soluciones TI en particular.
- Analizar los convenios y acuerdos de cooperación con otros países y organizaciones internacionales que Colombia ha establecido para fortalecer la lucha contra el cibercrimen y mejora de la seguridad de la información y su impacto en la gestión de proyectos del sector ITO.

Referencias

Abarca & Otros (2013). *Técnicas cualitativas de investigación*. San José: Editorial Universidad de Costa Rica.

ACIS.(2023). *EY: Colombia es el país en Latinoamérica con mayor índice de madurez digital en el sector de riesgos y ciberseguridad.* Recuperado el 7 de febrero de 2025, del sitio web: https://acis.org.co/portal/content/ey-colombia-es-el-pa%C3%ADs-en-latinoam%C3%A9rica-con-mayor-%C3%ADndice-de-madurez-digital-en-el-sector-de

Acosta J. & Otros. (2017). *Las capacidades dinámicas. Desarrollos teóricos y evidencias empíricas*. Barranquilla. Editorial Universidad Simón Bolívar.

AENOR (s/f). *Seguridad y Privacidad de la Información: ISO 27001 e ISO 27701.* Recuperado el 22 de febrero de 2022, del sitio web: https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion

Aiken L. (1985). *Three Coefficients for Analyzing the Reliability and Validity of Ratings*. Educational and Psychological Measurement, 45, 131-142.

Almanza A. & Cano J. (2020). *XX Encuesta Nacional de Seguridad Informática. Lecciones aprendidas y prospectiva de futuro*. Recuperado el 22 de febrero de 2022, del sitio web: https://sistemas.acis.org.co/index.php/sistemas/article/view/107/84

Arias F. (2012). *El proyecto de investigación. Introducción a la metodología científica.* Sexta Edición. Caracas: Editorial Episteme C.A.

Axelos (s/f) *Prince2.* Sitio oficial de Prince2. Recuperado el 3 de marzo de 2021, del sitio web: https://www.axelos.com/best-practice-solutions/prince2

Baltar F. & Gorjup M. (2012). *Muestreo mixto online: Una aplicación en poblaciones ocultas.* Intangible Capital, vol. 8, núm. 1, 2012, pp. 123-149. Universitat Politècnica de Catalunya Barcelona, España

Baraforta B., Mesquidab A., Masb A. (2017). *Integrating risk management in IT settings from ISO standards and management systems perspectives*. Journal of Computer Standards & Interfaces. Volume 54, Part 3, Pages 176-185. https://doi.org/10.1016/j.csi.2016.11.010

Benazeer, S. y Otros (2023). *Identifying the Concept of Modularity in IS/IT Outsourcing Cases: Some Empirical Evidence*. In M. Khosrow-Pour, D.B.A. (Ed.), Encyclopedia of Information Science and Technology, Sixth Edition. Advance online publication. https://doi.org/10.4018/978-1-6684-7366-5.ch034

Berrueta E. (2015). *Transmisión de Información por medio convencionales e informáticos.* España. Ediciones Paraninfo

Blanco A. & Otros. (2019). *Estructuras Organizacionales y Competitividad. Una mirada a las medianas empresas*. Barranquilla: Ediciones Universidad Simón Bolívar.

Borda M. (2016). *El proceso de investigación. Visión general de su desarrollo.* Quinta reimpresión. Barranquilla: Editorial Universidad del Norte.

Boza & Otros. (2021). *Introducción a las técnicas de muestreo.* Madrid: Ediciones Pirámide

Carpentier J. (2016). *La seguridad Informática en la Pyme*. Barcelona: Ediciones ENI.

CEPAL. (s/f). *Gestión de datos de investigación*. Biblioguías - Biblioteca de la CEPAL

Chinyamurindi W. (2017). *The role of information management in project management success: narratives from entrepreneurs operating within the South African construction industry*. South African Journal of Information Management Vol. 19, No. 1. https://doi.org/10.4102/sajim.v19i1.811

Charles M., & Benson O. (2023). *Strategic Outsourcing and Firm Performance: A Review of Literature*. International Journal of Social Science and Humanities Research (IJSSHR) ISSN 2959-7056 (o); 2959-7048 (p), 1(1), 20–29.

