
Vigilancia tecnológica:
El ojo invisible en la era digital
RED educativa digital
escartes

Vigilancia Tecnológica: El ojo invisible en la era digital

John Jairo García Mora
Sonia Jaquelliny Moreno Jiménez

Instituto Tecnológico Metropolitano
Grupo de Investigación GNOMON

Fondo Editorial RED Descartes

Córdoba (España)
2024

Título de la obra:
Vigilancia Tecnológica: El ojo invisible en la era digital

Autores:
John Jairo García Mora
Sonia Jaquelliny Moreno Jiménez

Código JavaScript para el libro: Joel Espinosa Longi, IMATE, UNAM.
Recursos interactivos: DescartesJS
Fuentes: Lato y UbuntuMono
Portada: Imagen de Firefly.adobe.com

Red Educativa Digital Descartes
Córdoba (España)
descartes@proyectodescartes.org
https://proyectodescartes.org

Proyecto iCartesiLibri
https://proyectodescartes.org/iCartesiLibri/index.htm

ISBN: 978-84-10368-07-1

Tabla de contenido

Prefacio

Antes de que el lector se entere de lo que va a encontrar al interior de este libro interactivo, es necesario que se oriente sobre lo que es una vigilancia tecnológica y para que se utiliza además de sus características.

Una definición de lo que se conoce como VIGILANCIA TECNOLÓGICA hace referencia a que es un proceso sistemático y continuo cuya intención es compendiar, detallar y promulgar lo datos releventes que caracterizan el entorno tecnológico de una empresa, organización o país. Esta información es el soporte de la toma de decisiones informadas cuando se investiga y desarrolla tecnología, al administrar la propiedad intelectual de sus creaciones, al detectar oportunidades y amenazas o cuando se pretende identificar las tendencias y cambios en el mercado.

La vigilancia tecnológica tiene como objetivos:

- Identificar oportunidades y amenazas en el entorno tecnológico.
- Monitorear la actividad de la competencia.
- Mantenerse actualizado sobre las últimas tendencias y desarrollos en el mercado.
- Detectar nuevas tecnologías y evaluar su potencial.
- Mejorar la toma de decisiones estratégicas.

Para conseguir dichos objetivos una vigilancia tecnológica debe caracterizarse porque:

- Sea un proceso sistemático y continuo.

- Sus acciones se enfoquen a la recolección, análisis y difusión de información relevante del contexto donde se lleve a cabo.
- Que sus resultados permitan la toma de decisiones estratégicas beneficiosas para el ejecutor de esa vigilancia.
- Se oriente hacia el entorno tecnológico y sus cambios.
- Se convierta en una actividad proactiva que busca anticiparse a los cambios en el mercado.

Por todos es sabido, comprobado o intuido que, en la era digital actual, la tecnología ha cambiado nuestra forma de vida de muchas maneras, incluida la forma en que nos comunicamos, trabajamos y socializamos. Esa nueva forma de vida ha dado lugar a una creciente preocupación por la vigilancia y la privacidad. Este libro explora las diferentes formas de vigilancia tecnológica, sus implicaciones y el equilibrio entre la seguridad y la privacidad de las personas en el siglo XXI.

En un primer capítulo abordamos la evolución de la vigilancia desde sus primeros días hasta la era digital, incluyendo la historia de los dispositivos de vigilancia, como cámaras y micrófonos, y cómo han evolucionado con el tiempo.

En este capítulo 1 encontraremos detalles de los objetivos y los conceptos prácticos de Vigilancia Tecnológica y, además, como se lleva a cabo una planeación ágil de la Vigilancia Tecnológica.

Luego en un segundo capítulo se detalla cómo se realiza la búsqueda y captura de datos, así como las herramientas de vigilancia y las estrategias requeridas para ejecutar convenientemente una vigilancia tecnológica en cualquier contexto.

El capítulo 3 hace referencia a la importancia de la inteligencia para llevar a cabo una vigilancia tecnológica y a la puesta en valor de la información, definida como un componente esencial para que la vigilancia tecnológica sea efectiva, ya que permite transformar datos en conocimiento útil y aplicable que pueda ser utilizado para la toma de decisiones estratégicas.

Es en este tercer capítulo donde se ilustrará la forma de utilización de los resultados y como aplicarlos en un proyecto porque una vez que la información ha sido valorada y transformada en conocimiento útil, es necesario difundirla adecuadamente a las personas o áreas responsables de la toma de decisiones. Esto puede involucrar la creación de informes y análisis detallados, la organización de reuniones y presentaciones, o la integración de los resultados de la vigilancia tecnológica en los procesos de planificación y toma de decisiones como un proyecto de la empresa u organización.

Luego, en un cuarto capítulo haremos referencia al análisis de patentes como herramientas de vigilancia tecnológica ya estas son documentos legales que protegen las invenciones y proporcionan detalles técnicos específicos sobre cómo funcionan nuevos productos, procesos o tecnologías. Al analizar patentes, se pueden obtener beneficios significativos para la vigilancia tecnológica.

En el capítulo quinto se explorará cómo la vigilancia, cuando se aplica de manera ética y legal en el ámbito empresarial, puede transformarse en inteligencia competitiva. Se discutirán temas como el monitoreo de competidores, el análisis del mercado y las tendencias de la industria, la vigilancia tecnológica, la identificación de riesgos y oportunidades legales y regulatorias, y la evaluación de la cadena de suministro y socios comerciales. Además, se abordarán las consideraciones éticas y legales al realizar la vigilancia en el ámbito empresarial.

En un sexto capítulo se generalizarán la ética como disciplina general aplicada a una vigilancia tecnológica de cualquier tipo, se abordan las implicaciones éticas y legales de la vigilancia tecnológica, incluidos los debates sobre la privacidad, la seguridad y el derecho a la libertad de expresión. Se discutirán las leyes y regulaciones existentes en diferentes países y cómo estas afectan a la vigilancia tecnológica.

En el capítulo siete el lector puede, a partir de un video creado por una inteligencia artificial sobre la historia de la protección de los datos o cifrado encontrar una descripción de como pueden ser violados y algunos consejos y estrategias sobre cómo protegerse de la vigilancia tecnológica y mantener la privacidad en la era digital. Se discutirán temas como la ciberseguridad, el cifrado y la importancia de la educación digital.

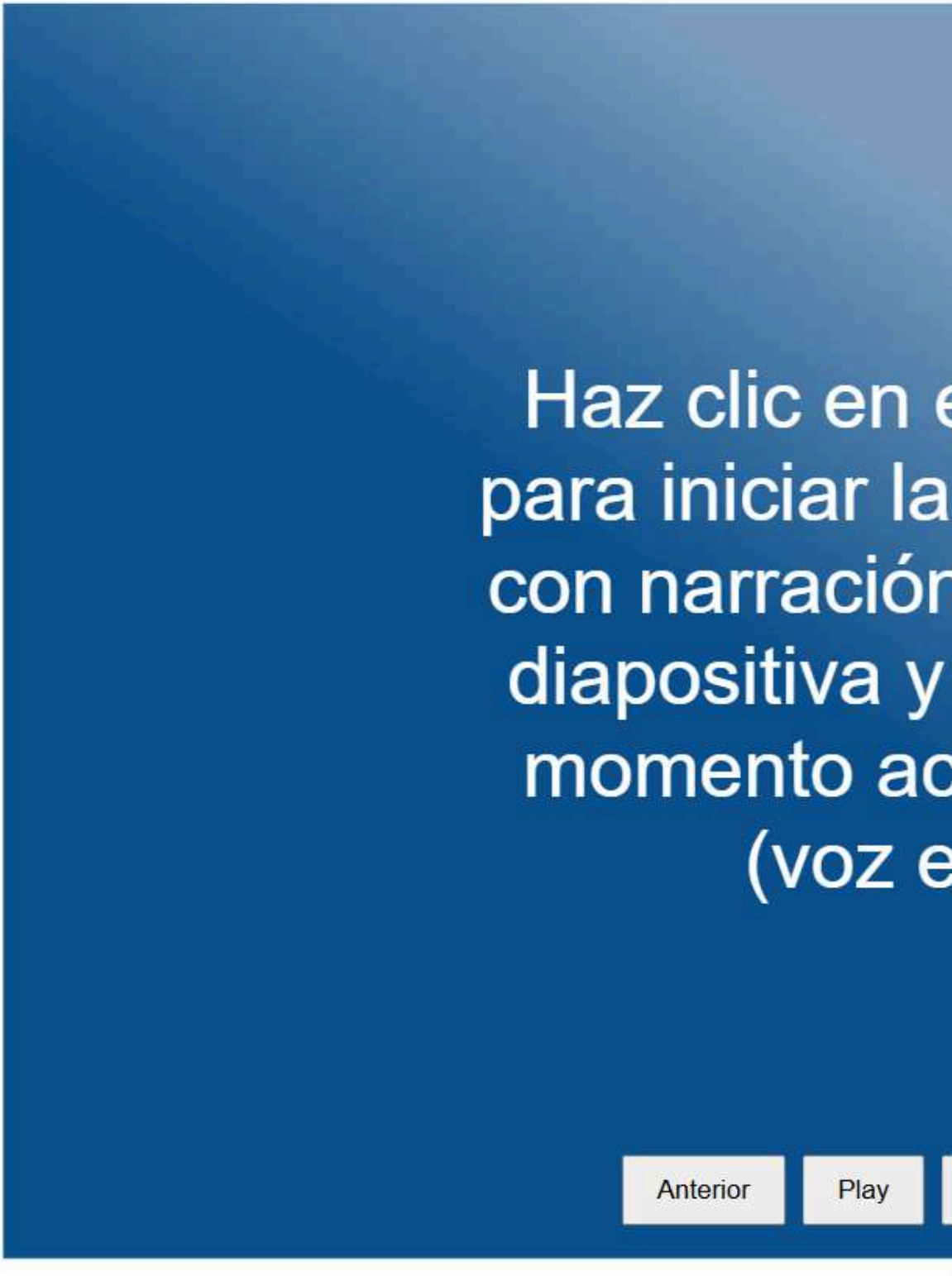
Un capítulo 8 muestra una proceso de vigilancia tecnológica en el campo educativo descrito como el enfoque prospectivo orientado hacia la identificación de oportunidades y amenazas del grupo de investigación del grupo GNOMON-ITM. con miras a obtener un posicionamiento dentro de la institución, se utilizaron dos enfoques para analizar las posibilidades prospectivas de I+D en el contexto de la Industria 4.0 y la educación.

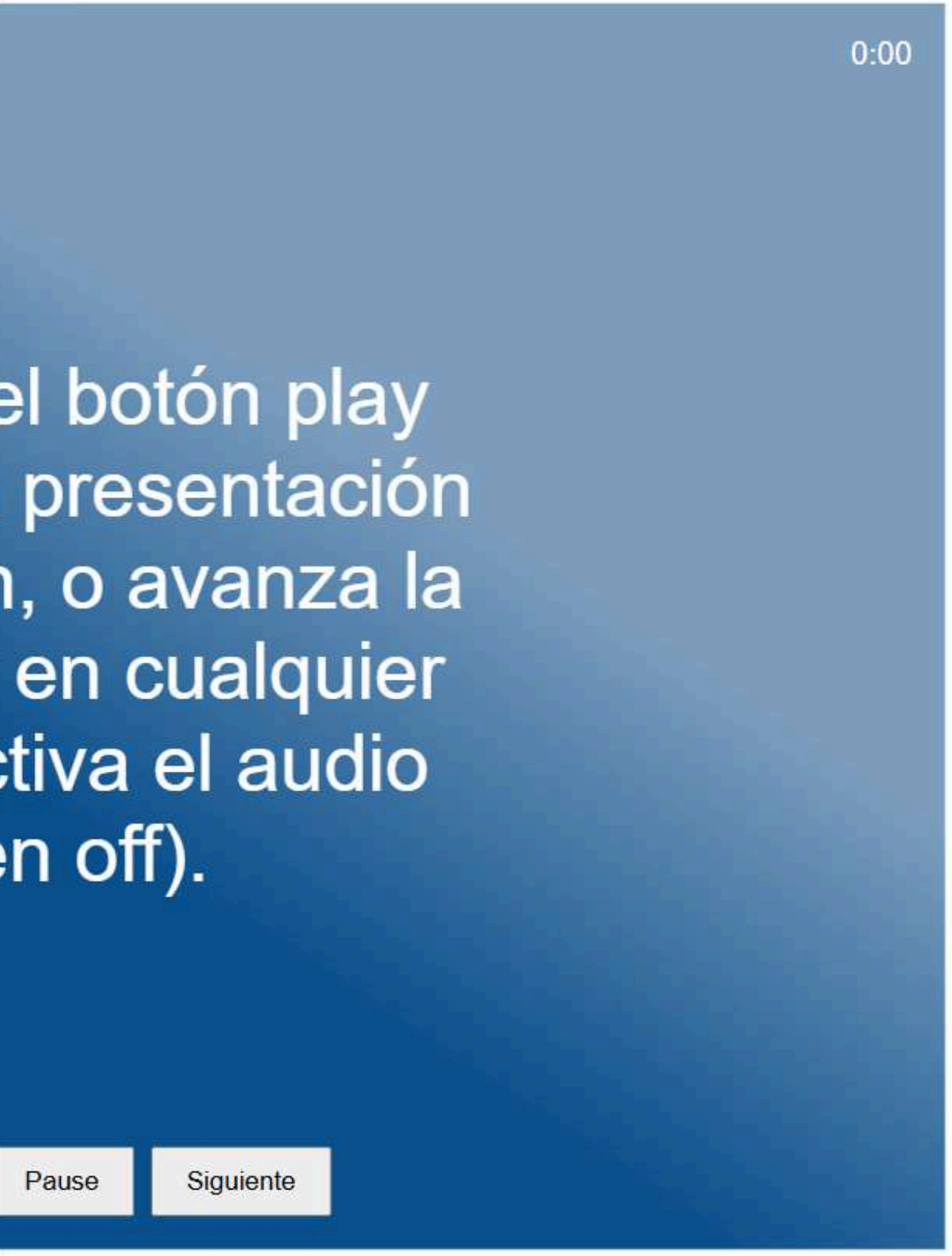
Por último, el noveno capitulo a manera de epílogo se presenta una diseño realizado con el apoyo de una IA, este es presentado en forma de chatbot. Es una herramienta de la era donde la inteligencia artificial toma cada día más ventaja y qué a pesar de ello genera interrogantes pesimistas.

