# Papel de las tecnologías disruptivas en la ocurrencia de delitos dentro de la cadena logística

Diego Fernando Pinzón Poveda

Linda Bibiana Rocha
Director

Universidad Abierta y a Distancia (UNAD)

Escuela de Ciencias Básicas Tecnología e Ingeniería

Especialización en Gerencia de Procesos Logísticos en Redes de Valor

Monografía de grado

2025

**Resumen**

En los últimos años, las tecnologías han logrado amplios desarrollos, que, impulsados por la globalización, han sido adoptados por las empresas para no sucumbir ante los cambios del mercado, buscando lograr ventajas que les permitan posicionarse y permanecer vigentes en un ámbito cada vez más competido, especialmente en procesos relacionados con los clientes como la logística y la cadena de abastecimiento, ya que de estas depende que se cumpla con los compromisos adquiridos con los *stakeholders* en los términos acordados.

El objetivo de esta monografía es analizar el papel de las tecnologías disruptivas en la ocurrencia de delitos dentro de la cadena logística en el ámbito organizacional, considerando los riesgos que se producen actualmente y que afectan el desarrollo de las actividades de la empresa, a partir de un enfoque cualitativo con alcance descriptivo e instrumentos de recolección de información constituidos por la consulta en fuentes documentales, medios de comunicación, artículos y trabajos de investigación relacionados con el tema, así como entrevistas a expertos.

Se aborda un tema actual derivado del riesgo por el uso de tecnologías disruptivas, las cuales son cada vez mayores y cercanas a todo público, especialmente si se tiene en cuenta que la delincuencia aprovecha estos instrumentos con el interés de obtener beneficios económicos sin considerar los daños que ocasiona por el robo de información y la usurpación de procesos.

*Palabras clave:* ciberdelito, información, logística, riesgo, seguridad, tecnologías disruptivas.

## Abstract

In recent years, technologies have achieved extensive developments, which, driven by globalization, have been adopted by companies so as not to succumb to market changes, seeking to achieve advantages that allow them to position themselves and remain current in an increasingly competed, especially in processes related to customers such as logistics and the supply chain, since compliance with the commitments acquired with the stakeholders in the agreed terms depends on these.

The objective of this monograph is to analyze the role of disruptive technologies in the occurrence of crimes within the logistics chain in the organizational sphere, considering the risks that currently occur and that affect the development of the company's activities, based on a qualitative approach with a descriptive scope and information collection instruments constituted by consulting documentary sources, media, articles and research papers related to the subject, as well as interviews with experts.

A current issue derived from the risk of the use of disruptive technologies is addressed, which are increasing and close to all public, especially if one takes into account that crime takes advantage of these instruments in the interest of obtaining economic benefits without considering the damage. caused by the theft of information and the usurpation of processes.


*Keywords:* cybercrime, information, logistics, risk, security, disruptive technologies.

# Tabla de Contenido

# Lista de Figuras

## Introducción

Las tecnologías disruptivas se refieren a transformaciones significativas que alteran de manera radical los procesos establecidos en diversos ámbitos, como resultado de la aparición o implementación de innovaciones tecnológicas. Estas tecnologías generan cambios sustanciales en la producción, gestión y prestación de bienes y servicios, modificando los modelos tradicionales de operación. Entre las más representativas se encuentran el internet móvil, el almacenamiento en la nube, el internet de las cosas (IoT), la robótica, la inteligencia artificial (IA), la realidad virtual y aumentada, la impresión 3D, los vehículos autónomos y las energías renovables, estas últimas orientadas hacia un futuro más sostenible (Espinel Abogados, 2022).

El presente estudio se fundamenta en los riesgos emergentes que acompañan la adopción de tecnologías disruptivas en los entornos organizacionales. Si bien estas herramientas buscan optimizar la administración, la gestión operativa y los procesos empresariales, también pueden generar amenazas que deben ser identificadas y gestionadas para alcanzar los resultados esperados por las organizaciones.

Cabe anotar que la importancia alcanzada por las tecnologías disruptivas se debe a su amplia aplicación en diferentes campos, incidiendo tanto en la generación de conocimiento como en la rápida obsolescencia para las tecnologías previas, debido a los cambios acelerados que se presentan en el contexto vigente y en los que además se transforman paradigmas existentes para responder de manera efectiva a las necesidades de la sociedad, considerando que cada día surgen nuevos campos en los que la innovación en tecnologías se convierten en la solución adecuada.

En el sector logístico, las tecnologías disruptivas se implementan con el propósito de mejorar la satisfacción del cliente final, mediante la automatización y simplificación de los procesos asociados a la cadena de abastecimiento. Estas herramientas permiten optimizar las

condiciones laborales, mejorar la ejecución de actividades operativas y ofrecer ventajas competitivas que favorecen el posicionamiento en el mercado.

La denominada cuarta revolución industrial ha impactado profundamente la logística, transformando los modelos de negocio y los sistemas de distribución. Las exigencias actuales de velocidad, precisión y calidad en la cadena de suministro demandan sistemas logísticos más eficientes, basados en la interconectividad de la información, la optimización del tiempo y el uso racional de los recursos. Este proceso implica inversiones significativas en innovación y desarrollo para alcanzar niveles superiores de competitividad (CEPAL, 2021)

La digitalización de procesos, masificación y difusión de tecnologías entre las que se encuentran el "*blockchain*, el internet de las cosas (IoT), la realidad aumentada y la inteligencia artificial (AI)" (Barleta et al., 2019); han abierto nuevas perspectivas para la transformación de la logística. No obstante, también han generado brechas significativas entre quienes tienen acceso a estas herramientas y quienes no, especialmente en lo relativo a la seguridad, donde las tecnologías juegan un papel determinante.

El desarrollo teórico del tema evidencia un creciente interés por parte de diversos autores, quienes han abordado su aplicación en múltiples disciplinas. La prospectiva tecnológica apunta a un avance acelerado que puede favorecer o comprometer la seguridad informática. En este marco, el objetivo de la presente investigación es analizar el papel de las tecnologías disruptivas en la ocurrencia de delitos dentro de la cadena logística organizacional, considerando los riesgos que podrían afectar el desarrollo de las operaciones logísticas.

Para ello, se propone contextualizar los fundamentos teóricos relacionados con la cadena de valor, las tecnologías disruptivas y la ciberseguridad; describir el alcance de los ciberdelitos

en el ámbito logístico; y examinar las estrategias implementadas por las autoridades competentes en Colombia para prevenir el ciberdelito mediante el uso de tecnologías disruptivas.

La estructura del trabajo contempla, en primer lugar, una revisión conceptual y estado del arte sobre las tecnologías disruptivas; en segundo lugar, su aplicación en el sector empresarial, con énfasis en la logística; y finalmente, el análisis de los riesgos asociados a la seguridad en la cadena de abastecimiento, derivados del uso de dichas tecnologías.

Cabe señalar que este trabajo surge del conocimiento y experiencia del autor como integrante de la Fuerza Pública, así como de los aprendizajes adquiridos en el marco de la Especialización en Gerencia de Procesos Logísticos en Redes de Valor, cursada en la Universidad Nacional Abierta y a Distancia (UNAD).

## Fundamentos teóricos asociados a la cadena de valor, tecnologías disruptivas y ciber seguridad

Este capítulo hace referencia a las definiciones y conceptos que hacen parte de la cadena de valor y que asocian a las tecnologías disruptivas como una forma para proporcionar seguridad a los procesos logísticos, pero también se configuran como un factor de riesgo para quienes los adoptan, principalmente por las necesidades que presenta el contexto empresarial actual.

El desarrollo tecnológico ha generado una creciente dependencia de sus avances, los cuales se han integrado de manera progresiva en la vida cotidiana, profesional y empresarial. A este fenómeno se suma la globalización, que, con todas sus implicaciones, ha impulsado una serie de transformaciones, entre ellas el predominio del dominio tecnológico, considerando que "en la actualidad no se concibe, ni es posible la integración de los mercados, ni la competitividad en los mismos sin el desarrollo, intercambio y uso de la tecnología" (Globalización.com, s.f).

En la actualidad, se experimenta una etapa de acelerado crecimiento tecnológico que transforma de manera profunda múltiples dimensiones de la vida social. Este fenómeno conlleva modificaciones sustanciales en los sistemas de producción, en las dinámicas empresariales, en los modelos educativos y, en términos generales, en el estilo de vida de la sociedad contemporánea. En este contexto, las tecnologías disruptivas abren nuevos panoramas al impulsar la creación de productos y servicios innovadores, mientras provocan la obsolescencia de tecnologías existentes, así como de estrategias tradicionales de negocio e investigación y desarrollo (I+D).

Además, las tecnologías ofrecen ventajas que permiten a las empresas incrementar su competitividad mediante la reducción de costos, la disminución de los tiempos de entrega y la optimización de la calidad, entre otros aspectos fundamentales en el contexto de un mercado

globalizado. El concepto de tecnologías disruptivas fue introducido por Clayton Christensen en su artículo "*Disruptive Technologies: Catching the Wave*" donde se analiza cómo ciertas innovaciones pueden transformar radicalmente industrias establecidas. Ejemplos contemporáneos de estas tecnologías incluyen la impresión 3D, el blockchain, la robótica, el Internet de las Cosas (IoT), la computación en la nube, la inteligencia artificial y los drones (Pérez, 2019, párr.3).

No obstante, los espacios que abre la digitalización también generan riesgos para las empresas en diversas áreas, incluida la logística. Si bien este proceso ofrece beneficios significativos en términos de optimización operativa, también plantea nuevos desafíos relacionados con la protección de datos y la seguridad de los procesos. Uno de los ámbitos que más ha capitalizado el uso de tecnologías en los últimos años (impulsado por fenómenos como la pandemia) es la cadena de suministro, que abarca desde la adquisición de materias primas e insumos, su transformación en productos, hasta su distribución final al consumidor (Centro Europeo de Posgrado México, 2021)

De acuerdo con Gutiérrez (2019), durante el Congreso AECOC de Supply Chain, el director de Operaciones Logísticas de Carrefour destacó la relevancia de la comunicación interna en la compañía y el papel que desempeñan las herramientas digitales en su optimización. Señaló que el entorno ha cambiado de forma significativa: anteriormente, el canal más ágil era el correo electrónico, mientras que actualmente predominan redes como los grupos de WhatsApp. En este contexto, dentro de las operaciones logísticas, un cliente puede reportar novedades mediante el envío inmediato de una fotografía de un producto en mal estado. Sin embargo, este tipo de canales también conlleva riesgos, como la posible filtración de información sensible que podría comprometer la seguridad y el funcionamiento de la organización. (Gutiérrez C. , 2019).