https://doi.org/10.61108/ijsshr.v1i1.5

Chauhan M. & Shiaeles. S. (2023). *An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions.* Network 2023, 3, 422-450. https://doi.org/10.3390/network3030018

Colombia Productiva. (2023).*¿QUÉ ES EL SECTOR DE BPO, KPO E ITO?.* Recuperado el 20 de marzo del 2024 del sitio web: https://www.colombiaproductiva.com/ptp-sectores/servicios/bpo-kpo-ito

Colombia Productiva, (s/f).*BPO, KPO E ITO. Plan de Negocios*. Recuperado el 20 de marzo del 2024 del sitio web

CEPAL (S/F). *Gestión de datos de investigación.* Recuperado el 20 de marzo del 2024 del sitio web: https://biblioguias.cepal.org/c.php?g=495473&p=4398114

Corrado & Otros. (2022). *Measuring Data as an Asset: Framework, methods and preliminary estimates*. OECD Economics Department Working Papers No. 1731. Paris: De Autor

Cyber Chief Magazine. 2025. *The 2024 Cybersecurity Roadmap: Trends and Mitigations.* Ed.1. Frisco, Texas: Netwrix

Dane. (2021). *Metodología para la Cuenta Satélite de Tecnologías de la Información y las Comunicaciones (CSTIC).* Bogotá: De autor.

Dane. (2024). *Cuenta satélite de las tecnologías de la información y las comunicaciones (CSTIC) - Información 2021 – 2023.* Recuperado el 21 de marzo de 2024 del sitio web: https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-satelite/cuenta-satelite-de-las-tecnologias-de-la-informacion-y-las-comunicaciones-tic

DANE y MinTIC. (2022). *Boletín Técnico - Encuesta de tecnologías de la información y las comunicaciones En empresas - ENTIC Empresas 2020.* Bogotá: De autor

Davidson J. (2005). *La nueva dirección de proyectos*. Buenos Aires: Ediciones Granica S.A

Deloitte. (2016). *La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información. Encuesta 2016 sobre Tendencias de Ciber-Riesgos y Seguridad de la Información en Latinoamérica.* Recuperado el 22 de febrero de 2022, del sitio web: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk

DNP.(2024). *El Gobierno del Cambio presenta la Estrategia Nacional Digital 2023-2026.* Recuperado el 8 de febrero de 2025, del sitio web: https://www.dnp.gov.co/Prensa_/Noticias/Paginas/gobierno-del-cambio-presenta-estrategia-nacional-digital-2023-2026.aspx

DNP. (s/f). *Dirección de Desarrollo Digital- Documentos CONPES-Confianza y Seguridad.* Recuperado el 8 de febrero de 2025, del sitio web: https://www.dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx

EAN. (2022). *Campo, grupos y líneas de investigación en la universidad EAN.* Recuperado el 22 de febrero de 2022, del sitio web: https://universidadean.edu.co/investigacion/grupos-de-investigacion

ESET. (2019). *ESET SECURITY REPORT Latinoamérica 2019*. Recuperado el 22 de febrero de 2022, del sitio web: https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf

Fabregues S. (2016).*Técnicas de investigación social y educativa.* Madrid: Editorial Oberta UOC Publishing, SL.

Fedesoft. (s/f). *Directorio de Afiliados*. Recuperado el 14 de mayo de 2022, del sitio web: https://fedesoft.org/directorio/

Fedesoft. (2019). *Caracterización y evolución del sector TI 2016-2018*. Bogotá: De Autor.

Fister Gale, S. (2018). *Under Lock and Key: There's Mounting Pressure to Ensure Data Safety; but Project Teams Must Manage Risk and New Requirements.* Journal Project Management Institute PM Network, 32(10), páginas 54–61

Flores F. & Mora R. (2023). *Investigación Cualitativa.* Primera Edición. Lima: Editorial Universidad Nacional de Educación Enrique Guzmán y Valle

Gartner. (s/f). *Bimodal Definition. Information Technology Glossary*. Recuperado el 4 de marzo del 2024 del sitio web: https://www.gartner.com/en/information-technology/glossary/bimodal

Gartner. (s/f). *IT Outsourcing Definitión. Information Technology Glossary.* Recuperado el 20 de marzo del 2024 del sitio web: https://www.gartner.com/en/information-technology/glossary/it-outsourcing

Gartner. (s/f). *Magic Quadrant de Gartner.* Recuperado el 4 de febrero del 2024 del sitio web: https://www.gartner.es/es/metodologias/magic-quadrant

Gartner. (2023). *Data Security Governance Must Balance Outcomes and Risks.* Stanford: De autor.