Este chatbot que presentamos está alimentado con la producción académica de los autores.

Lo descrito hasta este momento será ilustrado mediante escenas interactivas propias de los autores o ajustadas del subproyecto Plantillas del Proyecto Descartes, con videos interactivos propios o con licencias Creative Commons y además, el lector encontrará las referencias bibliográficas y los créditos a los autores de las imágenes utilizados a lo largo del libro.

Otro aspecto destacable del libro es la utilización de herramientas y recursos de la Inteligencia Artificial conocida como IA, entre ellas hemos adaptado algunas del libro "Plantillas para libros con inteligencia artificial" escrito por Juan Guillermo Rivera Berrío y Jesús María Calle publicado por el "Fondo Editorial RED Descartes", a continuación, una presentación con los momentos de una vigilancia tecnológica: la orientación de este texto.


Haz clic en e
para iniciar la
con narración
diapositiva y
momento ac
(voz e
Anterior
Play


0:00
el botón play
presentación
n, o avanza la
en cualquier
ctiva el audio
en off).
Pause
Siguiente


CAPÍTULO I
Historia de la vigilancia tecnológica

1.1 Introducción

La vigilancia ha sido un aspecto fundamental en la historia humana, desde los primeros sistemas de espionaje hasta las tecnologías de vigilancia modernas. A medida que la tecnología ha avanzado, también lo han hecho los métodos y dispositivos de vigilancia. Este capítulo aborda la evolución de la vigilancia desde sus primeros días hasta la era digital, destacando la importancia de entender cómo la vigilancia ha influido y sigue influyendo en nuestra sociedad.

1.2 Antecedentes históricos

La vigilancia ha existido desde tiempos antiguos, cuando los gobernantes y líderes militares utilizaban espías para obtener información sobre sus enemigos y mantener el control sobre sus propios territorios. Durante la antigüedad, las ciudades-estado griegas y el Imperio Romano empleaban sistemas de espionaje y vigilancia para proteger sus intereses y mantener la estabilidad política. Un ejemplo de ello fue el sistema de espionaje y vigilancia del Imperio Persa.

Considerado uno de los primeros y más sofisticados sistemas de espionaje y vigilancia de la historia antigua fue desarrollado por el Imperio Persa (c. 550-330 a.C.).

Los persas, bajo el gobierno de Ciro el Grande y sus sucesores, construyeron un vasto imperio que abarcaba desde el Mediterráneo hasta la India. Para mantener la estabilidad y el control en un territorio tan grande y diverso, los persas implementaron un eficiente sistema de espionaje y vigilancia.

Los ***"ojos y oídos del rey"*** eran agentes secretos y espías al servicio del emperador persa que recopilaban información y vigilaban a funcionarios y ciudadanos por todo el imperio. Estos agentes estaban entrenados para mezclarse con la población local, adquirir información a través de la observación y el interrogatorio, y reportar sus hallazgos directamente al rey.

Además de utilizar espías, el Imperio Persa también desarrolló un extenso sistema de comunicación llamado la "Ruta Real", que conectaba todas las provincias del imperio a través de una red de caminos y estaciones de relevo. Esta red permitía el rápido intercambio de información y mensajes entre el rey y sus gobernadores provinciales, lo que facilitaba la coordinación de esfuerzos de vigilancia y el mantenimiento del control sobre el vasto territorio persa.

El sistema de espionaje y vigilancia del Imperio Persa sirve como un ejemplo temprano de cómo las sociedades antiguas utilizaban la vigilancia para mantener el control y proteger sus intereses. Aunque las tecnologías y métodos de vigilancia han cambiado drásticamente a lo largo de la historia, este ejemplo muestra que la necesidad de información y control ha sido una constante en las civilizaciones humanas desde sus primeros días.

1.3 La era preindustrial

Con el advenimiento de la era preindustrial, se desarrollaron nuevas formas de vigilancia. La invención de la imprenta en el siglo XV permitió la circulación masiva de información, lo que llevó a la necesidad de controlar y monitorear la información y las comunicaciones. Los sistemas postales y las redes de mensajeros también jugaron un papel importante en la vigilancia durante este período.

En la era preindustrial, especialmente con la invención de la imprenta y el desarrollo de sistemas postales y redes de mensajeros, condujo al surgimiento de nuevas formas de vigilancia. A continuación, se presentan ejemplos adicionales que ilustran este punto:

La censura de libros en Europa

Con la invención de la imprenta en el siglo XV, la producción y distribución de libros se hizo más accesible y económica. Sin embargo, esto también condujo a la preocupación de las autoridades políticas y religiosas por el control de la información. Como resultado, se establecieron sistemas de censura y control de libros en varios países europeos, como el Índice de Libros Prohibidos de la Iglesia Católica [1], que enumeraba los libros considerados heréticos o inmorales. La censura de libros es un ejemplo temprano de vigilancia y control de la información en la era preindustrial.

El servicio de correos de Thurn und Taxis

En el siglo XVI, la familia Thurn und Taxis estableció un servicio postal que conectaba muchas ciudades y regiones de Europa. Esta red de mensajeros permitió la transmisión de información a larga distancia y fue utilizada tanto por particulares como por gobiernos. Sin embargo, también dio lugar a la vigilancia y el control gubernamental de las comunicaciones, ya que los gobiernos podían acceder fácilmente a la información enviada a través de la red postal.

Los espías de la Revolución Francesa

Durante la Revolución Francesa a fines del siglo XVIII, el Comité de Salvación Pública, una rama del gobierno revolucionario, estableció una red de espías e informantes para vigilar a los ciudadanos franceses y identificar a aquellos que eran considerados enemigos de la revolución.

Este sistema de vigilancia incluía la interceptación y apertura de cartas, la infiltración en grupos políticos y sociales, y la recopilación de información sobre las actividades y opiniones de los ciudadanos. La Revolución Francesa es un ejemplo de cómo la vigilancia fue utilizada en la era preindustrial para controlar y mantener el poder político.

Estos casos demuestran cómo la era preindustrial llevó al desarrollo de nuevas formas de vigilancia, particularmente en relación con el control de la información y las comunicaciones. Aunque los métodos y tecnologías de vigilancia de la época eran más rudimentarios que los de hoy en día, estos ejemplos ilustran la importancia y el impacto de la vigilancia en la sociedad preindustrial.

Dado que el punto en discusión se refiere a la era preindustrial (aproximadamente entre los siglos XVI y XVIII), no hay videos contemporáneos que respalden directamente este punto, ya que el video no existía en ese momento histórico. Sin embargo, hay documentales, películas y programas de televisión que abordan temas de la era preindustrial y pueden incluir discusiones sobre vigilancia y control de información. Por eso recomendamos al lector algunos recursos que podrían ser de interés:

- Documentales históricos

Existen documentales que cubren períodos históricos específicos y eventos relacionados con la vigilancia y el control de información en la era preindustrial. Estos documentales a menudo incluyen recreaciones y análisis de expertos para proporcionar contexto y comprensión de las prácticas de vigilancia de la época. Puedes buscar documentales que se centren en la historia de la censura, la imprenta, la Revolución Francesa, la Inquisición, entre otros temas.

- Series de televisión y películas históricas

Algunas series de televisión y películas históricas también pueden tocar temas de vigilancia y espionaje en la era preindustrial. Aunque estas producciones son principalmente de ficción y no son fuentes académicas o documentales, pueden ofrecer una idea de cómo la vigilancia pudo haber sido llevada a cabo en ese tiempo. Un ejemplo es la serie de televisión "The Tudors", que retrata el reinado de Enrique VIII de Inglaterra y toca temas de espionaje y control político.

- Conferencias y charlas en línea

Existen conferencias y charlas en línea de expertos en historia que abordan temas de vigilancia y control de información en diferentes períodos históricos. Estas presentaciones pueden estar disponibles en plataformas como YouTube o sitios web de universidades e instituciones de investigación. Algunos ejemplos de temas relevantes incluyen la historia de la censura y la imprenta, la Inquisición y el control de información en la Europa medieval y renacentista.

Al investigar y utilizar estos recursos, los autores destacan la importancia de verificar la calidad y confiabilidad de las fuentes y considerar el contexto histórico en el que se desarrollan los temas de vigilancia y control de información.

Según lo expuesto acerca de la información disponible sobre un tema histórico, es difícil encontrar artículos actuales de periódicos que cubran directamente la vigilancia en la era preindustrial. Sin embargo, pretendemos impulsar la búsqueda de recursos en línea como una práctica del aprendizaje por investigación abordando estos temas de manera académica o histórica.

A continuación, se presentan algunos enlaces y sitios web donde se puede encontrar información sobre la historia de la vigilancia y el control de información en la era preindustrial:

- La imprenta y la censura

"Printing and Censorship"(Biblioteca Británica), este artículo ofrece información sobre la relación entre la imprenta y la censura en la historia europea.

- La historia de la censura de libros

"A Brief History of Book Burning, from the Printing Press to Internet Archives" (Smithsonian Magazine). Este artículo del Smithsonian Magazine proporciona una visión general de la historia de la censura de libros y la quema de libros desde la invención de la imprenta hasta la era digital.

- La Revolución Francesa y la vigilancia

(The British Museum Blog). Este artículo del blog del British Museum examina la vigilancia y el espionaje durante la Revolución Francesa y su legado en la historia.

1.4 La revolución industrial del siglo XVIII

La Revolución Industrial en el siglo XVIII [2] trajo consigo importantes avances tecnológicos, lo que permitió el desarrollo de los primeros dispositivos de vigilancia. Por ejemplo, la invención del telégrafo en 1837 permitió la transmisión de información a larga distancia, lo que facilitó el monitoreo y la interceptación de comunicaciones.

Veamos en la siguiente escena algunos de los inventos que provocaron esa revolución y que al mismo tiempo formaron las bases del espionaje industrial:

La Revolución Industrial y los primeros dispositivos de vigilancia

La Revolución Industrial, que tuvo lugar entre mediados del siglo XVIII y principios del siglo XIX, marcó una época de cambios y avances tecnológicos sin precedentes. Estos avances permitieron el desarrollo de los primeros dispositivos de vigilancia y sentaron las bases para las prácticas de vigilancia modernas.

El telégrafo, inventado por Samuel Morse en 1837, fue uno de los primeros avances en comunicaciones que transformaron la manera en que la información era transmitida y monitoreada.

El telégrafo permitió la transmisión rápida y eficiente de información a larga distancia, lo que revolucionó la comunicación y tuvo un profundo impacto en la vigilancia. Los gobiernos y otras organizaciones podían utilizar el telégrafo para monitorear e interceptar comunicaciones, lo que les permitía mantener un control más estricto sobre la información y detectar actividades sospechosas o enemigas.

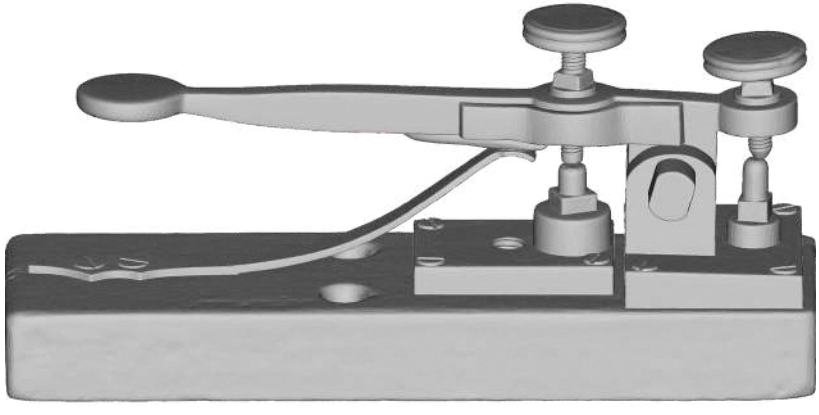


Figura 1.1. Telégrafo

Un ejemplo histórico de esto fue el uso del telégrafo durante la Guerra Civil Americana, también conocida como la Guerra de Secesión que duró 4 años, donde tanto la Unión como la Confederación emplearon a especialistas en criptografía para interceptar y descifrar mensajes enemigos.

Luego surgió una herramienta de vigilancia que permitía la captura y el almacenamiento de imágenes: la cámara fotográfica y que fue creada por varios inventores en diferentes momentos de la historia. Sin embargo, la primera cámara fotográfica práctica fue desarrollada por el francés Louis Daguerre en 1839. Esta cámara, conocida como la cámara Daguerrotipo, utilizaba una placa de cobre plateado y tratado químicamente para producir imágenes fotográficas.