Los expertos en ciberseguridad, como el coordinador de servicios de inteligencia de la firma Cipher, advierten que “lo primero que hay que tener en cuenta es la concienciación de que una fuga de información puede suponer una gran pérdida económica o de reputación” (Gutiérrez C. , 2019), En este sentido, se destaca que, según estimaciones de McAfee, el ciberdelito representa actualmente un coste global superior a los 800.000 millones de euros, lo que equivale a más del 1 % del PIB mundial.

Esta situación resulta especialmente alarmante si se consideran los alcances que pueden lograrse con la aparición constante de tecnologías disruptivas. Aunque estas representan factores clave para mejorar la competitividad empresarial, también exigen el desarrollo de mecanismos que fortalezcan la seguridad de las operaciones, evitando vulneraciones a través de los sistemas tecnológicos.

En este sentido, países como España han incrementado sus inversiones en ciberseguridad. Según el *Hiscox Cyber Readiness Report* 2019, citado por Gutiérrez (2019), “las empresas del sector en España dedican el 12,6 % de su presupuesto anual de tecnologías de la información a ciberseguridad, cuatro décimas por encima de la media de las compañías logísticas en los países analizados por Hiscox”. Esta tendencia se justifica por estimaciones que indican que el ciberdelito representa un coste global cercano a los 542.000 millones de euros (Gutiérrez C. , 2019).

## Estado del arte

Diversas investigaciones han abordado el estudio de las tecnologías disruptivas. Entre ellas destaca el artículo “Introducción a la Tecnología Disruptiva y su Implementación en Equipos Científicos” (Matovelle y Dabirian, 2015) en el que se describe el concepto, su

evolución histórica y sus aplicaciones en el ámbito científico, particularmente en el desarrollo de instrumentación de bajo costo mediante tecnologías como impresoras 3D, microprocesadores y unidades ópticas.

En el ámbito nacional, Dimaté y Rubio (2019), analizan las ventajas de las tecnologías emergentes aplicadas a la innovación y optimización del proceso logístico terrestre en el tramo Bogotá–Villavicencio. Su estudio considera las dificultades recurrentes en el transporte de carga, derivadas de derrumbes e inestabilidad del terreno, que afectan directamente a las empresas transportadoras. Estas condiciones inciden en la toma de decisiones orientadas a la reducción de costos, la mejora en los tiempos de entrega y la disminución de errores humanos mediante el uso de herramientas como Big Data, IoT, realidad aumentada y sistemas de conducción autónoma.

En el artículo “Transformación digital en la logística de América Latina y el Caribe” (Valdés y Pérez, 2020) se aborda el papel de las tecnologías disruptivas en el sector transporte y se enfatiza la relevancia de incorporar la transformación digital en este ámbito. Los autores destacan que, ante las exigencias del contexto actual (marcado por una economía y un comercio globalizado), resulta indispensable contar con sistemas logísticos fluidos, seguros y resilientes, apoyados en herramientas digitales que faciliten la trazabilidad y la eficiencia operativa.

Por su parte, Carvajalino (2020) analiza el crecimiento del comercio electrónico y las transformaciones que este ha generado en la logística de distribución, especialmente en lo que respecta a la necesidad de una trazabilidad más rigurosa que garantice altos niveles de confiabilidad. En este marco, profundiza en las tecnologías emergentes y las principales tendencias asociadas a la logística 4.0, orientadas al seguimiento de la mercancía en función de su seguridad. El estudio se fundamenta en una revisión bibliográfica de documentos especializados sobre herramientas tecnológicas aplicadas al rastreo de carga, destacando el uso

de soluciones como el Internet de las Cosas (IoT), Big Data, blockchain, computación en la nube y sensores inteligentes

Zúñiga (2020) realizó una revisión en la que analiza el papel de las tecnologías 4.0 en el contexto logístico postpandemia, destacando el interés generado por el impacto del COVID-19 y las nuevas exigencias que enfrentan las economías y las cadenas de abastecimiento en el comercio internacional. En este sentido, el aprovechamiento de las herramientas propias de la cuarta revolución industrial permite a las empresas replantear sus estructuras logísticas, adaptándolas a entornos más dinámicos, resilientes y tecnológicamente integrados.

Esta perspectiva se complementa con el estudio de Campos y Pérez (2021) quienes examinan las ventajas y desafíos que presentan los vehículos autónomos en los procesos de logística de carga. Los autores identifican oportunidades relevantes, especialmente en el ámbito ambiental, como la reducción de emisiones contaminantes derivadas de las actividades de transporte. Asimismo, destacan el potencial de estas tecnologías para contribuir a la superación de brechas estructurales en América Latina, tanto en infraestructura vial como en capacidades digitales, lo que resulta clave para avanzar hacia una logística más sostenible e inteligente.

Díaz (2021) analiza los cambios generados por las tecnologías emergentes de la cuarta revolución industrial y las transformaciones aceleradas por la pandemia del COVID-19 en los procesos de producción, exportación e importación en América Latina y el Caribe. Estas modificaciones responden a las necesidades surgidas durante el aislamiento, que obligaron a las organizaciones a establecer filiales virtuales bajo la modalidad de trabajo remoto. En este contexto, también se intensificaron las amenazas a la ciberseguridad, evidenciadas en el incremento de los ciberataques y en la afectación directa a las actividades logísticas de la región.

**Innovación, tecnologías, teorías y oportunidad**

El Centro Superior de Estudios de la Defensa Nacional (CESEDEN) en España sostiene que “la innovación es fundamental para la evolución y el progreso de la sociedad” (Centro Superior de Estudios de la Defensa Nacional, 2015). Esta afirmación cobra especial relevancia en el contexto organizacional, donde la apertura al cambio se convierte en una condición indispensable para la supervivencia institucional. Aquellas entidades que se resisten a adaptarse corren el riesgo de quedar rezagadas frente a aquellas que incorporan las transformaciones e innovaciones que surgen en los distintos ámbitos sociales, especialmente en el tecnológico.

Las tecnologías disruptivas, entendidas como “una innovación que ayuda a crear una nueva red de valor” (2015) generan impactos significativos en los entornos donde se implementan, con consecuencias tanto positivas como negativas, según el enfoque adoptado. En este escenario, las organizaciones deben orientar sus esfuerzos e inversiones (intelectuales y materiales) no solo al fomento de la innovación, sino también al fortalecimiento de sus capacidades de protección frente a los riesgos emergentes que estos nuevos escenarios tecnológicos implican.

La Teoría de la Oportunidad establece principios clave para la prevención situacional del delito, centrados en la identificación de factores que facilitan su ocurrencia. A través de la evaluación de oportunidades (definidas en un tiempo y espacio determinados) se reconocen condiciones específicas que propician la comisión de ilícitos. Sin embargo, esta misma identificación permite diseñar estrategias orientadas a reducir los riesgos asociados (Felson y Clarke, 2008). Desde esta perspectiva, el “análisis de problemas” se convierte en una herramienta fundamental para el desarrollo de modelos de intervención específicos, que permiten

prevenir el delito mediante la modificación del entorno y la gestión de oportunidades como se observa a continuación:

> la evaluación de aquellas oportunidades que se presentan en situaciones específicas y que a su vez facilitan o promueven la comisión de un delito; en el modelo de prevención del delito situacional, a partir de cinco formas principales por medio de las cuales se puede modificar una situación con la finalidad de reducir las oportunidades de que se cometan delitos (Camacho, s.f)

Este planteamiento se complementa con la teoría de la elección racional, según la cual "los delincuentes toman decisiones basándose en un juicio, derivado de estimar las oportunidades de tener éxito en la comisión del delito y los beneficios que se esperan obtener" (Cabezas, 2017). En este espacio, el delincuente realiza una evaluación comparativa entre el riesgo de ser capturado y el beneficio personal que espera obtener.

En consecuencia, las tecnologías disruptivas han facilitado la comisión de delitos dentro de la cadena logística, al generar condiciones concretas que amplían las posibilidades de acción para individuos y estructuras dedicadas a actividades ilícitas. Si bien estos avances tecnológicos, científicos y sociales ofrecen beneficios significativos, también incrementan los riesgos, ya que sus ventajas pueden ser aprovechadas tanto por las autoridades como por los actores delictivos.

### *Teoría de las tecnologías disruptivas*

Las tecnologías con efecto disruptivo poseen un alto poder transformacional, cuya aplicación en diversos campos de la humanidad ha marcado diferencias significativas entre civilizaciones y, particularmente, en el ámbito organizacional. Estas tecnologías se definen como innovaciones capaces de generar nuevas redes de valor, irrumpiendo e interrumpiendo los

mercados establecidos. Su implementación no solo transforma los modelos operativos vigentes, sino que también provoca el desplazamiento de tecnologías anteriores, alterando profundamente las dinámicas económicas, sociales y productivas (Matovelle & Dabirian, 2015).

La denominación de "tecnología disruptiva" proviene de la teoría desarrollada por el profesor de la Universidad de Harvard, Clayton M. Christensen, quien, a partir de su investigación sobre la industria de discos duros, expuso en su obra The Innovator's Dilemma (1997) cómo ciertas innovaciones transforman mercados o sectores existentes al introducir características deseables como simplicidad, comodidad, accesibilidad y asequibilidad (Matovelle & Dabirian, 2015). Este tipo de innovación no constituye un fenómeno reciente, ya que ha estado presente desde los primeros avances tecnológicos y continúa manifestándose en la actualidad, generando impactos significativos en diversos ámbitos, incluido el organizacional.