Gil J. (2016). *Técnicas e instrumentos para la recogida de información.* Madrid: Editorial UNED

Google Cloud. (s/f). *¿Qué es cloud computing?.* Recuperado el 10 de marzo de 2024. Del sitio web: https://cloud.google.com/learn/what-is-cloud-computing?hl=es

Grand View Research. (2023). *Market Analysis Report: IT Services Outsourcing Market Size, Share & Trends Analysis Report By Service (Application Services, Emerging Technology Services, Others), By Location (On-shore, Off-shore), By End-use, By Region, And Segment Forecasts, 2023 – 2030*. San Francisco: De Autor

Harrack M. (2021). *Cybersecurity Risks in Outsourcing Strategies.* Academia Letters, Article 4161. https://doi.org/10.20935/AL4161

Hernández A. & Otros. (2018). *Metodología de la investigación científica.* Primera Edición. Alicante: Editorial Área de Innovación y Desarrollo S.L.

Hernández-Sampieri R.& Mendoza C. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. Primera Edición. Ciudad de México: Editorial McGraw Hill.

Hernández R. & Otros (2006). *Metodología de la Investigación.* Cuarta Edición. México DF: Editorial McGraw Hill.

Hurtado F. (2011*). Dirección De Proyectos: Una Introducción Con Base En El Marco Del PMI.* Bloominton: Editorial Palibrio

Hope J. & Player S. (2012). *Mejores Prácticas de Gestión Empresarial.* Barcelona: Profit Editorial

IBM (s.f.). *¿Cuánto le costaría a su empresa una brecha de seguridad de datos?* Recuperado el 22 de febrero de 2022, del sitio web: https://www.ibm.com/pe-es/security/data-breach

INCIBE -Instituto Nacional de Ciberseguridad de España. (s/f). *Protección de la Información. Colección Protege tu Empresa*. Madrid: De autor.

INCIBE - Instituto Nacional de Ciberseguridad de España. (2022). *Guía de Ciberseguridad*. Madrid: De autor.

ISO. (2012). ISO 21500 – *Directrices para la Dirección y Gestión de Proyectos*. Suiza: De autor

ISO. (2017) ISO 10006-*Sistemas de Gestión de la Calidad*, *Directrices para la Gestión de la Calidad en los Proyectos*. Suiza: De autor

ISO. (2018). ISO 27000 *Sistemas de Gestión de Seguridad de la Información- Visión general y vocabulario*. Suiza: De autor

ISO. (2022). ISO 27001 *Sistemas de Gestión de Seguridad de la Información- Requisitos*. Suiza: De autor

Kaspersky (s.f.). *¿Qué es una brecha de seguridad?* Recuperado el 22 de febrero de 2022, del sitio web: https://www.kaspersky.es/resource-center/threats/what-is-a-security-breach

Kapersky (2022). *IT Security Economics Annual Report*. Londres: De autor.

Malvaceda E. & Otros. 2023. *La investigación cualitativa, sus aportes teóricos, metodológicos y prácticos.* Bogotá: Ediciones UCC

Mejía J. (2000). *El muestreo en la Investigación Cualitativa*. Revista Investigaciones Sociales. Año IV. Número 5. Junio 2000. Páginas 165 a 180. Recuperado el 3 de marzo de 2022 del sitio web: https://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/inv_sociales/n5_2000/a08.pdf

MinTIC, SENA y FEDESOFT. (2016). *Caracterización del Sector Teleinformática, Software y TI en Colombia 2015.* Bogotá: Mesa del Sector de Teleinformática, Software y TI en Colombia, SENA

MinTIC. (2023). *Gobierno Nacional atiende ataque cibernético que afecta a varias entidades e instala PMU CIBER*. Recuperado el 5 de febrero de 2025 del sitio web: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/278831:Gobierno-Nacional-atiende-ataque-cibernetico-que-afecta-a-varias-entidades-e-instala-PMU-CIBER

MinTIC. (2023). *Resolución 1978 de 2023 Ministerio de Tecnologías de la Información y las Comunicaciones. Anexo.* Bogotá. De Autor.