Otro inventor, William Henry Fox Talbot, también había desarrollado un proceso fotográfico en papel a mediados de la década de 1830, pero la cámara Daguerrotipo se convirtió en el primer proceso fotográfico práctico. Desde entonces, la tecnología de la cámara fotográfica ha evolucionado enormemente y ha permitido el desarrollo de la fotografía moderna.

Figura 1.2. Cámara fotográfica

1.5 El siglo XX y la era electrónica

El siglo XX marcó una era de rápido avance tecnológico, con la invención de dispositivos electrónicos y sistemas de comunicación que revolucionaron la vigilancia. La invención del teléfono en 1876 y la radio en la década de 1890[3] permitió una comunicación más rápida y eficiente, pero también facilitó la vigilancia a gran escala. Durante las Guerras Mundiales y la Guerra Fría, la vigilancia se convirtió en una herramienta esencial para la inteligencia militar y la seguridad nacional, con el desarrollo de tecnologías como el radar y las escuchas telefónicas.

Antes del auge de la tecnología digital, también surgieron diversos dispositivos de vigilancia no digitales que se utilizaron para recopilar información sobre individuos y grupos. Veamos algunos de estos dispositivos son:

- Micrófonos ocultos

Los micrófonos ocultos, también conocidos como "bugging devices", se utilizan para grabar conversaciones sin el conocimiento de los participantes. Estos dispositivos se han utilizado en investigaciones criminales y de inteligencia.

- Grabadoras de cinta

Las grabadoras de cinta se utilizan para grabar conversaciones, reuniones y discursos. Estos dispositivos se han utilizado en entrevistas y en investigaciones periodísticas.

- Cámaras espía

Las cámaras espía se utilizan para grabar imágenes de personas y lugares sin su conocimiento. Estos dispositivos se han utilizado en investigaciones criminales, en vigilancia privada y en operaciones de inteligencia.

- Binoculares y telescopios

Los binoculares y telescopios se utilizan para observar a personas y lugares a distancia. Estos dispositivos se han utilizado en vigilancia privada y en operaciones de inteligencia.

Para los ***ciudadanos de a pie***, el uso de estos dispositivos de vigilancia debe estar sujeto a regulaciones y restricciones legales para proteger los derechos y la privacidad de las personas.

1.6 La era digital y la vigilancia tecnológica

La era digital, impulsada por la invención de los microprocesadores y la creciente accesibilidad a la informática, ha transformado radicalmente la vigilancia. La aparición de Internet y las redes de comunicación global han permitido la recopilación, almacenamiento y análisis de grandes cantidades de datos personales. La evolución de dispositivos como cámaras de seguridad, micrófonos, drones y sistemas de reconocimiento facial [4] ha facilitado la vigilancia a un nivel nunca antes visto.

Después del teléfono y la radio, surgieron varios dispositivos de vigilancia que han sido utilizados por agencias gubernamentales y de seguridad para recopilar información sobre individuos y grupos. Algunos de los dispositivos de vigilancia que surgieron después del teléfono y la radio incluyen:

- Cámaras de vigilancia

Las cámaras de vigilancia se han utilizado durante décadas para vigilar lugares públicos y privados, incluidos edificios gubernamentales, calles, estacionamientos y tiendas.

- Satélites de vigilancia

Los satélites espaciales se han utilizado para vigilar áreas extensas y para recopilar información sobre la ubicación y el movimiento de objetos y personas en todo el mundo.

Drones

Los drones son aeronaves no tripuladas que pueden ser utilizadas para vigilar lugares inaccesibles o peligrosos, así como para recopilar información sobre personas y grupos. Veamos el Vídeo de Peter Florea de Pixabay como un ejemplo de ello:

Video

Video 1.1. Los drones

El desarrollo de los drones se atribuye a varios inventores y empresas a lo largo de la historia, pero se considera que el primer avión no tripulado fue el Kettering Bug, un avión autopropulsado diseñado por Charles Kettering en 1918 para su uso en la Primera Guerra Mundial.

En los años siguientes, se desarrollaron drones para fines militares, como el Ryan Firebee, desarrollado en la década de 1950 por Ryan Aeronautical Company, y el Predator, desarrollado por la empresa General Atomics en la década de 1990.

En las últimas décadas, la tecnología de drones ha evolucionado y se ha expandido para su uso en aplicaciones civiles.

Entre esas aplicaciones se encuentran la fotografía aérea, la agricultura de precisión, la vigilancia y la entrega de paquetes. Las empresas líderes en el desarrollo de drones incluyen DJI, Parrot, Yuneec y 3D Robotics, entre otras.

- Dispositivos de seguimiento GPS

Los dispositivos de seguimiento GPS se han utilizado para rastrear la ubicación de vehículos y personas y para recopilar información sobre sus movimientos.

El ***GPS (Sistema de Posicionamiento Global)*** fue desarrollado por el Departamento de Defensa de los Estados Unidos [5]. El proyecto fue iniciado en la década de 1970 y fue liderado por la Fuerza Aérea de los Estados Unidos con la colaboración de la Marina y el Ejército.

El desarrollo del GPS fue llevado a cabo por un equipo de ingenieros y científicos del Departamento de Defensa de los Estados Unidos, encabezado por Ivan Getting, quien fue uno de los primeros defensores del uso de satélites para la navegación terrestre.

La primera constelación de satélites GPS fue lanzada en 1978 y el sistema alcanzó su capacidad operativa inicial en 1995. Desde entonces, el GPS se ha utilizado en una amplia variedad de aplicaciones civiles y militares, como navegación de vehículos, control de tráfico aéreo.

Hoy día se emplea para geolocalización, y seguimiento y monitoreo de personas y objetos, entre otros.

- Software de vigilancia en línea

El software de vigilancia en línea se refiere a herramientas y tecnologías diseñadas para monitorear y rastrear la actividad en línea de una persona, ya sea en su computadora o en su dispositivo móvil. Estos programas pueden ser utilizados por empleadores, padres, gobiernos, parejas y otros para monitorear la actividad en línea de una persona.

El video de 31963655 de Pixabay nos puede dar idea de lo que significa esta práctica:

Video

Video 1.2. Vigilancia en línea

Algunos ejemplos de características de software de vigilancia en línea incluyen el monitoreo de correos electrónicos, registros de chat, historial de navegación, grabación de pantalla, monitoreo de actividad en redes sociales, entre otros.

El uso de este tipo de software puede tener implicaciones éticas y legales. En algunos casos, el uso de software de vigilancia en línea puede ser una violación de la privacidad de una persona y puede ser ilegal sin el consentimiento de la persona monitoreada.

Además, algunos empleadores pueden estar sujetos a leyes y regulaciones específicas sobre el monitoreo de la actividad en línea de sus empleados.

Es importante tener en cuenta que el uso de software de vigilancia en línea debe ser evaluado cuidadosamente antes de su uso, es un proceso crítico que debe ser llevado a cabo antes de implementar cualquier solución de monitoreo en línea.

El objetivo de esta evaluación es asegurarse de que el software de vigilancia en línea sea ético, legal y compatible con las políticas y objetivos de la organización o individuo que lo está utilizando.

Copilot de Bing expresa que el éxito de la vigilancia tecnológica mediante software se mide cuando existe una estricta selección de las herramientas adecuadas, cuando se logran sistematizar y monitorear los datos conseguidos entre los que se destacan las fuentes proporcionadas como las bases de datos de patentes, publicaciones científicas, noticias tecnológicas y redes sociales

La evaluación del software de vigilancia en línea puede incluir los siguientes pasos:

- Identificación de necesidades

Comprender las razones detrás del uso del software de vigilancia en línea y determinar los objetivos y los riesgos asociados con la implementación del mismo.

- Análisis de las características del software

Examinar las características del software de vigilancia en línea, incluyendo la funcionalidad, la facilidad de uso, la precisión, la confiabilidad y la seguridad.

- Evaluación de la privacidad

Evaluar cómo el software de vigilancia en línea recolecta, almacena, y utiliza los datos del usuario, y si existe el riesgo de vulnerar la privacidad del usuario monitoreado.

- Evaluación de la legalidad

Verificar si el uso del software de vigilancia en línea cumple con las leyes y regulaciones locales e internacionales relacionadas con la privacidad, la seguridad y el monitoreo de la actividad en línea.

- Evaluación de los riesgos y beneficios

Identificar y evaluar los riesgos y beneficios potenciales asociados con el uso del software de vigilancia en línea, tanto para el individuo que está siendo monitoreado como para la organización o individuo que está llevando a cabo el monitoreo.

- Desarrollo de políticas y procedimientos

Desarrollar políticas y procedimientos para garantizar que el software de vigilancia en línea se utilice de manera ética y legal y se implemente de manera segura y efectiva.

A continuación de algunos softwares más utilizados:

- Spyrix

Este software de vigilancia en línea es una herramienta de monitoreo de computadoras completa que permite rastrear y grabar todas las actividades realizadas en una computadora, incluyendo el historial de navegación, los correos electrónicos, los chats y el uso de aplicaciones.

- FlexiSPY

Este software de vigilancia en línea se enfoca en monitorear dispositivos móviles, y permite rastrear y grabar actividades como llamadas, mensajes de texto, correos electrónicos, chats de redes sociales, y el historial de navegación.

- mSpy

Este software de vigilancia en línea se enfoca en el monitoreo de dispositivos móviles y permite rastrear y grabar actividades como llamadas, mensajes de texto, correos electrónicos, chats de redes sociales, y el historial de navegación.

- Net Nanny

Este software de vigilancia en línea se enfoca en el control parental y permite a los padres monitorear y filtrar el contenido web, así como monitorear las actividades en línea de sus hijos.

- WebWatcher

Este software de vigilancia en línea se enfoca en el monitoreo de computadoras y dispositivos móviles, y permite rastrear y grabar actividades como el historial de navegación, los correos electrónicos, los chats y el uso de aplicaciones.

Al analizar el pasado y el presente de la vigilancia tecnológica, podemos aprender lecciones valiosas y aplicarlas en la búsqueda de un equilibrio adecuado entre la necesidad de protección y el respeto por nuestra privacidad en la era digital.

La inteligencia artificial (IA) está transformando prácticamente todos los aspectos de nuestras vidas, y la vigilancia tecnológica no es una excepción, los asistentes de "Poe", "GPT-4.0-mini" y "Llama-3-70b-Groq" coinciden en los siguientes:

- Sistemas de reconocimiento facial
    - FaceFirst: Un sistema de reconocimiento facial que utiliza aprendizaje automático para identificar a las personas en tiempo real.
    - DeepCam: Un sistema de reconocimiento facial que utiliza inteligencia artificial para analizar imágenes y videos en tiempo real.

- Análisis de actividad en redes sociales
  - Dataminr: Un software que utiliza inteligencia artificial para analizar información en tiempo real de redes sociales y detectar patrones y tendencias.
  - Brandwatch: Una plataforma de análisis de redes sociales que utiliza inteligencia artificial para monitorear y analizar el comportamiento de los usuarios.
- Monitoreo de dispositivos móviles
  - Cellebrite: Una herramienta de forense digital que utiliza inteligencia artificial para analizar y extraer información de dispositivos móviles.
  - MobileIron: Una plataforma de gestión de dispositivos móviles que utiliza inteligencia artificial para monitorear y controlar el uso de dispositivos móviles.
  - Sistemas de detección de anomalías
  - Anomaly Detection by AWS: Un servicio de Amazon Web Services que utiliza inteligencia artificial para detectar patrones anómalos en grandes conjuntos de datos.
  - Splunk: Una plataforma de análisis de datos que utiliza inteligencia artificial para identificar patrones inusuales y anomalías en grandes conjuntos de datos.

El big data se refiere a conjuntos de datos tan grandes y complejos que es difícil procesarlos con las herramientas de gestión de datos tradicionales.

Algunas características clave del big data hacen referencia a que se generan grandes volúmenes de datos que se procesan a gran velocidad así exista variedad de datos en sus formatos, es de anotar que su gran desafío es determinar la veracidad de la calidad de los datos. Es aquí dónde el software que los puede validar podría ser:

- Análisis de Big Data
  - Palantir: Una plataforma de análisis de datos que utiliza inteligencia artificial para procesar y analizar grandes volúmenes de datos de diversas fuentes.
  - SAS Institute: Una plataforma de análisis de datos que utiliza inteligencia artificial para analizar y procesar grandes volúmenes de datos.

- Herramientas de ciberseguridad
  - Darktrace: Un sistema de detección de amenazas que utiliza inteligencia artificial para identificar patrones anómalos en el tráfico de red.
  - Cylance: Un software de seguridad que utiliza inteligencia artificial para detectar y prevenir ataques cibernéticos.


CAPÍTULO II
Tipos de vigilancia tecnológica

Tipos de vigilancia tecnológica

2.1 Introducción

La clasificación del tipo de vigilancia tecnológica se realiza a partir de los objetivos y necesidades específicas de la organización que la realiza.

Algunas de las clasificaciones más comunes para los tipos de vigilancia tecnológica[6].

1. **Según su alcance temporal**

   - Vigilancia tecnológica prospectiva: se enfoca en identificar y analizar las tendencias tecnológicas emergentes que pueden impactar en el futuro.
   - Vigilancia tecnológica retrospectiva: se centra en el análisis de las innovaciones tecnológicas que ya han ocurrido en el pasado y su impacto en el presente.

2. **Según su objeto de vigilancia**

   - Vigilancia tecnológica interna: se realiza dentro de una organización y se enfoca en identificar las capacidades tecnológicas de la empresa y su evolución.
   - Vigilancia tecnológica externa: se enfoca en el análisis de las tendencias tecnológicas y de mercado externas a la organización, para identificar oportunidades y amenazas.