La innovación fue definida por Tundidor (2018) como transformar en valor una oportunidad de mejora modificando el sistema. En sus inicios fue poco atractiva para la industria, pero luego demostró que la podía revolucionar, cuando calcularon los márgenes de beneficios proyectados y lo que representaba en un planteamiento de costo-beneficio, esto porque las nuevas tecnologías son ignoradas en gran parte de los casos a consecuencia de la preferencia que tienen las tecnologías que se consideran como más populares, pero también es importante anotar que cuando la tecnología disruptiva logra su establecimiento, aparece una innovación en menor escala orientada a mejorar el rendimiento de dicha tecnología, de la forma más ágil posible (Matovelle & Dabirian, 2015). Por ejemplo, el computador se convirtió en una tecnología disruptiva alrededor de la cual se derivaron muchas otras. En sus inicios resultó costoso y poco asequible, pero con el transcurso de la historia y los nuevos desarrollos se consiguieron múltiples

funcionalidades con las que se lograron resultados impactantes y también se hizo más cercano a todos los grupos sociales.

Para Matovelle y Dabirian (2015, p. 2) existen diferencias entre lo que se considera como innovación establecida y la innovación disruptiva porque mientras las primeras se enfocan en la eficiencia y la calidad para obtener cambios graduales dentro de un proceso de mejora continua, la segunda se aparta de las necesidades tradicionales para ser utilizada en nuevos mercados y pueden parecer incluso, de calidad inferior al compararla con otras innovaciones vigentes, pero también ofrece oportunidades para que interesados con menos recursos puedan acceder a ellas, siendo productos robustos que mejoran con el tiempo, lo cual representa una interesante inversión.

La economía global actual, de acuerdo con la CEPAL es digital. Lo anterior considerando que se reportan más de "7.000 millones de suscriptores de telefonía móvil", también se establece que hay "3.200 millones de usuarios de internet", el "47% de la población accede a banda ancha móvil" y hay "más de 180.000 millones de aplicaciones descargadas" (Castillo, 2016). Se pasó del internet de consumo, al internet industrial en áreas como la seguridad, salud, industrias al por mayor y al detal y en transporte.

Las innovaciones disruptivas exponen un panorama diferente en el que ya no se asume la competitividad desde quien saca algo nuevo, sino desde el ofrecimiento de nuevas posibilidades a grupos que requieren solucionar necesidades específicas. Así, se puede establecer que mientras las innovaciones establecidas se dirigen hacia la retención de los mercados que ya se han conseguido, con la innovación disruptiva se accede a nuevos espacios que facilitan la implementación de cambios que tienen alta posibilidad de éxito por el uso de los últimos avances tecnológicos y la aplicación en perspectivas de negocio diferentes.

En otras palabras la innovación y la disrupción pueden ser parecidas, sin embargo, se puede decir que quien es disruptor es innovador, pero no sucede al contrario, es decir, que quien sea innovador sea disruptor, esto, porque mientras la disrupción es un cambio radical, no toda innovación provoca ese tipo de transformaciones.

### *Tecnologías disruptivas en las empresas*

La innovación disruptiva en las empresas es un factor que ha aportado para su crecimiento rápido, ya que favorece el ingreso a nuevos mercados. La disrupción como término de acuerdo con la Real Academia de la Lengua (RAE, s.f), se relaciona con "rotura o interrupción brusca", lo que en otras palabras lleva a establecer que se rompe con las condiciones tradicionales para explorar nuevos espacios en procesos, clientes, proveedores, etc.

Clayton M. Christensen, explica que existen dos tipos de innovación: en primer lugar, se identifica la sostenible, empleada por las empresas grandes que están en la búsqueda constante de la optimización de un producto/servicio que ya existe en el mercado y es adquirido por los clientes actuales en el objetivo de obtener mayor rentabilidad. La innovación disruptiva, está centrada en la formulación de productos/servicios novedosos, que presenten ventajas en la facilidad de su uso, sean menos costosos en su venta y en su proceso de producción (Russo, s.f).

Esta innovación disruptiva les aporta a las empresas, especialmente a las pequeñas, crear un nuevo mercado o interrumpir el existente reemplazando un producto establecido, o en la satisfacción de las necesidades futuras del cliente. Conforme a lo argumentado por Vilanova (2018) la tecnología influye en los "factores clave de la empresa como la comunicación, la productividad o el entorno competitivo", lo que supone cambios en los procesos productivos y exige a las empresas adecuarse al nuevo panorama.

***Logística disruptiva***

Los cambios radicales implementados en los procesos logísticos se reflejan en la incursión y uso de tecnologías y el rediseño de su cadena de agregación de valor, para ofrecer servicios de mayor calidad que proporcionan un mayor beneficio frente a sus costos, por eso no es extraño observar "las entregas mediante drones, los camiones autodirigidos (sin conductor), y la utilización del Internet de las cosas para el autocontrol de la cadena de frio" (Gutiérrez R. , 2017).

Esto permite observar una transformación en los últimos cincuenta años pasando de la "logística operativa" parte de los procesos comerciales y de manufactura, a proyecciones y gestión estratégica de cadenas de suministro que contribuyan a agregar de valor y ventajas Competitivas.

De ese modo, se desarrollaron equipos e infraestructura tanto en el transporte como para la lectura electrónica del código de barras, sistemas de identificación, entre otros, que para la gestión de la cadena de abastecimiento, se complementan con un profundo conocimiento del negocio y de las necesidades de las demandas (actuales y potenciales), en la creación de valor de percepción para el cliente, más que al cumplimiento de indicadores de eficiencia en el costo operacional (Gutiérrez R. , 2017).

Es de anotar que la cadena de valor para el consumidor se deriva de la compra de un bien o de un servicio con al menos cuatro eslabones: los consumidores evalúan los bienes disponibles; escogen uno o dos; lo compran, y finalmente lo consumen. Los tres primeros se materializan en la tienda, pero la tecnología disruptiva puede facilitar alguno de estos procesos y allí se generan espacios para la compra *on line,* por ejemplo.

La tecnología disruptiva busca consolidar a las organizaciones mediante la innovación, incrementando su participación en el mercado tanto a nivel local como global. Cuando una empresa identifica elementos ineficientes en su operación, puede transformarlos en oportunidades de mejora mediante la adopción tecnológica.

La denominada logística disruptiva, o logística 4.0, surge como consecuencia de la cuarta revolución industrial. Esta propone el diseño de cadenas de abastecimiento que integren avances tecnológicos para proporcionar valor agregado y alcanzar niveles óptimos de eficiencia. Ejemplos como eBay, Amazon, Mercado Libre y Linio han modificado sus modelos de negocio, superando a sus competidores mediante la incorporación estratégica de tecnologías en sus procesos logísticos (Herrera, 2017).

Aunque sus orígenes se remontan a los años sesenta con el intercambio electrónico de datos, la logística ha evolucionado con la inclusión de aplicaciones que han transformado el flujo, la velocidad, el dinamismo y la seguridad de la información intercambiada en la cadena de suministro. Esta evolución ha permitido responder de manera eficiente a las necesidades de los clientes en un entorno cada vez más complejo, globalizado y competitivo.

La capacidad de optimización de la tecnología 4.0 se refleja en los “tiempos y recursos, trazabilidad de la cadena, seguridad e integridad de los datos, así como una adecuada interoperabilidad entre distintos actores humanos y digitales”, buscando una operación más eficiente y segura dentro de un comercio más sostenible desde el punto social y ambiental (Barleta, Pérez, y J, 2019).

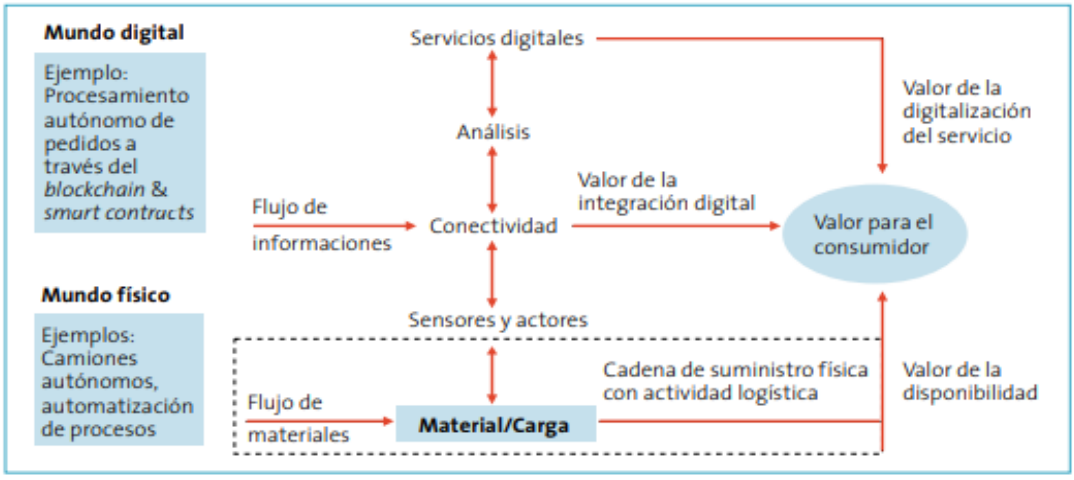
Esta revolución 4.0 ha incursionado en todos los ámbitos y por ello, formula nuevos retos en los que se integra el mundo *online* y *offline* como consecuencia de los cambios y la utilidad que proporcionan las tecnologías disruptivas, aportando cambios útiles a la cadena de suministro

e integrando estas tecnologías en un centro neurálgico en el que se aprovechan las ventajas de la inteligencia artificial y la realidad aumentada.

Para las organizaciones la cooperación e intercambio surgido desde el uso de tecnologías para compartir información se logra una trazabilidad en la que además de optimizarlos flujos de carga, se consigue un uso más eficiente de la infraestructura, recursos humanos, tecnológicos que facilitan la disposición de grandes volúmenes de carga y la toma de decisiones acertada en un óptimo desarrollo operacional, que se refleja en costos menores y mayor productividad.