MinTIC.(s/f). *MSPI.* Recuperado el 5 de febrero de 2025 del sitio web: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Miranda J. (2006). *El desafío de la Gerencia de Proyectos*. Segunda Edición. Bogotá: MM Editores.

NCSC-National Cyber Security Center. (s/f). *Cyber Security Toolkit for Boards- Developing a positive cyber security culture.* Recuperado el 18 de noviembre de 2023 del sitio web: https://www.ncsc.gov.uk/collection/board-toolkit/developing-a-positive-cyber-security-culture

Neelov K. (2017). *Considerations for Information Security in Projects*. PM (Project Management) World Journal. Vol. VI, Issue X. November 2017. Páginas 25-27. Recuperado el 3 de marzo de 2024 del sitio web: https://pmworldlibrary.net/wp-content/uploads/2017/11/pmwj64-Nov2017-Kar-Information-Security-in-Projects-second-edition.pdf

Ortega. (2024). *Ciberseguridad: Manual Práctico.* Bogotá: Ecoe Ediciones

Ortegón A. & Otros. (2018). *La gerencia de proyectos como impulsor de la estrategia organizacional*. 1ª. Edición. Bogotá. Ediciones EAN

Pang G. (2020). *Adaptation of Information Security in the Agile World,* ISACA. Journal / Issues / 2021 / Volume 1 / 31 December 2020. Pages 29 a 46.

PMI (s/f). *Breve Historia del PMI- Página oficial del Project Management Institute*. Recuperado del sitio web: https://www.pmi.org

Piattini M. & Ruiz F. (2021). *Gobierno y Gestión de las Tecnologías y Sistemas de Información.* 1ª. Edición. Bogotá: Ediciones de la U.

Polgar & Thomas. (2021). *Introducción a la investigación en ciencias de la salud.* Séptima Edición. Barcelona: Editorial: El Sevier España.

Portafolio (2020). *Cifras de ciberseguridad en Colombia prenden alarmas al cierre de 2020.* Sección Tendencias. Diciembre 10 De 2020. Recuperado del sitio web: https://www.portafolio.co/tendencias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020-547412

Project Management Institute. (2021). *Guía de los Fundamentos para la Dirección de Proyectos (Séptima Edición).* Pennsylvania: De autor.

Quispe A. (2013). *El uso de la encuesta en ciencias sociales.* Primera Edición. Tlaxcala: Editorial Diaz de Santos

Romero M, Figueroa G, Álava J y otros (2018). *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades*. Alicante: Editorial Área de Innovación y Desarrollo.

Ruiz, E. (2017). *Nuevas Tendencias en los Sistemas de Información.* Madrid: Editorial Universitaria Ramón Areces

Salazar M. (2013). *Sobre conceptos y las categorías de análisis*. Santo Domingo: Editorial Mediabyte

Sanjuán L. (2019). *Introducción a la Metodología Cualitativa de Investigación*. Primera Edición. Barcelona: Oberta UOC publishing

Seymour, T., & Hussein, S. (2014). *The History Of Project Management.* International Journal of Management & Information Systems (IJMIS), 18(4), 233-240. https://doi.org/10.19030/ijmis.v18i4.8820

Simunic D. & Pavic I. (2020). *Standards and Innovations in Information Technology and Communications*. Cham: Springer Nature Switzerland AG

Supó J. (2013). *Como validar un instrumento. La guía para validar un instrumento en 10 pasos.* Lima: Biblioteca Nacional del Perú.

The Open Group. (2022). *TOGAF® Standard, 10th Edition*. United Kingdom: De Autor

Taherdoost, H. (2022). *Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview*. Electronics 11, no. 14: 2181. https://doi.org/10.3390/electronics11142181

Tovar J. & Perez A. & Rodriguez A.(2017). *El concepto de personalidad de la empresa: Antecedentes conceptuales y examen crítico.* Cuadernos Hispanoamericanos de Psicología, 16(1), 17–28. https://doi.org/10.18270/chps.v16i1.1966

Universidad EAN. (2020). *Lineamientos para la presentación y evaluación de los trabajos de grado para los programas de Maestría*. Bogotá: De Autor.