3. **Según su ámbito de aplicación**

- Vigilancia tecnológica general: se enfoca en una amplia gama de tecnologías y campos de aplicación.
- Vigilancia tecnológica especializada: se enfoca en tecnologías específicas y campos de aplicación especializados.

4. **Según el tipo de información que se busca**

- Vigilancia tecnológica básica: se enfoca en la recolección y análisis de información básica sobre la tecnología, como patentes y publicaciones científicas.
- Vigilancia tecnológica avanzada: se enfoca en la recolección y análisis de información más compleja, como la actividad de los competidores, el análisis de patentes y la vigilancia de tendencias.

2.2 El alcance temporal de una vigilancia tecnológica

La elección del alcance temporal de la vigilancia tecnológica dependerá de los objetivos específicos de la empresa y de la información que necesite para tomar decisiones informadas sobre su negocio.

Este tipo de vigilancia tecnológica se efectúa si se desea implementar una estrategia de vigilancia tecnológica para estar al tanto de las últimas tendencias en la industria de la tecnología y anticiparse a los cambios que puedan impactar su negocio.

La temporalidad del alcance sucede cuando una empresa podría optar por realizar una vigilancia tecnológica prospectiva cuyo objetivo consiste en identificar las tendencias tecnológicas emergentes que pueden impactar en el futuro.

Lo anterior se logra monitoreando las últimas investigaciones y desarrollos en áreas como inteligencia artificial, ciberseguridad, computación cuántica, entre otras.

En la siguiente escena diseñada por Juan Guillermo Rivera con ayuda de la AI, podemos visualizar los aspectos que el **MIT Technology Review** fundada en 1899, es la revista sobre tecnología más antigua del mundo y la autoridad global en el futuro de la tecnología en internet, telecomunicaciones, energía, informática, materiales, biomedicina y negocios. La revista destaca con respecto a dichas tendencias lo que apreciamos abajo, el documento puede leerse aquí.

Interactivo 2.1. Tendencias de vigilancia tecnológica prospectiva.

Pero también suele suceder que la empresa que implementa la vigilancia quisiera analizar las innovaciones tecnológicas que ya han ocurrido en el pasado y su impacto en el presente, entonces optaría por una vigilancia tecnológica retrospectiva.

Normalmente la estrategia consiste en analizar el historial de patentes y publicaciones científicas en el área de la tecnología que le interese, para determinar cómo han evolucionado las tecnologías y cómo se han aplicado en diferentes campos.

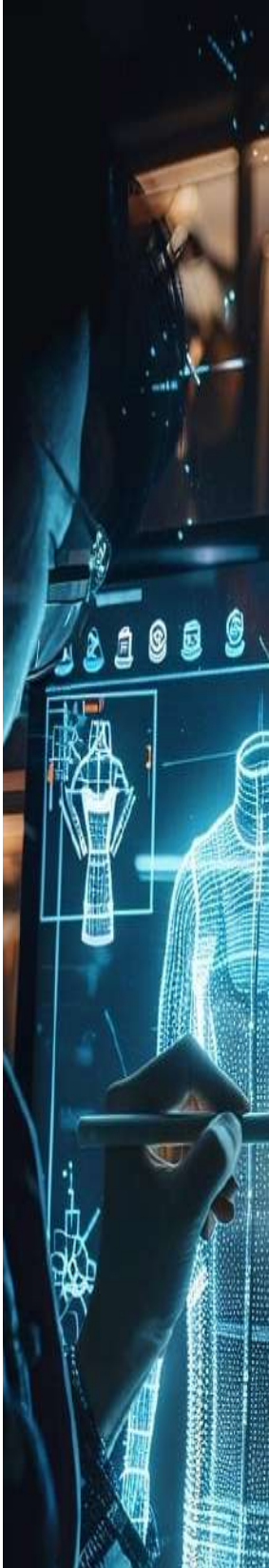
2.3 El objeto de una vigilancia tecnológica

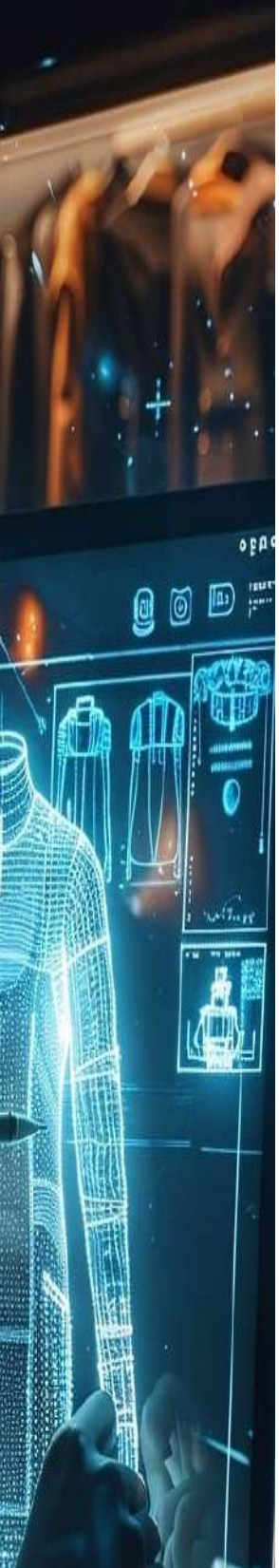
Para poder realizar una vigilancia tecnológica externa, creemos que la vigilancia tecnológica interna da pautas para ello puesto que en una organización se refiere al proceso de monitorear y analizar de manera sistemática el entorno tecnológico en el que opera la organización creando lo que se denomina matriz **DOFA**.

Esta matriz se elabora con el fin de identificar oportunidades, amenazas, tendencias y desarrollos que puedan tener un impacto en su competitividad, innovación y estrategia.

Para este proceso la tecnología juega un rol fundamental [7], ya que brinda diversas posibilidades y beneficios:

- Identificación temprana de tendencias tecnológicas





Utilizando la tecnología existente en la organización se logra rastrear y analizar de cerca las tendencias emergentes en campos relevantes para la organización misma. Esto puede ayudar a la empresa a anticipar cambios en el mercado y a prepararse para adoptar nuevas tecnologías o enfoques.

- Monitorización de competidores y benchmarking

La tecnología de la organización facilita recopilar información sobre las actividades tecnológicas y estratégicas de los competidores. Esto ayuda a la organización a entender cómo se están desarrollando en comparación con otros actores del mercado.

- Detectar aquellas oportunidades de innovación

La vigilancia tecnológica interna contribuye a identificar las oportunidades para innovar y desarrollar nuevos productos, servicios o procesos basados en las últimas tecnologías y tendencias aprovechando sus propiedades intelectuales de sus procesos productivos.

- Evaluación de riesgos y amenazas tecnológicas

El empleo de la tecnología también permite al interior de la organización, identificar posibles riesgos, amenazas y desafíos que puedan surgir en el entorno tecnológico, como cambios regulatorios, avances de la competencia o cambios en la demanda del mercado.

- Mejora de la toma de decisiones estratégicas

Al contar con información actualizada y relevante, la dirección puede tomar decisiones informadas sobre inversiones en investigación y desarrollo, adopción de tecnologías y estrategias de mercado.

Esto último significa que Las inversiones en investigación y desarrollo **(I+D)** y la adopción de tecnologías y estrategias de mercado son dos aspectos fundamentales para el crecimiento, la innovación y la competitividad de una organización.

- Gestionar la optimización de la propiedad intelectual

La vigilancia tecnológica interna puede facilitar la identificación de nuevas oportunidades de propiedad intelectual, así como a proteger los derechos de propiedad intelectual existentes sobre sus procesos.

- Alineación de la estrategia empresarial con la tecnología

La tecnología brinda la capacidad de alinear la estrategia de la organización con las tendencias tecnológicas emergentes, lo que puede ayudar a mantener la relevancia y competitividad en el mercado.

- Mejora de la capacidad de adaptación a la innovación y las nuevas tecnologías

Al estar al tanto de las tendencias tecnológicas, la organización puede adaptarse más rápidamente a los cambios del mercado y a las nuevas condiciones.

2.4 "Metodología para determinar los factores a tener en cuenta en una vigilancia"

Video

Video 2.1. Metodología de vigilancia tecnológica e inteligencia estratégica
Universidad de Antioquia.

Ahora, cuando se realiza la vigilancia interna y se logra una vigilancia externa a la organización y se logra la innovación es porque se halló el punto de equilibrio en el contexto de la vigilancia tecnológica.[8]

Ese equilibrio se refiere al punto en el que una organización logra un balance óptimo entre la inversión y los recursos dedicados a la vigilancia tecnológica interna y externa, de modo que pueda mantenerse al tanto de las tendencias tecnológicas globales y avanzar en su desarrollo de manera competitiva. Este equilibrio implica encontrar la cantidad adecuada de recursos financieros, humanos y tecnológicos para llevar a cabo estas actividades de manera efectiva.

Hallar el punto de equilibrio entre las vigilancias interna y externa, la organización debe considerar varios factores:

1. **Necesidades y objetivos**
2. **Recursos disponibles**
3. **Sector y mercado**
4. **Tecnologías relevantes**
5. **Riesgos y oportunidades**
6. **Ritmo de cambio tecnológico**
7. **Tamaño y alcance de la organización**

2.5 El ámbito de una vigilancia tecnológica

Los diccionarios nos indican que la palabra ámbito puede poseer las siguientes connotaciones:

1. **Espacio comprendido dentro de ciertos límites reales o imaginarios.**
2. **Espacio y conjunto de personas o cosas en que se desarrolla una persona o una cosa.**

Por lo anterior, cuando nos referimos al espacio donde se realiza una vigilancia tecnológico estamos haciendo referencia al proceso sistemático de selección, observación, análisis y difusión de información relevante acerca de los avances, tendencias, novedades y cambios en el ámbito tecnológico y competitivo de una organización o sector en particular. Esta actividad tiene como objetivo principal ayudar a las organizaciones a estar al tanto de los desarrollos tecnológicos y las tendencias del mercado, de manera que puedan tomar decisiones informadas y anticiparse a posibles cambios en su entorno.

Un espacio donde se ejecuta la vigilancia tecnológica puede orientarse a diversas áreas:

- Área tecnológica

Cuando su espacio de ejecución se centra en la búsqueda y seguimiento de avances científicos, desarrollos tecnológicos, patentes, publicaciones científicas y técnicas, así como innovaciones emergentes en diversos campos de la ciencia y la tecnología.

- Campo de la Competitividad

En este espacio de vigilancia tecnológica, el proceso se enfoca en analizar la actividad de la competencia, identificando sus tácticas, productos, servicios y movimientos en el mercado. Esto permite a la organización entender su posición relativa y tomar medidas para mantener o mejorar su competitividad.

- Sistema de Economía y mercadeo

La vigilancia realizada en este sistema implica el monitoreo de tendencias económicas, de mercado y consumidor. Esto incluye análisis de demanda, comportamiento del consumidor, precios, segmentación de mercado y oportunidades emergentes.

- Campo legal

Hace referencia al campo de las regulaciones y normas, aquí una vigilancia tecnológica se concentra en seguir la evolución de regulaciones, leyes y normativas que puedan afectar a la industria o sector en cuestión, incluyendo temas de seguridad, salud y medio ambiente entre otros aspectos que permiten la innovación que se pretende luego del proceso.

No existe una normativa universal única para la vigilancia tecnológica, pero existen ciertos principios generales que pueden aplicarse en diversas jurisdicciones.

Las normas y regulaciones que rigen la vigilancia tecnológica pueden variar dependiendo del país, la industria y el sector en cuestión. Algunas de las áreas en las que pueden influir las normas incluyen la privacidad, la propiedad intelectual y la ética en la recopilación y el uso de datos.

Una vigilancia tecnológica debe ejecutarse con el seguimiento correcto de:

1. **Privacidad y Protección de Datos**

Regulaciones como el **Reglamento General de Protección de Datos (GDPR)** en la Unión Europea [9] y leyes similares en otras regiones, establecen reglas para la recopilación, almacenamiento y procesamiento de datos personales.

El objetivo principal es proteger la privacidad de los individuos y garantizar que sus datos sean utilizados de manera adecuada y segura.

La **Ley Patriota** en Estados Unidos, es una ley federal que permite a las agencias gubernamentales recopilar información sobre ciudadanos estadounidenses y extranjeros en los Estados Unidos, otra ley importante es la **Ley de Vigilancia de Inteligencia Extranjera (FISA)**, que permite al gobierno estadounidense recopilar información sobre ciudadanos extranjeros fuera de los Estados Unidos.

2. **Propiedad Intelectual**

Las leyes de propiedad intelectual, como las patentes, los derechos de autor y las marcas registradas, rigen la protección de los activos intangibles y fomentan la innovación. En la vigilancia tecnológica, es importante respetar los derechos de propiedad intelectual de otros y evitar infringir patentes u otros derechos exclusivos.

3. **Competencia y Antimonopolio**

Las leyes antimonopolio y de competencia buscan prevenir prácticas comerciales desleales y promover la competencia justa en el mercado.

En el contexto de la vigilancia tecnológica, estas leyes pueden influir en cómo se recopila y utiliza la información sobre la competencia.

4. **Ética y Responsabilidad**

Son dos términos que no implican normativas legales en sí, los principios éticos y de responsabilidad son fundamentales en la vigilancia tecnológica. Esto implica la consideración de las implicaciones éticas de la recopilación y el uso de información, así como la transparencia en las prácticas.