Los servicios logísticos relacionados con las tecnologías disruptivas se sustentan en la optimización de procesos basados en la gestión del conocimiento. Por ejemplo, en la logística portuaria se destacan desarrollos en la robótica, la inteligencia artificial, el internet, automatización y el *blockchain* que junto con el *cloud computing* y otras herramientas informáticas se logra una cadena logística más completa y eficiente como se observa en la siguiente figura.

**Figura 1. Modelo para un negocio digitalizado**




***Nota:*** la figura expone un modelo que puede ser implementado en una organización para la digitalización de su logística. Fuente: Barleta, Pérez, y J, (2019, p. 4).

Este modelo ilustra cómo la digitalización de un negocio logístico integra diversas tecnologías disruptivas para optimizar sus procesos, se destacan componentes clave como la robótica, inteligencia artificial (IA), Internet de las Cosas (IoT), automatización, blockchain y cloud computing.

La implementación de estas tecnologías busca la gestión del conocimiento, monitoreo en tiempo real, reducción de tiempos y costos, y mejora de la calidad y seguridad, sin embargo, esta interconexión masiva y dependencia digital amplía exponencialmente la superficie de ataque para los ciberdelincuentes, convirtiendo cada elemento digitalizado en un potencial punto de entrada para amenazas. La eficiencia y trazabilidad que aportan se ven contrarrestadas por los riesgos si no se implementan medidas de ciberseguridad robustas.

En la actualidad se identifican diversas tecnologías que potencialmente pueden aportarle a la logística. Por ejemplo, aquellas en las que se integra información para ser utilizada en otros sistemas además del de distribución como los Sistemas Inteligentes de Transporte que facilitan la comunicación entre actores productivos, dispositivos y la infraestructura logística, incidiendo en "la reducción de tiempos, los costos y externalidades negativas ambientales y sociales" (Barleta, Pérez, y J, 2019), con la base tecnológica que facilita la planeación, toma de decisiones y la definición de metas en procesos que se monitorean en tiempo real, para establecer acciones de mejora y cambios modales en una operación logística, permitiendo que eventualmente los actores comprometidos compartan información en torno a la cadena de distribución para todos aquellos productos donde el servicio de distribución se de en un ambiente de colaboración.

En consecuencia, es fácil afirmar que las tecnologías que tienen capacidades disruptivas inciden en la mayoría, por no decir que todos, los aspectos logísticos relacionados con el transporte local e internacional, posicionando al cambio como una dinámica constante, que exige

la vinculación de las organizaciones en la gestión del conocimiento, la capacitación continua y la innovación como fuentes para la generación de ventajas y aspectos diferenciadores frente a la competencia.

Es de anotar que la más reciente prueba para la logística disruptiva y su aprovechamiento se dio durante la pandemia del COVID-SARS 19, en donde por las condiciones ya conocidas, se incrementaron las compras por internet, la demanda y el flujo de transporte superaron las capacidades que tenían las organizaciones hasta ese momento, propiciando una crisis en las cadenas de suministros en Colombia y en el mundo, derivando en otros problemas asociados como la sustentabilidad y otros procesos dirigidos a "lograr un abastecimiento de material más limpio; disminuir las emisiones del transporte; optimizar la logística y obtener certificaciones de cumplimiento" (Rueda et al., 2022, p. 164).

**Tendencias digitales en la industria 4.0**

Son diferentes los mecanismos que se están utilizando para lograr la preferencia de los consumidores de hoy, entre ellas se encuentra la "Gamificación", como una forma de aprovechar el interés de muchos por los juegos móviles. Así, se utilizan estas técnicas en el comercio minorista a través de una aplicación que asiste a los clientes con la tecnología de seguimiento, permitiéndoles compartir estadísticas en las redes sociales, que promocionan el valor agregado y la participación del cliente (Ardila, 2014).

La "comercialización del comportamiento" utiliza las bases de datos en las que se reúnen datos sobre las conductas y preferencias de los clientes objetivo, logrando que los editores y los anunciantes utilicen la publicidad basada en intereses para llegar a los usuarios teniendo en

cuenta esta variable más su situación demográfica, los anunciantes crearon campañas que al final influyeron en el logro de un tráfico eficiente (Ardila, 2014).

Con la "impresión 3D" se logran archivos digitales y otros elementos con los que se eliminan costos de transporte y los tiempos de espera para los fabricantes. La "Predicción de la demanda" facilita que se programe la llegada de las mercancías, respondiendo a interrogantes como: qué producir, cuándo producirlo, y cuánto producir, aunque cabe precisar que esto es algo que ya tiene un buen tiempo de uso, actualmente proporciona una visión en tiempo real en el proceso de producción (Ardila, 2014).

**Ciberseguridad en términos generales**

Las diferentes amenazas que se vienen presentando a través de internet son noticia continua y afectan tanto a personas como a empresas, demandando mecanismos urgentes para ofrecer protección a la información (Fundación Telefónica, 2016). Lo anterior se beneficia de la digitalización de los servicios y la economía y aunque se afirma que los empresarios tienen una mayor capacidad para afrontar los retos que se derivan de este fenómeno porque cuentan con profesionales preparados para contrarrestarlo, la realidad es que el problema de la inseguridad de la información se sigue presentando.

Esto tiene que ver igualmente, con el incremento del uso de las TIC y que abre más espacios de riesgo, ya que es común que la mayoría de las personas utilicen estas tecnologías desde su interés individual hasta el plano organizacional, dando lugar a la "Sociedad de la Información" o "Sociedad del Conocimiento" como manera de identificar esta nueva realidad.

De acuerdo con Bartolomé (2021) "a comienzos del año 2020 alcanzaba a 4.5 mil millones de usuarios, casi el 60% de la población mundial" que incursionaron en un "entorno

virtual de información e interacciones entre personas" en un ámbito global y dinámico, cimentado a partir de infraestructuras y sistemas de información y telecomunicaciones. Esto generó competencias y pujas por diferentes actores heterogéneos como organizaciones terroristas, criminales, de espionaje, empresas privadas, hackers que produjeron amenazas y riesgos materializados a través del ciberterrorismo, cibercriminalidad y ciber-espionaje (Bartolomé, 2021).

Lo anterior se beneficia del costo relativamente bajo que pueden tener estos ataques, comparados con otras formas para generar daño, teniendo en cuenta que el agresor puede valerse de computadoras de uso cotidiano y software que tiene costos accesibles, no utiliza armamento u otros recursos que pueden ser mucho más onerosos, solo requiere del conocimiento del ejecutor que en algunos casos, no requiere competencias muy sofisticadas.

Aquí aparecen conceptos como *malware*, *software* malicioso representados en virus, gusanos, troyanos, *ransomware* o *spyware* que pueden ser descargado en una computadora, para originar daños o filtraciones de datos. También se conoce la Denegación Distribuida de Servicio (DDoS), que representa una parálisis intencional de una red de computadoras (Bartolomé, 2021).

### *Ataques a la infraestructura empresarial*

Cuando se presenta un ataque a la infraestructura empresarial, se entiende que los objetivos pueden ser espionaje o robo de información. Otras amenazas denominadas como persistentes y que se denominan como APT (Advanced Persistent Threat) por sus siglas en inglés, incluyen procesos informáticos que se ejecutan de manera sigilosa y continua, por medio de técnicas sofisticadas en las que se implementa un software malicioso dirigido a explotar las vulnerabilidades presentes en los sistemas (Fundación Telefónica, 2016).

Las empresas cuando definen sus políticas de seguridad buscan prevenir la destrucción de los datos que resultan de sus operaciones, actualizadas de forma constante, e incluyendo las últimas tendencias y aspectos relacionados con la seguridad. Lo anterior se apoya en el proceso de la ciberseguridad que incluye etapas asociadas que influyen en la prevención, además de la detección y el desarrollo de una reacción o respuesta, que lleva inserta el aprendizaje como medio para la mejora continua.

Frente a ello, cabe decir que la ciberseguridad está asociada también a la capacidad económica para implementar infraestructura que contribuya a que la organización pueda tener altos niveles de seguridad en sus sistemas y también desde las instancias comprometidas, buscar medios que apoyen a las medianas o pequeñas empresas que no tienen los recursos para acceder a este tipo de herramientas.

## Metodología

Las tecnologías disruptivas han generado transformaciones significativas en los estilos de vida laboral y personal de la sociedad contemporánea. En el ámbito empresarial, estos avances han permitido la apertura de nuevos nichos de mercado y el fortalecimiento de los procesos logísticos mediante la incorporación de soluciones tecnológicas innovadoras.

Este estudio se fundamenta en un enfoque cualitativo con énfasis descriptivo, privilegiando la observación sistemática y la investigación documental, en concordancia con los antecedentes teóricos y los hallazgos de estudios previos.

La información se ha recopilado a partir de fuentes secundarias como artículos académicos, investigaciones especializadas y canales oficiales de consulta de las autoridades colombianas. Particularmente, se ha prestado atención a los índices delictivos asociados al uso de tecnologías disruptivas que inciden negativamente en la seguridad de las cadenas logísticas del sector empresarial.

Los esfuerzos de las organizaciones por ofertar servicios con mayor eficiencia y oportunidad, los lleva a enfrentarse con amenazas por la implementación de tecnologías disruptivas, las cuales son accesibles a todo público incrementando los entornos digitales, y consigo conductas delictivas que impactan directamente la operación logística por medio de *malware, phishing y ransomware,* entre otros, evidenciado en el Balance de Ciberseguridad 2022 emitido por el Centro Cibernético Policial de la Dirección de Investigación Criminal e Interpol donde el comportamiento delictivo incremento en un 21.6% con 65.794 denuncias por delitos informáticos acorde a la Ley 1273 de 2009, lo anterior en comparación con los registros de 2021 que cerró con 51.579 requerimientos. (Dirección de Investigación Criminal e Interpol, 2022)

**Figura 2. Evolución Denuncias 2022**


***Nota:*** la figura presenta la evolución del número de denuncias relacionadas con delitos informáticos en Colombia entre 2010 y 2023, en correspondencia con lo definido en la Ley 1273 de 2009 que se constituye en un punto de referencia normativa para el tratamiento penal de conductas delictivas en entornos digitales Fuente: Dirección de Investigación Criminal e Interpol (2022).