United Nations. (2023). *Terms of Reference for the Task Force on Hard-to-Reach Groups in Administrative Sources*. Economic Commission for Europe. Conference of European Statisticians. Cardiff, UK, 9-10 October 2023.

Van Der Heijden Amber, Broasca Cosmin, Serebrenik Alexander (2018). *An empirical perspective on security challenges in large-scale agile software development*. ACM (Association for Computing Machinery) Digital Library. ESEM '18: Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement. October 2018. Article No.: 45. Pages 1-4 https://doi.org/10.1145/3239235.3267426

Toro F. (2012). *Administración de Proyectos de Informática*. Bogotá: Ecoe Ediciones.

Whelen T. & Hunger J. (2007). *Administración estratégica de negocios*. México. Pearson Education.

Wittkop, J. (2016). *Building a Comprehensive IT Security Program: Practical Guidelines and Best Practices*. New York: Apress.

World Economic Forum. (2023). *La gestión de riesgos es para todas las empresas, no solo las gigantes.* Recuperado el 5 de febrero de 2025 del sitio web: https://es.weforum.org/stories/2023/09/la-gestion-de-riesgos-es-para-todas-las-empresas-no-solo-las-gigantes/

Yong W.& Otros. (2024). *Managing partial outsourcing on information security in the presence of security externality, Expert Systems with Applications*. Volume 246, 2024 https://doi.org/10.1016/j.eswa.2023.123003

Anexo A. Cuestionario utilizado para la recolección de datos e información.

https://questionpro.com/t/AXeGcZxO

Investigación de Gestión de Proyectos

Lógica Ajustes

Reciba un cordial saludo del grupo de investigación de Gestión de Proyectos de la Universidad EAN de Colombia. Actualmente nos encontramos realizando un estudio sobre modelos, metodologías y sistemas en gestión aplicados por las compañías que ofrecen outsourcing de servicios y soluciones TI en Bogotá. Como miembro de los equipos de gerencia de proyectos de estas compañías nos gustaría contar con su ayuda mediante el diligenciamiento de la presente encuesta.

Instrucciones:
A continuación, encontrará una seria de preguntas relacionadas con la gestión de riesgos de seguridad de la información de los activos de información propiedad de los clientes. Agradecemos las responda de la manera más sincera y honesta marcando las casillas de SI o NO y agregue los comentarios que crea pertinentes.
Si considera que uno de sus contactos este interesado en contestar esta misma encuesta, por favor diligencie la casilla correspondiente al final de este formulario. Garantizamos que tanto sus datos como los de su contacto permanecerán anónimos.
Muchas gracias por su valiosa colaboración.

	Pregunta	SI	NO	Comentarios
Actitud frente a la protección de activos de información				
	¿La compañía cuenta con una política de uso de activos de información pertenecientes a los clientes aprobada por la alta Dirección que contemple los escenarios de riesgos a los cuales están expuestos tales activos de información?			
	¿La compañía tiene formalizada y en operación una estructura organizacional que define los roles y responsabilidades frente a la seguridad de la información de los activos de información pertenecientes a los clientes?			
	¿Los requisitos legales, regulatorios, y/o estatutarios relacionados con los activos de información del cliente son definidos de forma explícita?			
Enfoque metodológico frente a la protección de activos de información				
	¿La compañía posee certificaciones de estándares de seguridad como ISO 27001 u otras certificaciones relacionadas cómo PCI (Payment Card Industry)?			
	¿La compañía define un plan de gestión de la seguridad específico para cada proyecto/servicio prestado que establezca los requisitos de seguridad de los activos de información del cliente y el enfoque para cumplirlos?			
	¿La compañía ha implementado controles para la identificación, detección y bloqueo de fuga de información confidencial y critica de los clientes?			

Fortalecimiento de la cultura de protección de activos de información			
¿Existen programas concientización y entrenamiento definidos para que los equipos de proyecto/servicio que incluyan aspectos relevantes en seguridad de la información y uso adecuado de los activos de información de los clientes?			
¿Se ha definido e implementado un proceso disciplinario formal, que incluya las acciones a tomar ante aquel personal que haya provocado alguna brecha de seguridad respecto a los activos de información de los clientes?			
¿Como gerente/líder de proyecto/servicio, cuenta con certificaciones relacionadas con buenas prácticas en seguridad de la información?			