5. **Regulaciones Sectoriales**

Algunas industrias específicas pueden estar sujetas a regulaciones adicionales relacionadas con la seguridad, el medio ambiente o la salud.

Estas regulaciones pueden influir en cómo se lleva a cabo la vigilancia tecnológica dentro de un sector particular.

El objetivo principal de estas normas y regulaciones es crear un equilibrio entre la obtención de información valiosa y el respeto por los derechos y la privacidad de las personas, así como el fomento de la competencia y la innovación responsable.

Lo anteriormente descrito implica que una vigilancia tecnológica debe realizarse de manera ética y legal, garantizando que se cumplan todas las leyes y regulaciones aplicables en el proceso de recopilación, análisis y uso de la información relevante.


SECURITY
CAMERA


CAPÍTULO III
Herramientas y técnicas de vigilancia tecnológica
GEOLOCATION

Herramientas y técnicas de vigilancia

3.1 Introducción

En este tercer capítulo se exploran las diferentes herramientas y técnicas utilizadas en la vigilancia tecnológica, incluyendo cámaras de seguridad, reconocimiento facial, geolocalización, metadatos, escuchas telefónicas y otras técnicas de monitoreo digital.

La siguiente línea del tiempo nos da una idea de las principales técnicas empleadas para ejecutar una vigilancia tecnológica:

1. **Observación Empírica**

Técnica que caracterizó la vigilancia tecnológica durante los siglos XVI y XVII, los científicos y artesanos dependían de la observación directa para descubrir nuevos conocimientos y avances técnicos.

2. **Propias de las Sociedades Científicas**

La formación de sociedades científicas y academias durante los siglos XVIII y XIX permitió a los investigadores compartir y difundir información sobre avances tecnológicos.

3. **Patentes y Oficinas de Patentes**

Durante los siglos XIX y XX, La introducción de sistemas de patentes permitió la documentación y protección legal de invenciones, impulsando la vigilancia tecnológica.

4. **El espionaje industrial**

En la década de los años 40 durante el desarrollo de la Segunda Guerra Mundial, el espionaje industrial se intensificó, con agencias gubernamentales y empresas compitiendo por obtener información clasificada.

5. **Análisis de Patentamiento**

En la década de los años 60, las empresas comenzaron a utilizar el análisis de patentes para identificar tendencias tecnológicas y detectar posibles innovaciones de la competencia.

6. **Vigilancia Competitiva**

En la década de los años 70, las empresas establecieron departamentos de vigilancia competitiva para rastrear y analizar la actividad de sus competidores en busca de oportunidades y amenazas.

7. **Bases de Datos y Minería de Datos**

A partir de los años 80, la digitalización permitió el desarrollo de bases de datos tecnológicas y herramientas de minería de datos para identificar patrones y tendencias en grandes conjuntos de información.

8. **Internet y Vigilancia en Línea**

A partir de los años 90, la expansión de Internet facilitó el acceso a información en tiempo real, lo que permitió a las empresas monitorear a sus competidores y el entorno tecnológico de manera más eficiente.

9. **Vigilancia en Redes Sociales**

Con el inicio del siglo XXI, las redes sociales se convirtieron en una fuente valiosa de información para la vigilancia tecnológica, permitiendo el seguimiento de conversaciones y opiniones de los usuarios.

10. **Analítica Avanzada y Aprendizaje Automático**

Las técnicas de analítica avanzada y aprendizaje automático se aplicaron en la década del año 2010 para analizar grandes volúmenes de datos y predecir tendencias tecnológicas.

11. **Inteligencia Artificial y Automatización**

A partir del año 2020 el mundo está viviendo el auge de la inteligencia artificial, esta se está utilizando para automatizar procesos de vigilancia tecnológica, desde la recopilación de datos hasta la generación de insights y recomendaciones

3.2 Vigilancia tecnológica antes del siglo XVII

Aunque no existen evidencias concretas de que la vigilancia tecnológica, tal como la entendemos en la actualidad, haya existido en la prehistoria.

Pero si consideramos que la vigilancia tecnológica implica la recolección y análisis sistemática de información sobre avances tecnológicos, tendencias y novedades en un campo específico para tomar decisiones informadas y mantenerse competitivo, pero si es posible argumentar que en cierta medida, los grupos prehistóricos pudieron haber compartido conocimientos y técnicas a través de la observación directa, la imitación y la transmisión oral.

Si una comunidad descubría una técnica más eficiente para hacer algo, es posible que esa información se transmitiera a otras comunidades cercanas de una manera informal y localizada, y no se asemejaría a la vigilancia tecnológica estructurada que vemos en la actualidad.

En el contexto de la antigua Grecia, se han logrado identificar ciertos elementos que podrían considerarse como antecedentes de la vigilancia tecnológica, aunque no necesariamente se aplicaba de la misma manera que en la actualidad.

Los griegos en la antiguedad eran una civilización altamente innovadora y creativa en campos como la filosofía, las matemáticas, la astronomía, la medicina, la arquitectura y más, aunque no tenían una noción formal de "vigilancia tecnológica", sí había intercambio de información y conocimiento entre diferentes ciudades-estado y áreas geográficas.

Esto permitía que las innovaciones y los desarrollos tecnológicos se difundieran a lo largo del mundo griego.

Los griegos fundaron colonias en diferentes partes del Mediterráneo y el Mar Negro, y estas colonias mantenían contactos comerciales y culturales con la Grecia continental.

A través de estos contactos, se podrían haber difundido nuevas técnicas, conocimientos y tecnologías. Además, los grandes eventos como los Juegos Olímpicos y otros festivales atraían a personas de diferentes regiones, lo que también facilitaba la difusión de conocimientos.

Es aquí donde podemos suponer que los griegos estaban comprometidos con la observación sistemática y el estudio de la naturaleza.

Filósofos como Aristóteles documentaron y analizaron una amplia gama de fenómenos naturales y tecnológicos y aunque no tenían una estructura formal de vigilancia tecnológica, su enfoque en la observación, el análisis y la documentación podría considerarse una forma rudimentaria de adquirir y compartir conocimientos tecnológicos.

Otra cultura que mostró al mundo una serie de avances tecnológicos fue la romana, aunque no practicaban la vigilancia tecnológica de la manera en que la entendemos hoy, también se puede inferir que su expansión territorial, contacto con diversas culturas y énfasis en la ingeniería y la educación contribuyeron a la difusión y adopción de tecnologías y conocimientos en todo su imperio.

Los romanos fueron conocidos por su habilidad para conquistar, administrar y desarrollar vastos territorios.

A medida que expandían su imperio, establecían contactos con diversas culturas y comunidades que les proporcionaban nuevas ideas y tecnologías, veamos algunos elementos relevantes que pudieron ser el foco de una posible vigilancia tecnológica por parte de los romanos:

1. **Ingeniería y Construcción**

Los romanos eran maestros de la ingeniería y la construcción, desarrollando avanzadas técnicas de arquitectura, construcción de carreteras, acueductos y puentes.

Estas innovaciones a menudo se transmitían a través de los ingenieros y arquitectos que trabajaban en diferentes partes del imperio, contribuyendo a la difusión de conocimientos tecnológicos.

Acueducto romano

Figura 3.1. Ingeniería romana

2. **Comunicación y Comercio**

El extenso sistema de comunicación y comercio de los romanos facilitó la difusión de conocimientos y tecnologías a lo largo de su imperio. Las rutas comerciales y los contactos entre diferentes regiones permitieron la transferencia de productos y técnicas innovadoras.

3. **Las artes y las ciencias**

La educación romana valoraba la erudición y el conocimiento, lo que llevó a la acumulación de información y técnicas en campos como la medicina, la agricultura y la metalurgia. Aunque no tenían una estructura formal de vigilancia tecnológica, el interés en el avance de las artes y las ciencias contribuyó a la propagación de conocimientos.

4. **Las conquistas territoriales y la asimilación cultural**

La expansión del imperio romano implicaba la conquista y asimilación de otras culturas y sociedades. Esta integración cultural también llevó a la adopción y adaptación de tecnologías y prácticas de otras civilizaciones, contribuyendo a un intercambio de conocimientos tecnológicos a lo largo y ancho de su imperio.

Ya en la edad media no podemos dejar de hablar d Leonardo Da Vinci, no podemos afirmar de que este haya empleado un proceso formal de vigilancia tecnológica en el sentido moderno para dar a conocer sus investigaciones. Sin embargo, su enfoque multidisciplinario, su insaciable curiosidad y su deseo de explorar y experimentar en una variedad de campos podrían considerarse precursores de ciertos aspectos de la vigilancia tecnológica.

Diseño de Leonardo Da Vinci

Figura 3.2. Modelo de ala de Leonardo Da Vinci

En la figura 3.2 podemos observar el Modelo de ala, de Leonardo Da Vinci, en el Museo Nacional de Ciencia y Tecnología de Milán una contribución de Jakub Hałun en Wikimedia Commons.

Leonardo da Vinci fue un genio renacentista cuyos intereses abarcaban la pintura, la escultura, la anatomía, la ingeniería, la arquitectura, la música, la matemática y muchas otras disciplinas. Mantenía cuadernos de dibujos y anotaciones en los que documentaba sus observaciones y reflexiones en una amplia gama de temas. A través de estos cuadernos, Leonardo exploraba conceptos científicos y técnicos, además de plasmar sus ideas creativas.

Aunque no practicaba la vigilancia tecnológica en el sentido empresarial o industrial, su enfoque en la observación, el análisis y la experimentación podría interpretarse como una búsqueda constante de nuevas ideas y soluciones. Si bien no tenía la intención explícita de compartir sus descubrimientos con otros en el mismo sentido que la vigilancia tecnológica moderna, sus escritos y diseños a menudo inspiraban a otros a expandir y construir sobre sus ideas.

Es importante recordar que Leonardo vivió en una época en la que el intercambio de información y el acceso al conocimiento eran diferentes a los de la actualidad. Sus trabajos y descubrimientos no se difundieron ampliamente durante su vida, y gran parte de su legado fue redescubierto y valorado siglos después de su muerte.

Los egipcios

Los egipcios eran conocidos por su ingeniería y arquitectura avanzadas,aunque no se dispone de evidencia sólida y directa de un sistema formal de vigilancia tecnológica en el antiguo Egipto, existen algunas indicaciones de que los antiguos egipcios estaban interesados en el desarrollo y la aplicación de tecnologías en su sociedad.

Evidencias de esa ingeniería y arquitectura del antiguo Egipto son la construcción de las pirámides y otros monumentos, ello implica una comprensión profunda de la geometría, la mecánica y la logística.

Arquitectura en Egipto

Figura 3.3. Construcción del antiguo Egipto

De esas aplicaciones se puede inferir que la sociedad egipcia estaba activamente involucrada en la creación y mejora de tecnologías para abordar sus necesidades y por lo tanto no se puede descartar algún tipo de vigilancia tecnológica.

Los egipcios desarrollaron técnicas de irrigación y agricultura para aprovechar al máximo el río Nilo y su entorno, lo que refleja un enfoque pragmático en la gestión de recursos.

Además de lo descrito, los egipcios también dominaron la metalurgia, la cerámica y la fabricación de textiles, lo que sugiere una comprensión sólida de la tecnología en esas áreas.

Los antiguos egipcios compartían y transmitían sus conocimientos a través de generaciones. Muchos de los avances tecnológicos y científicos se transmitían oralmente y a través de la práctica, lo que posiblemente funcionaba como un sistema de preservación y evolución de la tecnología.

3.3 La observación: primera herramienta y técnica de vigilancia tecnológica

La observación directa es una estrategia de vigilancia tecnológica que implica la recolección de información mediante la observación directa de productos, procesos, sistemas o actividades relacionadas con la tecnología.

Aunque es la práctica más simple en comparación con las técnicas modernas de recopilación de información y que describiremos en este texto, tiene varias bondades y características positivas:

Figura 3.4. Observación de los procesos

1. **Acceso a detalles concretos**

La observación directa permite obtener información de primera mano y en tiempo real. Esto permite captar detalles específicos que podrían pasarse por alto en otras formas de recopilación de información. En el contexto de la vigilancia tecnológica o cualquier otro ámbito, un detalle concreto se refiere a una observación específica y precisa que proporciona información detallada sobre un aspecto particular.

2. **Legitimidad de la información**

La observación directa es auténtica y por lo tanto la información recopilada no está filtrada por interpretaciones o análisis posteriores. Esto puede proporcionar una imagen más precisa y objetiva de lo que se está observando.

3. **Contexto completo**

Al observar una tecnología en acción, se puede comprender su funcionamiento en un contexto completo. Esto ayuda a identificar las interacciones entre diferentes componentes y procesos.

4. **Identificación de problemas y mejoras**

La observación directa puede revelar problemas, ineficiencias o áreas de mejora en un proceso o tecnología. Esta información es valiosa para realizar ajustes y optimizaciones.

5. **Identificación de tendencias emergentes**

Cuando se observan una serie de eventos o situaciones, es posible identificar patrones y tendencias emergentes en el uso de la tecnología.

6. **Validación de información**

La observación directa puede usarse para validar o contrastar información obtenida de otras fuentes, como documentos escritos o informes.

En el contexto de la vigilancia tecnológica se refiere al proceso de verificar la exactitud, autenticidad y confiabilidad de la información recopilada antes de utilizarla en la toma de decisiones o en el análisis.

Es fundamental para asegurarse de que los datos obtenidos sean precisos y reflejen la realidad de manera adecuada.