Como se observa en la figura 2 hay un crecimiento sostenido en el número de denuncias reportadas entre 2010 y 2023, pasando de 572 casos en 2010 a 65.794 en 2023. Este incremento refleja no solo una mayor incidencia de delitos asociados al uso de tecnologías disruptivas en el entorno empresarial y logístico, sino también una posible mejora en los mecanismos de reporte y visibilización institucional.

La referencia a la Ley 1273 de 2009, que tipifica los delitos informáticos en Colombia, sugiere que el marco normativo ha influido en el aumento de denuncias al brindar herramientas jurídicas para enfrentar nuevas modalidades delictivas. Este comportamiento ascendente plantea retos significativos para la seguridad de las cadenas logísticas, especialmente en contextos de digitalización acelerada y comercio transnacional.

## Ciberdelitos en el ámbito de la logística organizacional, mediante el aprovechamiento de tecnologías disruptivas

La aparición de tecnologías disruptivas ha generado beneficios significativos para la sociedad; no obstante, también ha sido aprovechada por ciertos actores para afectar negativamente a organizaciones y empresas, ya sea mediante prácticas de competencia desleal o con el propósito deliberado de causar perjuicios económicos.

A partir del análisis del Boletín FAL N.º 382, publicado por la CEPAL en 2020, se identifican diversos factores técnicos en materia de seguridad que deberían implementarse al interior de las organizaciones. Estas recomendaciones se orientan a mitigar el riesgo cibernético, considerando no solo los incidentes y pérdidas económicas derivadas de dichas afectaciones, sino también otros impactos asociados al uso indebido de las tecnologías de la información y la comunicación (Mariano, 2022).

En el tema logístico se pueden destacar ejemplos como lo ocurrido en el Puerto de Amberes en Bélgica en el año 2022 cuando un cartel de la droga atacó los sistemas terminales mediante la acción de piratas informáticos, liberando contenedores con drogas ilícitas, armas de fuego y contrabando por un valor aproximado de 365 millones de dólares de una manera tan efectiva que las autoridades portuarias no lo notaron. Otros casos son el ataque de *ransomware* a MAERSK en junio de 2017 y que originó perdidas de u$s 264.000.000, lo que impulsó la instalación de *Smart Logistics* implementando junto a IBM para la gestión global de documentación de la carga, utilizando *blockchain* para la trazabilidad de estos documentos y así como estos, son múltiples los que se pueden mencionar a nivel global en relación con la afectación a través de tecnologías disruptivas a la cadena logística.

Mariano Díaz (2022) señala que la logística ocupa el segundo o tercer lugar entre los sectores más vulnerables a los ciberataques, según informes publicados por IBM Security. Esta afirmación se sustenta en el efecto dominó que generan las afectaciones a la cadena logística: un solo incidente puede desencadenar múltiples impactos operativos, económicos y reputacionales sin requerir esfuerzos adicionales por parte del atacante.

En América Latina, se han documentado casos relevantes que ilustran esta vulnerabilidad, como los ataques a infraestructuras portuarias, sistemas de trazabilidad y plataformas de comercio electrónico, los cuales han comprometido la continuidad operativa y la seguridad de los datos en sectores estratégicos como los que se enuncian a continuación (Mariano, 2022):

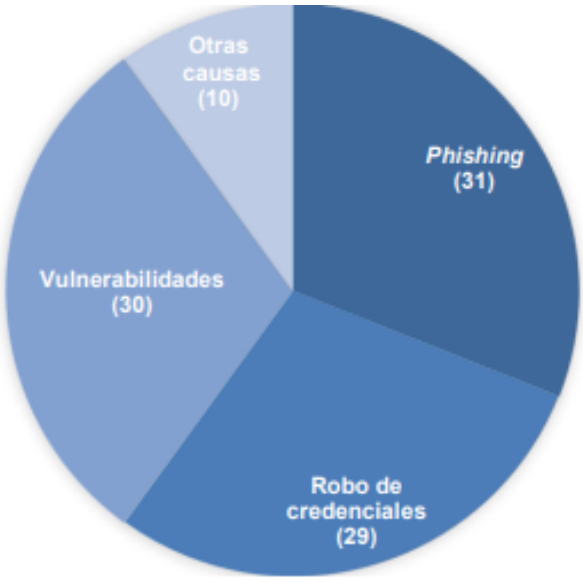
- El sucedido a la compañía mexicana Pemex en 2019 y que afectó al 5% de los equipos de la compañía.
- En 2020, la empresa Electrobras Termonuclear S.A. proveedora de servicios de energía eléctrica, fue víctima de un *ransomware* en sus sistemas administrativos.
- La exfiltración de más de 100 GBytes con datos (1000 GBytes) de la firma Copel S.A

Otro ejemplo representativo es el ciberataque sufrido por la compañía Colonial Pipeline en mayo de 2021, cuando fue afectada por un malware tipo ransomware que comprometió tanto el sistema de facturación del combustible como el software operativo encargado de gestionar las funciones del oleoducto. Este incidente, atribuido al grupo criminal DarkSide, obligó a la empresa a interrumpir sus operaciones como medida de contención, lo que derivó en la declaración de emergencia regional en al menos 17 jurisdicciones de Estados Unidos, incluyendo Alabama, Arkansas, Washington D.C., Delaware, Florida, Georgia, Kentucky, Luisiana, Maryland, Misisipi, Nueva Jersey, Nueva York, Carolina del Norte, Pensilvania, Carolina del

Sur, Tennessee, Texas y Virginia, evidenciando la vulnerabilidad de las infraestructuras críticas ante amenazas digitales y el impacto sistémico que puede generar un solo ataque en la cadena logística energética de una nación. (Mariano, 2022).

Según la CEPAL en esta región aproximadamente el 72% de las organizaciones ha sido objeto de un ciberataque en 2021 revelando al mismo tiempo las posibles debilidades que facilitan a los atacantes lograr sus objetivos, ya que estos actúan utilizando técnicas de phishing en el 31% de los casos, roban credenciales por filtración de datos en el 29% y 30 % utilizan vulnerabilidades técnicas de *hardware* y *software*, dejando solo un 10% a otras causas como se observa en la figura 1. Esto permite observar que la mayor circunstancia para vulnerar los sistemas de las organizaciones se constituye en la irrupción dentro de las redes y es efectuada en gran parte de los casos por las mismas personas de la empresa (CEPAL, 2021).

**Figura 3. Causa de los incidentes en las organizaciones**




*Nota*. La figura evidencia la distribución porcentual de las principales causas de incidentes de ciberseguridad, destacando que el phishing (31 casos), el robo de credenciales (29 casos) y las vulnerabilidades del sistema (30 casos) constituyen los factores más recurrentes. Fuente: Mariano (2022) a partir de información publicada en informes de la CEPAL.

Las categorías que se observan en la figura 3 representan la mayoría de los incidentes reportados, lo que sugiere que los ataques se concentran en la explotación de debilidades humanas y técnicas dentro de las organizaciones. La categoría “otras causas” (10 casos) ocupa un lugar marginal, lo que refuerza la necesidad de priorizar estrategias de prevención centradas en la capacitación del personal, la gestión de accesos y el fortalecimiento de la infraestructura tecnológica. Este patrón de distribución permite inferir que los riesgos cibernéticos no solo dependen de la sofisticación del ataque, sino también de la exposición y preparación institucional frente a amenazas comunes.

Cabe anotar que los informes incluyen a las organizaciones que denunciaron hechos, pero también es un hecho que muchas de ellas no dan a conocer esas situaciones, lo que puede modificar esas causas identificadas.

## Estrategias aplicadas por las autoridades competentes en Colombia para prevenir el ciberdelito mediante el aprovechamiento de tecnologías disruptivas.

En este capítulo se examina la situación nacional respecto al uso de tecnologías disruptivas como herramienta para la prevención del ciberdelito. Se analizan las ventajas que dichas tecnologías ofrecen en los ámbitos logístico y de seguridad, así como las perspectivas y conocimientos aportados por expertos nacionales en la materia. El enfoque busca resaltar el papel estratégico de la innovación tecnológica en la formulación de políticas públicas orientadas a la protección digital y la gestión eficiente de riesgos cibernéticos.

### Algunas medidas internacionales

El análisis de las medidas internacionales adoptadas para la prevención del ciberdelito permite identificar referentes estratégicos que pueden orientar el fortalecimiento de políticas nacionales en materia de seguridad digital. Diversos países han implementado marcos normativos, programas de cooperación y tecnologías emergentes con el fin de mitigar riesgos cibernéticos y proteger infraestructuras críticas. Este apartado presenta una síntesis de iniciativas relevantes, destacando aquellas que integran tecnologías disruptivas en sus esquemas de prevención, respuesta y resiliencia institucional, con el propósito de aportar elementos comparativos que enriquezcan el diseño de estrategias en el contexto colombiano.

#### *Tecnologías disruptivas y ciberdelito transnacional: riesgos emergentes en entornos digitales*

El ciberdelito, impulsado por el vertiginoso desarrollo de tecnologías disruptivas, constituye una amenaza transnacional que impacta directamente la cadena logística y las

operaciones empresariales a escala global. Expertos estiman que su costo asciende a aproximadamente 542.000 millones de euros, lo que representa cerca del 0,8 % del PIB mundial. Este fenómeno se ve favorecido por el bajo costo relativo de los ataques, que en muchos casos solo requieren equipos informáticos convencionales y software de fácil acceso, en contraste con el uso de armamento tradicional.

La digitalización de procesos y la expansión de tecnologías como *blockchain*, el Internet de las cosas (IoT), la realidad aumentada y la inteligencia artificial han transformado significativamente los entornos logísticos; sin embargo, también han generado nuevas brechas de seguridad. El entorno virtual global (al que accedía cerca del 60 % de la población mundial a inicios de 2020) se ha convertido en un escenario propicio para la acción de actores maliciosos, como organizaciones criminales y hackers, quienes materializan amenazas a través del ciberterrorismo, la cibercriminalidad y el ciberespionaje. Esta dinámica plantea desafíos complejos para la gobernanza digital y exige respuestas coordinadas que integren innovación tecnológica, cooperación internacional y fortalecimiento institucional (Márquez y otros, 2024).

**Casos representativos de ciberdelito en operaciones logísticas internacionales**

El estudio de casos representativos de ciberdelito en operaciones logísticas internacionales permite comprender la magnitud y complejidad de las amenazas digitales que enfrentan los sistemas de transporte, distribución y gestión de mercancías a nivel global. Estos incidentes evidencian cómo actores maliciosos aprovechan vulnerabilidades tecnológicas, brechas en la ciberseguridad y fallos en la gobernanza digital para afectar la trazabilidad, la integridad de los datos y la continuidad operativa de las cadenas de suministro.

El sector logístico se encuentra entre los más atacados globalmente, según informes de IBM, debido al efecto dominó que un incidente puede generar en toda la cadena de suministro.

1. **Ataque al Puerto de Amberes (Bélgica, 2022)**

Un cartel de drogas utilizó hackers para atacar los sistemas terminales, logrando liberar contenedores con drogas, armas y contrabando valorado en 365 millones de dólares, sin que las autoridades portuarias lo advirtieran de inmediato.

2. **Ataque de Ransomware a MAERSK (2017)**

Este incidente causó pérdidas de aproximadamente 264 millones de dólares y llevó a MAERSK a colaborar con IBM para implementar Smart Logistics utilizando blockchain para la trazabilidad global de la documentación de carga.

**Incidentes en América (2019-2020)**

El periodo comprendido entre 2019 y 2020 estuvo marcado por un incremento significativo en los incidentes de ciberdelito en América, afectando sectores estratégicos como la logística, las telecomunicaciones y los servicios financieros. La región evidenció vulnerabilidades críticas frente a ataques cibernéticos que comprometieron infraestructuras digitales, expusieron datos sensibles y alteraron la continuidad operativa de múltiples organizaciones.

1. **Pemex (México, 2019)**

Un ciberataque afectó al 5% de los equipos de la compañía.

2. **Electrobras Termonuclear S.A. (Brasil, 2020)**

Fue víctima de ransomware en sus sistemas administrativos.

3. **Copel S.A. (Brasil)**

Sufrió la exfiltración de más de 100 GBytes de datos.

4. **Colonial Pipeline (Estados Unidos 2021)**

Un ataque de *malware* afectó el sistema de facturación y las operaciones del oleoducto, forzando su cierre y la declaración de emergencia en múltiples estados.

## Medidas y Marcos de Respuesta Internacional

La creciente sofisticación del ciberdelito ha impulsado a diversos países y organismos multilaterales a desarrollar marcos normativos, estrategias de cooperación y mecanismos tecnológicos orientados a la protección del entorno digital. Estas medidas internacionales no solo buscan mitigar los riesgos asociados a las amenazas cibernéticas, sino también establecer estándares comunes que faciliten la respuesta coordinada ante incidentes transnacionales. En este apartado se examinan iniciativas relevantes implementadas por actores globales, con énfasis en aquellas que integran tecnologías disruptivas en sus esquemas de prevención, detección y resiliencia institucional.

Ante la magnitud de esta amenaza, la comunidad internacional ha establecido diversas iniciativas para combatir el ciberdelito:

1. **Programa Mundial sobre Ciberdelincuencia de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC)**

Impulsa el desarrollo de capacidades a largo plazo para la lucha contra el cibercrimen, ofreciendo asistencia técnica en prevención, cooperación internacional, recopilación de datos, investigación y análisis.

2. **Comité Interamericano contra el Terrorismo (CICTE) de la OEA**

A través de su Programa de Ciberseguridad, participa en la prevención y respuesta a estos delitos.

**3. Convenio de Budapest**

Aunque Colombia no es signatario directo, sus lineamientos influyen en las políticas nacionales de ciberseguridad.

4. **El Pacto - Europa Latinoamérica Programa de Asistencia contra el Crimen Transnacional Organizado**

Facilita la cooperación transnacional en la lucha contra el crimen organizado.

**5. Entes Reguladores y de Control Globales**

Incluyen la Unión Internacional de Telecomunicaciones (UIT), la Agencia de la Unión Europea para la Ciberseguridad (ENISA), y organizaciones policiales como Interpol (con su Estrategia Mundial contra la Ciberdelincuencia), CSIRT Américas (plataforma regional de cooperación), y Ameripol.

A pesar de estos esfuerzos, persisten desafíos como la poca normatividad específica para sancionar el ciberdelito y la falta de preparación de los empresarios, es fundamental una acción articulada entre autoridades, empresas y todos los actores de la cadena de suministro, así como la capacitación continua y la inversión en ciberseguridad para mitigar estos riesgos y proteger la infraestructura logística global.

Colombia como firmante de convenios y tratados internacionales, se ajusta a esos compromisos entre los que se destaca el Programa Mundial Sobre Ciberdelincuencia de la Oficina de las Naciones Unidas Contra la droga y el Delito (UNODC) en el cual se impulsa el desarrollo de capacidades para que se sostengan a largo plazo en la lucha contra el delito cibernético por lo cual proporciona asistencia técnica para la generación de capacidades dirigidas hacia la prevención y la cooperación internacional, la recopilación de datos, la investigación y el

análisis frente al delito cibernético. También participa la OEA – mediante el Comité Interamericano Contra el Terrorismo (CICTE) y su Programa de Ciberseguridad

Otros mecanismos importantes son el Convenio de Budapest que rige a los estados involucrados en el Consejo de Europa y aunque no tiene relación directa con Colombia, si cuenta con unos lineamientos que influyen en las medidas asumidas por el país. Esto se complementa con El Pacto - Europa Latinoamérica Programa de Asistencia contra el Crimen Transnacional Organizado.

Además hay unos entes reguladores a nivel global entre los que se pueden mencionar a la Unión Internacional de Telecomunicaciones (UIT), la Agencia de la Unión Europea para la Ciberseguridad – ENISA y organismos de control entre los que están la Interpol con su Estrategia Mundial Contra la Ciberdelincuencia, CSIRT Américas que se constituye en una plataforma en la que se apoya la cooperación regional y el intercambio de información, Ameripol

Otros actores destacados son organizaciones militares que se apoyan en lo acordado en la Organización del Tratado del Atlántico Norte (OTAN).

**Análisis de la logística y seguridad proporcionada por las tecnologías disruptivas**

La gestión logística como actividad básica en los procesos empresariales no solo implica la búsqueda de mecanismos para ser eficaz ante las solicitudes de los clientes, sino que incluye necesidades frente a la reducción de los riesgos que puedan afectar la consecución de objetivos organizacionales en cuanto al posicionamiento en el mercado y la preferencia del cliente objetivo.

En desarrollo de la investigación se recolectó información documental y en las entrevistas realizadas a dos funcionarios del Centro Cibernético Policial, quienes se ocupan de la

investigación de las denuncias realizadas por los delitos que se cometen en el ciberespacio y de los cuales hacen parte las tecnologías disruptivas que son utilizadas para afectar la cadena logística de las empresas.

De ese modo, se pudo determinar que en definitiva, son diversos los riesgos que se presentan en la cadena de suministro y que se asocian con el uso de tecnologías disruptivas ya que en este momento resulta muy sencillo de acuerdo a lo establecido por el Intendente José Córdoba, (Córdoba, comunicación personal, 11 de abril del 2021) del Centro Cibernético Policial que se pueda utilizar un teléfono, un computador, elementos más sofisticados como el Big Data o la Robótica, por mencionar algunos ejemplos.

La ciberseguridad alcanza de acuerdo a ello, una alta significación, debido a que es fundamental que quienes gestionan o administran estas cadenas cuenten con los instrumentos tecnológicos y todo lo necesario para contrarrestar esos riesgos que presentan los avances tecnológicos actuales y que desde un ataque informático puede afectar gravemente a la cadena de suministros, alterando información sustancial para los registros de la empresa.

En este punto, se destaca lo determinado por el Mayor Roberto Moreno cuando establece que en otros países como Perú, uno de los más afectados por el cibercrimen hay un incremento notable de los delitos informáticos, varios de ellos, afectando la logística y otros procesos en las empresas, lo cual debe alertar a sus gerentes y propietarios para establecer medidas urgentes orientadas a la prevención y si se diera el problema, a contrarrestar cualquier afectación causada mediante el uso de avances tecnológicos(Moreno, comunicación personal, 11 de abril del 2021).

La ciberseguridad en todos sus avances puede ser un instrumento válido para realizar esta gestión, ya que así como se usan las tecnologías disruptivas para cometer delitos, también pueden implementarse en su prevención y control, logrando sistemas que protejan la información

y los procesos de las empresas. De ese modo y de acuerdo a Moreno, con la ciberseguridad se pueden utilizar tecnologías con las que se consiga un control más cercano de la cadena logística (Moreno, comunicación personal, 11 de abril del 2021), lo cual se logra con técnicas de hacking y otras herrramientas ya creadas por los expertos, pero también, fomentando la capacitación y actualización continua de los responsables, en un proceso permanente de gestión del conocimiento y transferencia para fortalecer e impulsar mecanismos dirigidos a reducir estas afectaciones para los empresarios.

Ventajas como el conocimiento de quien está permitiendo la fuga de información o empleados que están desarrollando su función de manera incorrecta son esenciales para evitar daños mayores, especialmente en la cadena de abastecimiento, que se relaciona directamente con el cumplimiento al cliente. Esto debe acompañarse de políticas en la organización y a nivel de Estado en las que se fortalezca el aparato normativo, se potencien procesos y se aborden los retos que genera continuamente la tecnología como instrumento utilizado en contra de la gestión logística en una empresa.