La validación de la información implica varios pasos y consideraciones:

- Verificación de la fuente

Es importante asegurarse de que la fuente de la información sea confiable y legítima. Esto puede involucrar la evaluación de la reputación de la fuente y su experiencia en el campo.

- Cruce de información

Comparar la información recopilada con otras fuentes independientes puede ayudar a confirmar su precisión y reducir el riesgo de datos incorrectos o sesgados.

- Consistencia interna

Verificar que la información no contradiga otras partes de la misma fuente o documento.

- Comparación con fuentes confiables

Comparar la información con fuentes ampliamente aceptadas y confiables en el campo puede proporcionar un punto de referencia para evaluar su veracidad.

- Validaciones cruzadas

Si es posible, confirmar la información con personas que tengan experiencia en el área o con conocimientos específicos sobre el tema.

- Contexto y lógica

Evaluar si la información tiene sentido en el contexto más amplio y si es coherente con otros conocimientos existentes.

- Fecha y actualización

Asegurarse de que la información sea actualizada y relevante para la fecha en la que se está realizando la validación.

- Supervisión continua

La validación de la información no es un proceso único; es importante continuar supervisando y actualizando la información a medida que evoluciona el panorama tecnológico.

En la vigilancia tecnológica, donde la precisión y la relevancia son clave, la validación cuidadosa de la información garantiza que los avances tecnológicos sean comprendidos y utilizados de manera precisa y efectiva.

La validación de la información es esencial para tomar decisiones informadas y para evitar basar acciones en datos erróneos o desactualizados.

7. **Flexibilidad**

La observación directa puede adaptarse a diferentes contextos y escenarios, lo que permite ajustar la estrategia a las necesidades y objetivos específicos.

En el contexto de la observación directa como estrategia de vigilancia tecnológica se refiere a la capacidad de adaptarse y ajustarse a diferentes situaciones, contextos y necesidades.

En otras palabras, la flexibilidad implica la habilidad de aplicar la observación directa de manera versátil y adecuada a diversas circunstancias.

Esta flexibilidad se caracteriza por:

- Permite aplicar la observación directa en una variedad de entornos, desde laboratorios de investigación hasta lugares de producción o instalaciones de prueba.
- Puede realizarse a diferentes niveles de detalle, desde un enfoque general hasta la observación detallada de componentes específicos.
- Implica observar una amplia gama de tecnologías y procesos, sin importar la industria o el campo.
- Trae consigo que el ejecutor debe estar preparado para adaptarse a situaciones cambiantes y ajustar el enfoque de observación según sea necesario.

- Interactuar con expertos y usuarios para obtener información adicional y comprender mejor la tecnología en uso.

- Presenta la opción de elegir el método de observación más adecuado para la situación, ya sea observación participante, no participante, estructurada o no estructurada.

- Contiene datos recolectados a lo largo del tiempo que se utilizan para identificar tendencias y cambios en la tecnología o el proceso observado.

8. **Aprender de expertos**

Al observar tecnologías en uso, se puede interactuar con expertos y profesionales en el campo, lo que puede proporcionar información adicional y perspectivas valiosas.

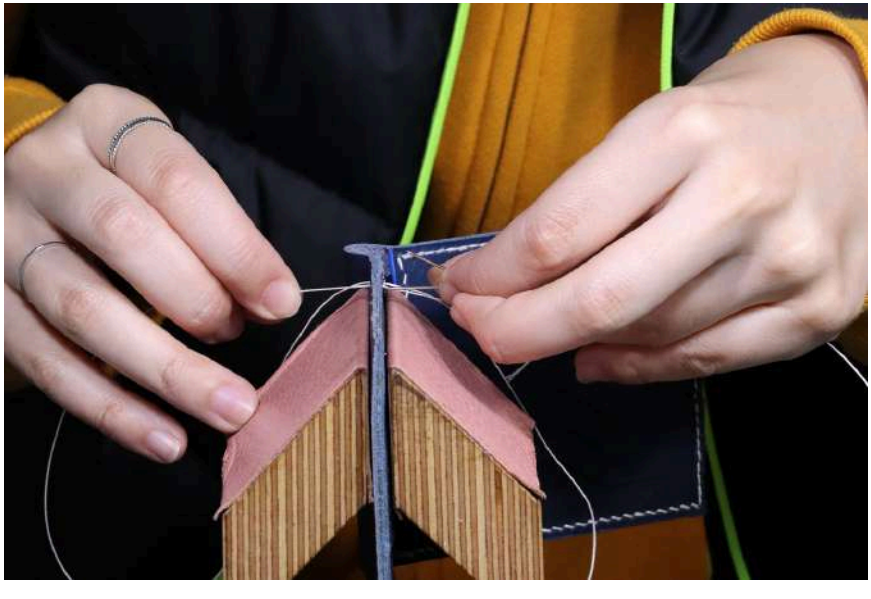


Figura 3.5. Aprender de expertos

En el contexto de la vigilancia tecnológica se refiere a obtener conocimientos, información y perspectivas de individuos con experiencia y conocimientos profundos en un campo tecnológico específico. Normalmente estos expertos suelen ser profesionales, investigadores, académicos u otros profesionales altamente calificados que tienen una comprensión profunda de las tendencias, los avances y los desarrollos en su área de especialización.

Aprender de expertos cuando se realiza la vigilancia tecnológica lnvolucra varios aspectos:

- Acceso a información actualizada

Los expertos suelen estar al tanto de los desarrollos más recientes en su campo, lo que permite a los investigadores de vigilancia tecnológica obtener información actualizada y relevante.

- Perspectivas en profundidad

Los expertos pueden proporcionar una comprensión más profunda y contextualizada de los avances tecnológicos, incluyendo su impacto potencial y sus implicaciones.

- Interacción personal

La comunicación directa con expertos permite realizar preguntas específicas y obtener respuestas detalladas sobre aspectos tecnológicos complejos.

- Identificación de tendencias emergentes

Los expertos a menudo pueden anticipar tendencias y cambios tecnológicos antes de que se vuelvan ampliamente reconocidos.

- Evaluación de viabilidad

Los expertos pueden ayudar a evaluar la viabilidad y la aplicabilidad de nuevas tecnologías en diferentes contextos.

- Análisis crítico

Los expertos pueden proporcionar análisis críticos de los beneficios y desafíos asociados con tecnologías específicas.

- Retroalimentación y consejos

Los expertos pueden ofrecer retroalimentación valiosa sobre estrategias de vigilancia tecnológica, enfoques de investigación y fuentes de información.

- Colaboración potencial

Aprender de expertos puede abrir oportunidades de colaboración en proyectos de investigación o iniciativas tecnológicas.

Es importante establecer una relación de confianza con los expertos y respetar su conocimiento y experiencia. La colaboración con expertos puede enriquecer significativamente la vigilancia tecnológica al proporcionar información valiosa que complementa las fuentes tradicionales y las estrategias de recopilación de datos.

9. **Investigación en tiempo real**

La observación directa permite captar eventos y desarrollos en tiempo real, lo que es especialmente útil para tecnologías en constante evolución.

En el contexto de la vigilancia tecnológica, la investigación en tiempo real implica monitorear y captar los avances, cambios y desarrollos tecnológicos a medida que ocurren.

La investigación en tiempo real al realizar una vigilancia tecnológica tiene las siguientes ventajas:

- Permite captar novedades y cambios tecnológicos casi inmediatamente después de que ocurran.
- Proporciona la capacidad de responder rápidamente a los cambios en el mercado o en la tecnología.
- Facilita el detectar tendencias emergentes antes de que se vuelvan ampliamente conocidas.
- Garantiza que la información recopilada sea la más actualizada y precisa posible.
- Facilita la toma de decisiones basada en datos y en el contexto actual.
- Ayuda a mantenerse al tanto de las actividades y avances de competidores y actores clave en el sector.
- Permite identificar oportunidades para innovar o expandirse, así como posibles riesgos y amenazas.

Este tipo de investigación puede presentar algunos desafíos, como la necesidad de recursos para monitorear y analizar constantemente la información y la posibilidad de obtener datos incompletos o sesgados debido a la inmediatez. Por lo tanto, es importante combinar la investigación en tiempo real con otras estrategias de vigilancia tecnológica para obtener una comprensión más completa y objetiva de los desarrollos tecnológicos.

10. **Aplicación en diversas industrias**

La observación directa es aplicable en una amplia gama de industrias y campos, desde la manufactura hasta la atención médica, pasando por la investigación científica y la ingeniería.

3.4 Vigilancia tecnológica de las sociedades científicas

En la actualidad existen infinidad de sociedades científicas que juegan un papel fundamental en el fomento de la investigación científica, el intercambio de conocimientos y la promoción de la metodología científica.

La historia nos cuenta que las primeras sociedades científicas surgieron durante los siglos XVII y XVIII en Europa y otras partes del mundo occidental:

1. **Royal Society of London for Improving Natural Knowledge (Sociedad Real de Londres para el Avance del Conocimiento Natural)**

Fundada en 1660 en Londres, esta es una de las sociedades científicas más antiguas del mundo. Fue establecida con el objetivo de promover la investigación científica y el intercambio de ideas. La Royal Society ha desempeñado un papel fundamental en el desarrollo de la ciencia moderna y en la publicación de resultados de investigación.

2. **Académie des Sciences (Academia de Ciencias)**

Fundada en 1666 en París, Francia, por el rey Luis XIV, la Académie des Sciences se convirtió en un importante centro de investigación científica.

La Académie des Sciences fue uno de los primeros organismos que estableció normas para la publicación y revisión de trabajos científicos.

3. **Accademia dei Lincei (Academia de los Linces)**

Fundada en 1603 en Roma, Italia, esta academia fue una de las primeras sociedades científicas en Europa. Estaba formada por científicos y eruditos que se centraban en el estudio de la naturaleza y la investigación científica.

4. **American Philosophical Society (Sociedad Filosófica Americana)**

Fundada en 1743 en Filadelfia, Estados Unidos, por Benjamín Franklin y otros científicos, la American Philosophical Society se dedicó a la promoción de la investigación científica y la difusión del conocimiento.

5. **Königliche Gesellschaft der Wissenschaften (Real Sociedad de Ciencias)**

Fundada en 1700 en Gotinga, Alemania, fue una de las primeras sociedades científicas en el mundo germanoparlante. Jugó un papel importante en el desarrollo de la investigación científica en Alemania.

Estas primeras sociedades científicas proporcionaron un espacio para los científicos y eruditos de la época para compartir sus descubrimientos, presentar investigaciones y colaborar en proyectos científicos, fueron precursoras de las actuales organizaciones científicas y académicas que desempeñan un papel fundamental en la promoción y difusión de la investigación científica en todo el mundo.

Las sociedades científicas no suelen centrarse en la vigilancia tecnológica como una función principal, y sus enfoques pueden variar según su alcance y objetivos, sin embargo, facilitan determinadas estrategias informales pueden ayudar a sus miembros a mantenerse al tanto de los avances tecnológicos relevantes en sus campos.

Las estrategias más comunes para la divulgación de los avances científicos:

1. **Publicaciones científicas**

Las sociedades científicas publican revistas científicas, en ellas se presentan los últimos avances en investigación y tecnología en sus campos. A través de la revisión de artículos y estudios publicados en estas revistas, los miembros de la sociedad pueden obtener información sobre los desarrollos tecnológicos que sus miembros o personas relevantes de otras sociedades ejecutan.

La **Royal Society of London for Improving Natural Knowledge** por ejemplo publica los hallazgos en revistas de alto impacto, las más relevantes:

- Philosophical Transactions A: Publica artículos temáticos influyentes en ciencias físicas, matemáticas e ingeniería.
- Proceedings A: Publica artículos de investigación y revisiones en ciencias físicas.
- Interface: Publica artículos de investigación y revisiones en ciencias interdisciplinarias entre las ciencias físicas y las ciencias biológicas.
- Philosophical Transactions B: Publica artículos temáticos influyentes en ciencias biológicas.

- Proceedings B: Publica artículos de investigación y revisiones en ciencias biológicas.
- Biology Letters: Publica artículos cortos de investigación, revisiones y opiniones en ciencias biológicas.

2. **Conferencias y eventos científicos**

Las sociedades científicas organizan conferencias, congresos y eventos donde los investigadores y expertos presentan sus investigaciones y avances tecnológicos, sesiones y resultados que son publicados en sus páginas Web.

3. **Grupos de trabajo y comités técnicos**

La **Académie des Sciences** por ejemplo dispone de comités de expertos para los siguientes aspectos de la ciencia: Enviromental Sciences, Space Research, Energy Prospects, Science and Metrology, Science and Biosafety, Science, ethis and Society, Defending the men of the Science, Teaching Sciences, History of Science and epistemology e Internationales relations.

4. **Colaboraciones e intercambio de información**

Las sociedades científicas suelen fomentar la colaboración y el intercambio de información entre sus miembros. A través de discusiones y redes de contacto, los miembros pueden compartir información sobre tecnologías emergentes y novedades en sus campos.

5. **Colaboración con la industria**

Estas colaboraciones pueden proporcionar información sobre las últimas tecnologías y tendencias adoptadas por las empresas.