Además, es necesario aclarar que los ciberataques pueden involucrar los procesos para la entrega de los pedidos a los clientes, pero también demanda de la formulación de soluciones a las necesidades surgidas en los canales con los proveedores, con los socios o los clientes en un daño menos directo pero que también puede tener consecuencias muy desfavorables en la cadena de suministro. El flujo de mercancías y la transformación digital de algunos procesos empresariales ha llevado a la formulación de mecanismos como la logística 4.0, que se dirige a la conexión de tecnologías en red, que puede ser muy benéfica por la integración de información, pero también muy dañina si se observan las múltiples amenazas que se dan en el momento actual. Lo anterior demuestra en palabras del Mayor Moreno que ya no solo hay que preocuparse por la seguridad

física, sino también se debe implementar una atención prioritaria a los sistemas de información y los procesos inmersos en estos (Moreno, comunicación personal, 11 de abril del 2021).

Una de las grandes debilidades en torno al tema en Colombia es la poca normatividad para sancionar conductas relacionadas con el ciberdelito, apenas es un tema en desarrollo en el pais, pero además, se necesita de mayor preparación y capacitación de parte de los empresarios en el tema, así como una acción articulada entre autoridades, empresarios y todos los actores que hacen parte de la cadena de suministro (Córdoba, comunicación personal, 11 de abril del 2021).

**Seguridad en procesos logísticos y tecnologías disruptivas**

La transformación digital y la cultura para la prevención y protección de riesgos en las empresas originó que la ciberseguridad ocupe un rol muy importante “porque con el uso de las nuevas tecnologías en los procesos de negocio, hemos ampliado las posibilidades de ataque” (Portafolio, 2019). El crecimiento de incidentes de ciberseguridad tanto en el mundo como en Colombia muestra cifras hasta del 50 por ciento, lo cual puede ser superior en organizaciones donde se cuenta con un bajo nivel de formación en seguridad y se produce incremento del uso de las nuevas Tecnologías de la Información y las Telecomunicaciones.

En muchas partes del mundo se desarrollan robots que parecen humanos, frigoríficos con conexión a Internet, entre otros, que fomenta la aparición de nuevos productos y servicios, provocando también que las tecnologías y estrategias de negocio e I+D que se encuentran vigentes o que tienen un largo recorrido en su aplicación, se conviertan en algo obsoleto con mucha rapidez, influyendo en la capacidad competitiva de las organizaciones, pero también en la creación de espacios de riesgo.

Las tecnologías disruptivas en “manos equivocadas puede ser utilizado en actividades maliciosas y ser un obstáculo para la ciberseguridad” (Marketing digital, s.f). Con el Internet, por

ejemplo, todos los procesos cotidianos se digitalizan y se conectan a esta red, transportando una cantidad de información que es de interés para los hackers. El software de rescate, se trata de un software malicioso que utilizan estas personas y que les facilita la restricción del acceso a la red, asumiendo, además, el control de sus vehículos inteligentes o dispositivos de operaciones y cuando los bloquean piden rescate por ello, frustrando las operaciones y todo lo que tiene que ver con el funcionamiento de la empresa, incluso, los procesos logísticos.

La inteligencia artificial, la realidad virtual, entre otros, origina el robo de identidad y muchos otros mecanismos con los que los atacantes tienen la oportunidad de modificar una oficina virtual u otra información, destruyendo la imagen e incidiendo en la experiencia de los usuarios. Con el *cloud computing*, muchas empresas pueden almacenar su información y en el caso que un hacker la obtenga, origina riesgos para la privacidad de los clientes y para la operación del negocio, consiguiendo incluso, su destrucción.

Esto también exige la generación de medidas que regulen el uso de las tecnologías 4.0, considerando que varias de las plataformas utilizadas se encuentran en la nube (*cloud computing*) y aún se observan brechas y vacíos en la regulación, lo que puede facilitar la ocurrencia de delitos a través de tecnologías disruptivas que afecten el desarrollo de las operaciones logísticas. Normas para las telecomunicaciones, la IoT, el espectro radioeléctrico, la autorización de licencias, definición de estándares que a nivel local o en el plano regional van a permitir que se garantice una competencia leal y a la vez, lograr criterios de calidad en el ámbito internacional.

Lo anterior, se adiciona a las necesidades en regulaciones sobre la protección de los datos, la privacidad y la seguridad, un tema que también ha sido controversial por el robo de datos y el bloqueo de plataformas que originan daños costosos para las empresas y traumatismos en sus procesos, especialmente en la recuperación de la información, por eso, la modernización,

ajuste, flexibilidad en los marcos jurídicos promueve la adopción de las nuevas tecnologías y su interoperabilidad.

La universalidad de los sistemas también provoca vulnerabilidades en las plataformas para que sean objeto de ataques informáticos. Los ciberataques, se diferencian de los virus de épocas anteriores en donde lo fundamental era desplegar tácticas para exponer vulnerabilidades de los sistemas informáticos, pero actualmente son grupos especializados los que dirigen sus ataques a sistemas críticos para robar información comercial o industrial, secuestrándolos, solicitar rescate y en casos específicos, trastornar el correcto trabajo de las cadenas de suministro.

En Colombia con la expedición de la Ley 1978 de 2019 del Ministerio de las TIC, no solo moderniza el sector de las Tecnologías de la Información y las Comunicaciones, sino que, además, articula los modelos de ciberseguridad y las tecnologías disruptivas en la cadena logística, respaldada por un conjunto de políticas Públicas que buscan fortalecer la confianza digital, esto con la finalidad de proteger a las empresas, no solo en el ámbito de la logística, sino en todas sus áreas. Adicionalmente, cuenta con el documento CONPES 3995 de 2020, cuyo objetivo es: "Establecer medidas para desarrollar la confianza digital a través de la mejora de 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" impartiendo con este instrumento, lineamientos a las diferentes entidades estatales que permiten la mejora continua en la seguridad digital, así mismo, dentro del marco normativo se expidió la Ley 2181 de 2021 por medio de la cual se establecen normas para garantizar la seguridad de la cadena logística y prevenir los delitos transnacionales, y la Resolución 02277 del 2025, con el

propósito de fortalecer la estrategia de seguridad digital del Estado colombiano, conforme a los lineamientos de la norma internacional ISO/IEC 27001DE 2022, documento CONPES 3995 de 2020 y desarrollando las directrices impartidas en el Decreto 338 de 2022, que han propiciado un impulso, junto con el trabajo de la fuerza pública con el fin de enfrentar estos nuevos desafíos.

Por otra parte, las acciones tecnológicas disruptivas de la criminalidad han originado que instancias como la Dirección de Investigación Criminal de la Policía Nacional - DIJIN, investigue de forma general los ataques a entidades financieras y sus clientes, a las bases de datos de diferentes compañías, sus proveedores o clientes por medio de tecnologías inteligentes que no solo se orientan hacia grandes empresas, también lo hacen a pequeñas y medianas empresas, llegando en el 2017 a cifras que muestran que el 76% de las pymes y el 56% de las microempresas de Colombia son objeto del ciberdelito con el uso de softwares que pueden ser intervenidos con la cadena de valor disruptiva de las estructuras criminales (Redacción Tecnósfera, 2019); lo anterior se complementa con la identificación del crecimiento del cibercrimen en Colombia del 28,3% (párr. 11), cifra que evidencia que estas mismas organizaciones delictivas están valiéndose de las cadenas de valor disruptivas para entorpecer las acciones de las autoridades.

**Tabla 1. Ventajas e impacto de las tecnologías disruptivas en la cadena logística**

| VENTAJAS | IMPACTO |
|---|---|
| Automatización y eficiencia en los procesos | Disminución en los tiempos de la operación, aumentando la satisfacción del usuario |
| Acceso oportuno a la información | Fortalecer la seguridad previniendo la vulnerabilidad |
| Monitoreo en tiempo real de las tareas | Reducción de costos y mejora de calidad |
| Soluciones innovadoras | Satisfacción del cliente y trabajadores |
| Fortalecimiento de la seguridad tecnológica | Confianza en el desarrollo de la cadena logística |

Fuente: elaboración propia, 2025

La Tabla 1 presenta una síntesis de los principales beneficios que ofrecen las tecnologías disruptivas en el ámbito logístico, junto con los impactos que generan en la operación y

percepción institucional. En primer lugar, la automatización y eficiencia en los procesos permiten reducir significativamente los tiempos operativos, lo que se traduce en una mejora directa en la experiencia del usuario. El acceso oportuno a la información fortalece los sistemas de seguridad, al facilitar la detección temprana de vulnerabilidades y la toma de decisiones informadas.

El monitoreo en tiempo real de las tareas contribuye a la optimización de recursos, disminuyendo costos y elevando los estándares de calidad. Por su parte, la incorporación de soluciones innovadoras no solo mejora la productividad, sino que también incrementa la satisfacción tanto de los clientes como de los trabajadores, al ofrecer entornos más dinámicos y adaptativos. Finalmente, el fortalecimiento de la seguridad tecnológica genera confianza institucional, consolidando la cadena logística como un componente estratégico en la competitividad organizacional.

## Conclusiones y recomendaciones

Al contextualizar los fundamentos teóricos asociados a la cadena de valor, las tecnologías disruptivas y la ciberseguridad, se identificó la pertinencia de la teoría de la oportunidad, la cual permite comprender cómo la aparición de tecnologías cada vez más sofisticadas facilita el acceso a grandes volúmenes de información, pero también evidencia vacíos, brechas y riesgos en la gestión logística de las organizaciones. Este fenómeno se intensifica en un entorno donde las tecnologías están profundamente integradas en la mayoría de las actividades humanas.

Las tecnologías disruptivas tienen como propósito central la agilización y eficiencia de los procesos relacionados con el manejo de información estratégica para la toma de decisiones. No obstante, estas mismas herramientas son aprovechadas por estructuras ilegales para cometer ilícitos con mayor sofisticación, lo que plantea desafíos significativos para las autoridades y los actores logísticos. En este contexto, se requiere una gestión del conocimiento orientada a la prevención, el monitoreo permanente y la protección integral de los procesos logísticos.

La baja cultura de denuncia frente a los ciberdelitos dificulta la identificación precisa de la magnitud del problema. Sin embargo, se evidencian consecuencias relevantes para las organizaciones, especialmente en los procesos productivos, desde la adquisición de insumos hasta la atención al cliente, afectando el cumplimiento de entregas en tiempo, forma y calidad.

El alcance de los ciberdelitos en el ámbito logístico es complejo de dimensionar, debido a la constante evolución de las tecnologías disruptivas. Esta dinámica exige el diseño de procesos de prevención y seguimiento que sean flexibles y adaptativos, aunque ello representa un reto para las autoridades, que deben responder a amenazas que cambian más rápido que los mecanismos de control disponibles.

Este problema afecta por igual a grandes, medianas y pequeñas empresas. A pesar de los esfuerzos internacionales mediante convenios e iniciativas para prevenir la ciberdelincuencia, aún persisten vacíos en la implementación efectiva de medidas que reduzcan los factores de riesgo en los sistemas logísticos. La participación activa del sector empresarial es clave para fortalecer la resiliencia organizacional.

En el caso colombiano, los datos del Centro Cibernético de la Policía evidencian debilidades estructurales en las organizaciones para mitigar los riesgos cibernéticos asociados a la cadena de suministro. La falta de preparación y la escasa identificación de vulnerabilidades entre los actores logísticos incrementan los riesgos y dificultan su control.

Es urgente implementar medidas que frenen el avance de estructuras delictivas que vulneran los sistemas de empresas públicas y privadas. Esto implica no solo políticas públicas, sino también mecanismos legales que faciliten la investigación y judicialización de los responsables. En paralelo, se destacan avances tecnológicos como el uso de blockchain e inteligencia artificial, que ofrecen soluciones eficientes para tareas logísticas rutinarias y fortalecen la toma de decisiones.

Las empresas deben estar mejor capacitadas e informadas sobre los desarrollos tecnológicos emergentes. Aunque las tecnologías disruptivas ofrecen ventajas operativas, también representan herramientas de alto potencial para actores ilícitos, por lo que su uso debe estar acompañado de estrategias de seguridad robustas.

En este sentido, la prevención se consolida como la estrategia más efectiva. No basta con adoptar medidas reactivas; es necesario actuar de forma corresponsable con las autoridades, promoviendo la denuncia y aplicando mecanismos que reduzcan los factores facilitadores de la ciberdelincuencia. Tal como se evidenció durante la pandemia, la logística disruptiva fue clave

para responder a la demanda global de envíos y compras en línea, lo que obliga a las organizaciones a fortalecer sus sistemas de abastecimiento tanto internos como externos, con criterios de seguridad, eficiencia y sostenibilidad.

## Referencias

Ardila, I. (2014). 5 disrupciones en la tradicional cadena de valor. *P&M*. https://revistapym.com.co/destacados/las-5-disrupciones-tradicional-cadena-valor

Barleta, E., Pérez, G., & J, R. (2019). La revolución industrial 4.0 y el advenimiento de una logística 4.0. *Boletínn 375*. https://repositorio.cepal.org/bitstream/handle/11362/45454/S2000009_es.pdf?sequence=1&isAllowed=y

Bartolomé, M. (2021). *La Ciberseguridad en la segunda década del siglo 21. Curso Ciberseguridad y Seguridad Pública, del CID.*

Cabezas, S. (2017). Aproximación a las principales teorías de la criminalidad ambiental. *Qdc(37)*. https://revistaqdc.es/aproximacion-a-las-principales-teorias-de-la-criminologia-medioambiental/

Camacho, J. (s.f). La prevención del delito situacional. https://popcenter.asu.edu/sites/default/files/library/pdfs/espanol/scp_esp.pdf

Campos, R., & Pérez, G. (2021). Vehículos autónomos y energías alternativas para la logística postpandemia. *Boletín FAL*. https://repositorio.cepal.org/handle/11362/47385

Carvajalino, S. (2020). *Tendencias tecnológicas en la logística 4.0 para el seguimiento de mercancía: un estado del arte.* Bogotá.

Castillo, M. (12 de diciembre de 2016). *Tecnologías disruptivas en la era digital.* Comisión Económica para América Latina y el Caribe: https://www.cepal.org/sites/default/files/events/files/01_mario_castillo_-_tecnologias_disruptivas_en_la_era_digital.pdf

Centro Europeo de Posgrado México. (3 de marzo de 2021). *Qué es una cadena de suministros?* . https://www.ceupe.mx/blog/que-es-una-cadena-de-suministro.html

Centro Superior de Estudios de la Defensa Nacional. (2015). *Tecnologías disruptivas y sus efectos sobre la seguridad.* http://www.ieee.es/Galerias/fichero/docs_trabajo/2015/DIEEET12-2015_Tecnologias_Disruptivas_EfectosSeguridad.pdf

CEPAL. (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe.* Publicación de las Naciones Unidas. https://repositorio.cepal.org/bitstream/handle/11362/47240/1/S2100485_es.pdf.

Díaz, R. (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe.* Santiago: CEPAL.

Dimaté, J., & Rubio, J. (2019). *Ventajas de la tecnología disruptiva en la logística del transporte terrestre ben Colombia en el tramo Bogotá-Villacencio [Trabajo de Grado].* Fundación Universitaria San Mateo. http://caoba.sanmateo.edu.co/jspui/bitstream/123456789/185/1/TECNOLOGIAS%20DISRUPTIVAS.pdf

Dirección de Investigación Criminal e Interpol. (2022). *Balance de Ciberseguridad.* Bogotá.

Espinel Abogados. (9 de Mayo de 2022). *Espinel Abogados*. https://espinelabogados.com/noticias/tecnologias-disruptivas-en-energia-renovable/

Felson, M., & Clarke, R. (2008). *La ocasión hace al ladrón. Teoría práctica para la prevención del delito.* http://repositorio.gobiernolocal.es/xmlui/bitstream/handle/10873/855/claves06_09_felson_clarke.pdf

Fundación Telefónica. (2016). *Ciberseguridad, la seguridad, la protección de la información en un mundo digital.* Madrid: Ariel.

Globalización.com. (s.f). *¿Qué es la globalización tecnológica".* https://www.queeslaglobalizacion.com/globalizacion-tecnologica.htm

Gutiérrez, C. (24 de noviembre de 2019). La creciente digitalización en la logística aumenta la necesidad de invertir en ciberseguridad. *El mercantil*. http://elmercantil.com/2019/11/24/la-creciente-digitalizacion-en-la-logistica-aumenta-la-necesidad-de-invertir-en-ciberseguridad/

Gutiérrez, R. (22 de febrero de 2017). *Logística Disruptiva.* https://revistadelogistica.com/logistica/logistica-disruptiva/

Herrera, A. (2017). Logística disruptiva, tendencia global. https://www.diariodelexportador.com/2017/10/logistica-disruptiva-tendencia-global.html

Mariano, R. (2022). *Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe.* CEPAL. https://repositorio.cepal.org/bitstream/handle/11362/48065/S2200203_es.pdf?sequence=1&isAllowed=y

Marketing digital. (s.f). *Tecnologías disruptivas un reto para la ciberseguridad.* http://marketing-digital.web360.com/digital/tecnologias-disruptivas-un-reto-para-la-ciberseguridad/

Márquez, J., Prieto, A., & Castañeda, L. B. (2024). *Industria 4.0. Internet de las Cosas: ciberseguridad y aplicaciones.* Sello editorial Universidad de Cundinamarca. https://doi.org/10.36436/9786287621862

Matovelle, L., & Dabirian, R. (septiembre de 2015). Introducción a la Tecnología Disruptiva y su Implementación en Equipos Científicos. *Revista Politécnica, 36*(3). https://revistapolitecnica.epn.edu.ec/images/revista/volumen36/tomo3/IntroduccionalaTecnologiaDisruptivaysuImplementacionenEquiposCientificos.pdf

Pérez, G. (2019). OPINIÓN: La tecnología disruptiva en la cadena de valor. *Expansión*. https://expansion.mx/opinion/2019/03/06/opinion-la-tecnologia-disruptiva-en-la-cadena-de-valor

Portafolio. (26 de julio de 2019). *"Somos el 'partner' en transformación digital y ciberseguridad".* https://www.portafolio.co/contenido-patrocinado/somos-el-partner-en-transformacion-digital-y-ciberseguridad-531964

RAE. (s.f). *Disruptivo.* https://dle.rae.es/disruptivo

Redacción Tecnósfera. (2019). *Cibercrimen le cuesta a Colombia 190.000 millones de pesos al año*. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cibercrimen-le-cuesta-a-colombia-190-000-millones-de-pesos-al-ano-380830

Rueda, H., Buelvas, M., & Rocha, L. (2022). 163Uso de las tecnologías disruptivas en las cadenas de suministro para el soporte a la sostenibilidad empresarial. *Red Internacional de Investigadores en Competitividad XVICongreso*. https://riico.net/index.php/riico/article/view/2113/1923

Russo, F. (s.f). *¿Qué es la innovación disruptiva y cómo puedo aplicarla a mi empresa?* https://tentulogo.com/innovacion-disruptiva-que-es-como-aplico-modelo-de-negocio-en-mi-empresa/

Tundidor, A., Hernández, E., Peña, C., Martínez, J., Campos, J., & Hernández, C. (2018). *Cadena de suministro 4.0.* Marge Books.

https://books.google.es/books?id=LjB8DwAAQBAJ&dq=tecnolog%C3%ADas+disruptivas+y+cadenas+de+suministro&lr=&hl=es&source=gbs_navlinks_s

Vilanova, N. (22 de enero de 2018). *La innovación disruptiva, gran reto empresarial.* https://www.larepublica.co/analisis/nuria-vilanova-509356/la-innovacion-disruptiva-gran-reto-empresarial-2590526

Zúñiga, A. (2020). *Tecnologías 4.0 al servicio de la logística en la pospandemia.* https://americana.edu.co/medellin/wp-content/uploads/2020/09/Diagn%C3%B3stico-estrategias-e-innovaci%C3%B3n-empresarial.pdf#page=265