6. **Recopilación de datos y tendencias**

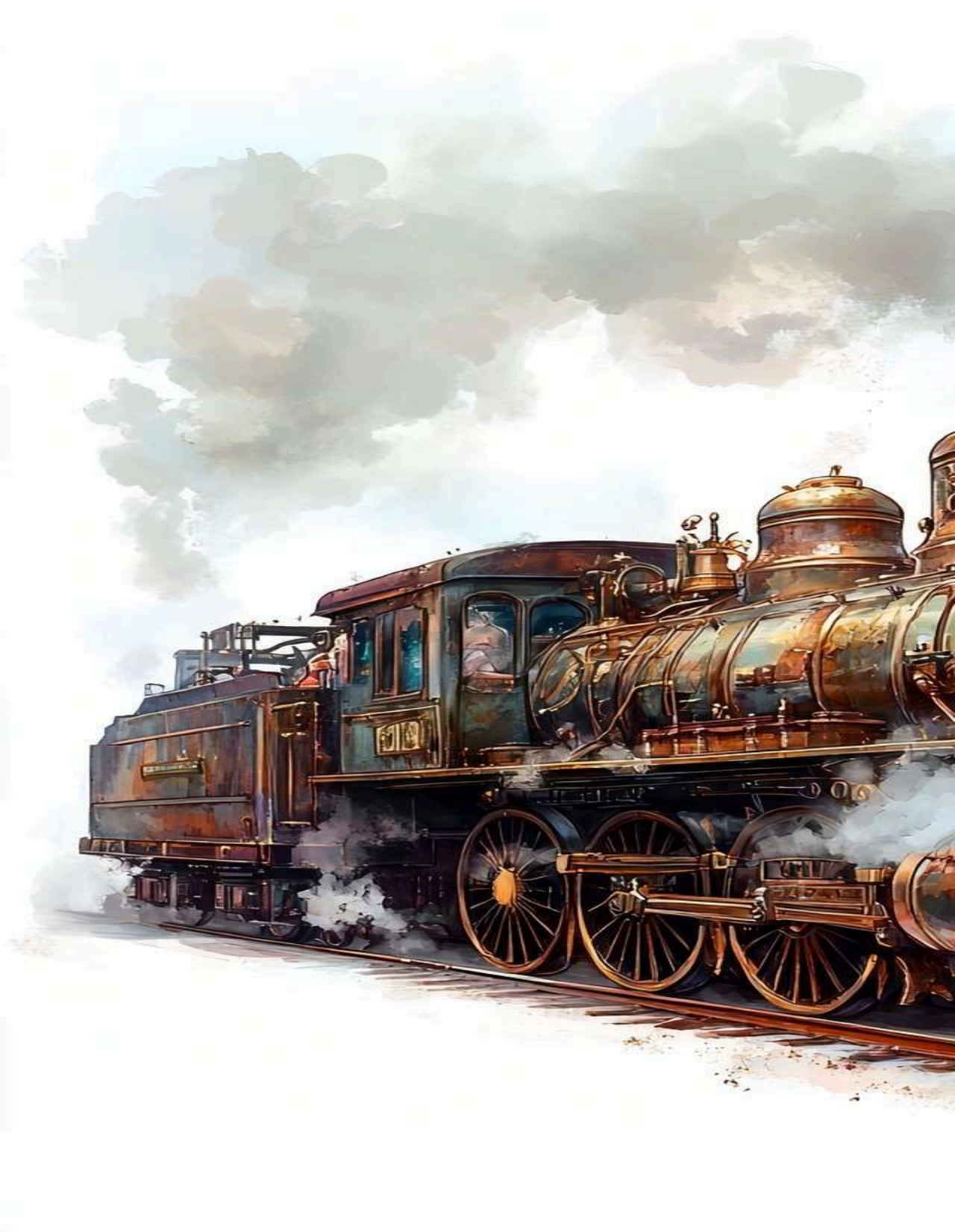
A través de encuestas, cuestionarios o análisis de datos existentes en su área de enfoque las sociedades científicas recopilan datos sobre tendencias tecnológicas.

7. **Monitoreo de literatura científica**

Mediante la revisión periódica de la literatura científica y técnica, las sociedades científicas pueden identificar menciones de nuevas tecnologías, enfoques y desarrollos.

8. **Seguimiento de organismos reguladores**

Las sociedades científicas pueden seguir de cerca las pautas y regulaciones emitidas por organismos gubernamentales o internacionales por los cuales sus objetos de conocimiento se encuentran regulados.



CAPÍTULO IV

Las patentes como herramienta de vigilancia tecnológica

Las patentes

Las patentes son documentos legales que protegen las invenciones y proporcionan detalles técnicos específicos sobre cómo funcionan nuevos productos, procesos o tecnologías. Al analizar patentes, se pueden obtener beneficios significativos para la vigilancia tecnológica.

4.1 Análisis de patentes como estrategia de vigilancia tecnológica

Para realizar un análisis de patentes efectivo, es importante tener acceso a bases de datos de patentes y utilizar herramientas de búsqueda y análisis específicas. La interpretación de las patentes requiere comprender la terminología técnica y legal utilizada en estos documentos [10].

Figura 4.1. Solicitud de patente de motocicleta Harley

El seguimiento del análisis de una patente a lo largo del tiempo puede revelar patrones y tendencias en el desarrollo tecnológico, dicho de otra forma, proporciona una visión más amplia de las direcciones en las que se está avanzando en un campo específico.

En la vigilancia tecnológica moderna, el análisis de patentes es una herramienta poderosa para mantenerse al tanto de los avances tecnológicos y las tendencias en una variedad de campos que permiten:

1. **Identificación de nuevas tecnologías**

Un patente puede revelar nuevas tecnologías y enfoques que están siendo desarrollados, su analísis puede ayudar a identificar tecnologías emergentes antes de que se vuelvan ampliamente conocidas en la literatura científica o en la industria.

2. **Seguimiento de tendencias**

Seguir las tendencias significa monitorear de cerca las solicitudes y concesiones de patentes en un campo específico de la tecnología o industria para identificar patrones, innovaciones emergentes y áreas de enfoque de las empresas y organizaciones, ese seguimiento puede incluir:

- En una patente se reflejan todas las nuevas y valiosas innovaciones tecnológicas de cualquier producto.
- Permite conocer las estrategias de propiedad intelectual de tus competidores
- El descubrir oportunidades de mercado emergentes al identificar tecnologías inconclusas o susceptibles de mejoramiento.

3. **Evaluación de la competencia**

Las patentes propias de una empresa y las patentes de sus competidores pueden proporcionar información sobre sus áreas de enfoque y actividades de investigación, permite construir la matriz DOFA ayude a identificar fortalezas, debilidades y áreas de oportunidad.

4. **Identificación de colaboradores potenciales**

El análisis de patentes puede conducir a oportunidades de colaboración y asociación puesto que un análisis puede revelar posibilidades de colaboración entre diferentes actores en el campo.

5. **Evaluación de la viabilidad técnica**

Las patentes proporcionan detalles técnicos sobre cómo funcionan las invenciones, esto puede ayudar a evaluar la viabilidad técnica y la aplicabilidad de una tecnología en diferentes contextos.

6. **Evaluación del estado de la técnica**

El análisis de patentes puede ayudar a determinar el estado actual de la técnica en un campo. Esto puede ser útil para identificar áreas no exploradas y quizá lo más importante: evitar la duplicación de esfuerzos.

Aquí es importante detectar el por qué se duplican los esfuerzos:

- Dos o más equipos de investigación en la misma organización trabajan en proyectos similares sin saber que el otro está abordando la misma cuestión, es decir no existe diferencia alguna en la innovación proyectada.

- Diferentes departamentos recopilan la misma información de diferentes fuentes o lo que es peor: de las mismas fuentes, lo que lleva a una duplicación de esfuerzos y recursos.
- La creación de soluciones similares para un mismo producto a partir de visiones diferentes sin compartir información sobre sus respectivos proyectos.
- El proceso interno ejecutado por los empleados contiene tareas manuales que podrían automatizarse debido a la falta de comunicación sobre las soluciones ya existentes.
- La confusión generada por el contacto con un mismo cliente por diferentes equipos de la empresa sin comunicación entre ellos para comunicarse las interacciones anteriores.
- No se programa la coordinación de esfuerzos, lo que resulta en solapamientos y pérdida de recursos.

7. **Detección de oportunidades de inversión**

El análisis de patentes puede ayudar a identificar áreas tecnológicas prometedoras que podrían ser de interés para la inversión o el desarrollo empresarial.

8. **Monitorear la competencia**

Analizar las patentes de los competidores clave puede proporcionar información sobre su estrategia tecnológica y su enfoque de innovación. Es el enfoque estratégico o la perspectiva desde la cual se aborda el proceso de desarrollo y aplicación de una nueva idea, producto, servicio o tecnología.

El enfoque de una innovación hace referencia a la dirección, al enfoque estratégico o a la perspectiva desde la cual se aborda el proceso de desarrollo y aplicación de la nueva idea, producto, servicio o tecnología [11] . Es decir, se trata de cómo se planifica, dirige y orienta el proceso de innovación para lograr los objetivos deseados.

En ese enfoque es importante tomar decisiones sobre aspectos clave en el desarrollo de la innovación:

1. **Planeación del o de los objetivos a lograr**

¿Cuáles son los objetivos específicos que se pretenden lograr con la innovación? Esto podría incluir mejorar la eficiencia, aumentar la calidad, entrar en nuevos mercados y resolver problemas específicos entre otros aspectos clave.

2. **¿A quiénes se dirige la innovación?**

¿Qué segmentos de mercado se pretende alcanzar? Comprender las necesidades y deseos del público objetivo es fundamental para orientar la innovación de manera efectiva.

3. **Recursos existentes y recursos no existentes**

Un inventario de ambos tipos de recurso podría implicar la investigación y desarrollo de nuevas tecnologías, la adaptación de tecnologías existentes, o la colaboración con socios tecnológicos, deben surgir del cuestionamiento: ¿qué tecnologías y recursos se utilizarán para llevar a cabo la innovación?

4. **Estrategia competitiva**

Definir una estrategia competitiva sólida puede ayudar a posicionarse de manera efectiva en el mercado.

Para que dicha estrategia sea sólida se debe tomar como puntos de partida la diferenciación positiva de la innovación que surge de la vigilancia tecnológica con respecto al producto de la competencia, y por otro lado ¿Cuál es la propuesta única de valor que ofrece?

5. **Escalabilidad y crecimiento**

Es importante determinar cómo se gestionará la producción, distribución y demanda a medida que la innovación gane tracción si se pretende que la innovación crezca y se expanda a gran escala.

Si la intención es que esta innovación crezca y se convierta en algo ampliamente utilizado o reconocido, es esencial pensar en cómo manejar todos los aspectos prácticos relacionados con su desarrollo y distribución en una escala más grande.

Para esa aceptación de la innovación en el mercado hay que considerar aspectos como:


Cuando la innovación se vuelve más popular, es necesario lograr una producción eficiente y por lo tanto es necesario asegurar de que se pueda producir en cantidades suficientes para satisfacer la demanda sin afectar la calidad ni elevar excesivamente los costos de producción.


Planificar adecuadamente las cadenas de suministro de tal manera que sean eficientes y con métodos de distribución efectivos.


Asegurar la existencia de suficientes unidades de tal manera que los clientes puedan obtener el producto sin problemas.


Diseñar el ajuste de las estrategias de marketing para llegar a un público más amplio y diverso.

- El aumento de la demanda de la innovación puede aumentar la necesidad de brindar un buen servicio al cliente para resolver problemas y responder a preguntas.

- Si la competencia se incrementa se debe considerar la manera de diferenciarse y mantener una ventaja competitiva.

- La infraestructura y los recursos deben ser escalables para manejar un mayor volumen de producción y demanda, esto se denomina escalabilidad.

6. **Ciclo de vida llamativo**

Video

Video 4.1. Ciclo de vida de un producto o innovación

El ciclo de vida de un producto se refiere a las etapas que atraviesa un producto desde su concepción y desarrollo inicial hasta su retiro del mercado y eventual desaparición.

Estas etapas representan la evolución y el cambio en las ventas, la rentabilidad y la relevancia del producto a lo largo del tiempo.

Debe determinarse si la solución planteada es la innovación es la respuesta a una solución temporal, si es a mediano o largo plazo. El ciclo de vida del producto es un concepto importante en marketing y gestión de productos, ya que ayuda a comprender cómo se desarrolla un producto en el mercado y cómo planificar estrategias adecuadas en cada etapa.

4.2 Datos de un Patentamiento

Cuando se realiza el análisis de patentes como estrategia de vigilancia tecnológica, la identificación de nuevas tecnologías, el seguimiento de tendencias, la evaluación de la competencia, la identificación de colaboradores potenciales, la evaluación de la viabilidad técnica, la evaluación del estado de la técnica, la detección de oportunidades de inversión y el monitoreo la competencia, se logran debido a que una patente debe proporcionar los siguientes datos:

Realización de Análisis de Patentes para Vigilancia Tecnológica, este proceso se ha convertido en una herramienta fundamental para la vigilancia tecnológica, permitiendo a los investigadores, empresas y países comprender el panorama actual de la innovación y tomar decisiones estratégicas.

En la siguiente escena se describen las características de la realización del análisis de patentes para la vigilancia tecnológica:

Estrategia de vigilancia: las patentes existentes

Objeto interactivo 4.1. Proceso de analizar patentes como estrategia de vigilancia

A partir de la presentación podemos resumir que: el análisis de patentes para la vigilancia tecnológica es un proceso sistemático que utiliza la información contenida en los documentos de patentes para identificar tendencias, oportunidades y amenazas en el panorama de la innovación.

Esa información contenida en los documentos que sustentan la patente puede ser utilizada para la toma de decisiones estratégicas en materia de investigación, desarrollo e innovación.

4.3 Espionaje Industrial

El espionaje económico o industrial [12] se da en dos formas principales y su propósito es reunir conocimiento sobre una o más organizaciones.

Puede incluir la adquisición de propiedad intelectual, como información sobre fabricación industrial, ideas, técnicas y procesos, recetas y fórmulas.

Ese espionaje podría incluir el secuestro de información patentada u operativa, como la de conjuntos de datos de clientes, precios, ventas, marketing, investigación y desarrollo, políticas, ofertas potenciales, estrategias de planificación o marketing o las composiciones y ubicaciones cambiantes de la producción.

Puede describir actividades como el robo de secretos comerciales, el soborno , el chantaje y la vigilancia tecnológica. Además de orquestar el espionaje sobre organizaciones comerciales, los gobiernos también pueden ser objetivos, por ejemplo, para determinar los términos de una licitación para un contrato gubernamental.

Las patentes y el espionaje industrial están estrechamente relacionados, aunque de maneras opuestas, veamos la descripción de estos dos conceptos:

Patentes

Una patente representa los derechos de propiedad intelectual que protegen invenciones. Otorgan a su titular el derecho exclusivo de explotar comercialmente una invención durante un período limitado a cambio de revelar públicamente los detalles técnicos de la invención.

Espionaje industrial

Es la práctica ilegal de obtener secretos comerciales o información confidencial de competidores, generalmente para obtener una ventaja competitiva. Algunas características del espionaje industrial:

1. **Obtención de Información Confidencial**

Se centra en información que es crítica para el éxito de una empresa y que no está disponible al público. Esto puede incluir fórmulas químicas, métodos de producción, algoritmos de software o estrategias comerciales.

2. **Métodos Ilícitos y Encubiertos**

A diferencia de la vigilancia tecnológica o la investigación de mercado, el espionaje industrial suele recurrir a métodos ilegales o no éticos, como hackeos, soborno a empleados, infiltración, o acceso no autorizado a documentos o instalaciones.

3. **Objetivo de Ventaja Competitiva**

Quienes cometen espionaje industrial suelen ser competidores que buscan ganar mercado rápidamente copiando productos o métodos innovadores sin necesidad de hacer la inversión en investigación y desarrollo.

La relación entre patentes y espionaje industrial es equivalente a decir: ***Protección vs. Apropiación***. Las patentes protegen contra el espionaje industrial al hacer pública la información de manera legal, mientras que el espionaje busca obtener información de forma ilícita.

Paradójicamente, las patentes pueden incentivar el espionaje industrial. Al revelar parcialmente información valiosa, pueden despertar el interés de competidores en obtener más detalles por medios ilegales, es una práctica que conlleva a:

- Evasión de patentes: Algunas empresas recurren al espionaje para evadir patentes y desarrollar tecnologías similares sin infringir derechos.
- Secretos comerciales: Algunas empresas optan por no patentar ciertas invenciones para mantenerlas como secretos comerciales, lo que puede hacerlas más vulnerables al espionaje.
- Evidencia legal: Las patentes pueden servir como evidencia en casos de espionaje industrial, ayudando a demostrar la propiedad original de una tecnología.
- Competencia global: En el ámbito internacional, las diferencias en las leyes de patentes entre países pueden fomentar prácticas de espionaje industrial.

La motivación para el espionaje industrial es un tema complejo con múltiples facetas. Profundicemos en los principales factores que impulsan esta práctica ilegal:

1. **Ventaja competitiva**

Las empresas buscan obtener información privilegiada para adelantarse a sus competidores. Conocer los planes, tecnologías o estrategias de la competencia puede permitir ajustar las propias estrategias de mercado.

2. **Ahorro de tiempo y recursos**

El espionaje puede ahorrar años de investigación y desarrollo. Permite evitar costosos procesos de prueba y error.

3. **Superación de barreras tecnológicas**

Algunas empresas recurren al espionaje cuando no logran desarrollar ciertas tecnologías por sí mismas. Puede ser una forma de superar la brecha tecnológica con competidores más avanzados.

4. **Presiones económicas**

En mercados altamente competitivos, la presión por mantener o aumentar la cuota de mercado puede llevar a prácticas poco éticas. La necesidad de reducir costos y aumentar beneficios puede motivar estas acciones.

5. **Oportunismo**

La disponibilidad de información valiosa, aunque sea por medios ilícitos, puede ser una tentación difícil de resistir para algunas empresas.

6. **Factores geopolíticos**

Algunos gobiernos pueden fomentar o tolerar el espionaje industrial como parte de estrategias de desarrollo económico nacional.

7. **Curiosidad tecnológica**

El deseo de comprender cómo funciona una tecnología innovadora puede motivar acciones de espionaje, especialmente en sectores de alta tecnología.

8. **Validación de rumores o especulaciones**

El espionaje puede utilizarse para confirmar o desmentir información sobre los avances de los competidores.

9. **Anticipación a cambios en el mercado**

El espionaje puede utilizarse para confirmar o desmentir información sobre los avances de los competidores.

10. **Evasión de costos de licencias**

Algunas empresas pueden optar por el espionaje para evitar pagar costosas licencias por tecnologías patentadas. Destacamos que, aunque estas motivaciones existen, el espionaje industrial es ilegal y puede tener graves consecuencias legales y reputacionales.

4.4 Vigilancia Competitiva

La vigilancia competitiva la podemos considerar como un enfoque especializado dentro de la vigilancia tecnológica, dicho de otra forma, se describe la vigilancia competitiva como un tipo de vigilancia tecnológica que se centra en la información sobre los competidores, tanto actuales como potenciales.

Su objetivo de la vigilancia competitiva es obtener información estratégica sobre las acciones de la competencia, es recopilar información estratégica sobre las actividades de los competidores, lo que permite a la organización anticiparse a sus movimientos y tomar decisiones más informadas para mejorar su posición en el mercado como por ejemplo, sus políticas de inversión o su entrada en nuevas actividades. Existen algunas variantes:

- Vigilancia comercial

Estudia datos sobre clientes y proveedores, como la evolución de las necesidades de los clientes, su solvencia, o los nuevos productos ofrecidos por los proveedores.

- Vigilancia del entorno

Se enfoca en detectar eventos externos que puedan influir en el futuro de la organización, abarcando áreas como la sociología, la política, el medio ambiente y las regulaciones.

4.4.1 Inteligencia Competitiva

La inteligencia competitiva ***(IC)*** es un proceso ético y sistemático [13] que permite a las organizaciones recolectar, analizar, interpretar y diseminar información relevante sobre su entorno de negocios, sus competidores y su propia estructura.

A través de esta recolección de información estratégica, las empresas pueden prever tendencias del mercado, identificar fortalezas y debilidades de la competencia, y adaptar su estrategia para mejorar su posición en la industria.

La ***(IC)*** se integra en la toma de decisiones empresariales al aportar conocimiento clave en el momento oportuno, lo que permite a las organizaciones anticiparse y reaccionar eficazmente a los cambios en su entorno competitivo.

4.4.2 Inteligencia Estratégica

La Inteligencia Estratégica [14] como Herramienta para la Gestión de la Innovación se propone como un sistema holístico que permite a las organizaciones gestionar la innovación de manera efectiva. Esto se logra al:

1. Analizar información del pasado, presente y futuro: Se consideran estudios previos, investigaciones, tendencias, proyectos realizados y en desarrollo para comprender el estado del arte de cada tema particular.
2. Utilizar diversas herramientas: Se emplean la vigilancia tecnológica, la inteligencia competitiva y la prospectiva para recopilar y procesar información de manera integral.
3. Aplicar métodos y recursos tecnológicos: Se utilizan herramientas cienciométricas y tecnológicas para seleccionar, filtrar, procesar, evaluar, almacenar y difundir información, transformándola en conocimiento útil.

De esta manera, la inteligencia estratégica proporciona a las organizaciones información estructurada que les permite tomar decisiones estratégicas informadas brindando beneficios para la Gestión de la Innovación.

4.4.3 Inteligencia Estratégica con apoyo académico

La inteligencia estratégica ayuda a las organizaciones a gestionar la innovación y con el apoyo académico se logra:

Identificar amenazas y oportunidades: Permite identificar tendencias y necesidades tecnológicas del sector, así como oportunidades de mercado y negocios. También alerta sobre cambios importantes en el entorno que pueden impactar los planes y programas de la organización, entre ellos podemos nombrar:

1. **Definir y priorizar proyectos de I+D+i.**

El análisis integral de la información permite identificar proyectos de investigación con potencial para convertirse en innovaciones.

2. **Fomentar la articulación entre diferentes agentes.**

La inteligencia estratégica impulsa la colaboración entre diferentes actores del ecosistema de innovación, incluyendo el sector académico y productivo.

3. **Incrementar la competitividad.**

Al proporcionar información estratégica para la toma de decisiones, la inteligencia estratégica ayuda a las organizaciones a desarrollar ventajas competitivas y a mejorar su desempeño en el mercado.

4. **Incrementar la competitividad.**

Se propone desde la academia un proceso metodológico para la implementación de la inteligencia estratégica, que consta de cuatro pilares fundamentales:

- Diagnóstico actual

Se analizan los activos estratégicos de la organización, incluyendo recursos humanos, físicos, tangibles e intangibles, así como el conocimiento interno. Esto permite identificar las tecnologías y capacidades de innovación de la organización, los factores clave de éxito, las barreras de entrada y las ventajas competitivas actuales.

- Diseño de la estrategia

Se definen los objetivos estratégicos de la organización, teniendo en cuenta su misión, visión y valores, así como un análisis DOFA. Se consideran los planes nacionales de desarrollo y los ejes prioritarios de trabajo de la organización, con el fin de articular la estrategia con el contexto interno y externo.

- Implementación de la estrategia

Se definen, identifican y priorizan proyectos de I+D+i en línea con la estrategia diseñada. Se implementan y comercializan los proyectos de innovación seleccionados.

- Seguimiento y control

Se establecen indicadores de seguimiento, preferiblemente cuantitativos y medibles, para monitorear el progreso del plan estratégico.

Se consideran indicadores financieros, de eficiencia, aprendizaje, conocimiento e innovación.

Esta articulación estructurada de forma sistémica por la academia busca maximizar la efectividad del sistema de inteligencia estratégica, incentivando la gestión de la innovación en la organización.

La inteligencia estratégica se presenta como una herramienta clave para que las organizaciones gestionen la innovación de forma efectiva.

Al proporcionar información estratégica para la toma de decisiones, permite identificar oportunidades, minimizar riesgos y anticiparse a los cambios en un entorno dinámico, el soporte académico permite definir la prospectiva utilizada para identificar tendencias y escenarios futuros.

4.5 Bases de datos de patentes y la Minería de Datos

La minería de datos aplicada a las bases de datos de patentes [15] permite obtener información valiosa que de otra manera podría ser difícil de detectar debido al gran volumen de datos.

Este proceso de análisis facilita el trabajo de los investigadores, abogados de patentes, y profesionales de la industria, ayudándolos a tomar decisiones informadas sobre el desarrollo de nuevos productos, la dirección de la investigación y la protección de la propiedad intelectual.

Definiciones:

1. **Bases de datos de patentes**

Las bases de datos de patentes son repositorios que almacenan información detallada sobre invenciones registradas y protegidas por derechos de patente.

Estas bases contienen documentos de patentes que incluyen descripciones de las invenciones, reivindicaciones (definiciones de lo que se protege legalmente), información sobre los inventores, fechas de solicitud, y datos técnicos relevantes.

Entre las bases de datos de patentes más populares y accesibles están la USPTO (Oficina de Patentes y Marcas de los Estados Unidos), la EPO (Oficina Europea de Patentes), WIPO (Organización Mundial de la Propiedad Intelectual), y Google Patents, entre otras.

2. **Minería de datos**

La minería de datos es el proceso de analizar grandes cantidades de datos para descubrir patrones, relaciones y tendencias significativas. Este análisis se lleva a cabo mediante técnicas de inteligencia artificial, estadística y aprendizaje automático.

En el contexto de las bases de datos de patentes, la minería de datos puede ser especialmente útil para:

- Identificar tendencias tecnológicas: Permite identificar cuáles áreas de investigación están creciendo o qué tipos de tecnologías están emergiendo en el mercado.
- Analizar actividad competitiva: A través de patrones en las solicitudes de patentes, es posible inferir en qué áreas están invirtiendo empresas o sectores específicos.

- Detectar vacíos en la innovación: Mediante el análisis de tendencias y patrones, es posible identificar áreas tecnológicas poco exploradas, ofreciendo oportunidades de innovación.

Complementación de ambos conceptos

La minería de datos aplicada a las bases de datos de patentes permite obtener información valiosa que de otra manera podría ser difícil de detectar debido al gran volumen de datos. Este proceso de análisis facilita el trabajo de los investigadores, abogados de patentes, y profesionales de la industria, ayudándolos a tomar decisiones informadas sobre el desarrollo de nuevos productos, la dirección de la investigación y la protección de la propiedad intelectual.

4.6 Las patentes, Internet y Vigilancia en Línea

Internet y la vigilancia en línea son fundamentales en la práctica de la vigilancia tecnológica, ya que ofrecen acceso rápido y fácil a una enorme cantidad de información actualizada sobre desarrollos científicos, tecnológicos y comerciales en todo el mundo.

Al incorporar el análisis de patentes, Internet y la vigilancia en línea se convierte en un proceso que permite obtener una visión estratégica sobre el avance de tecnologías específicas, la actividad de competidores y las tendencias de innovación.

La Vigilancia en línea y su rol en la vigilancia tecnológica implica la observación y el análisis continuo de la información digital disponible sobre un tema específico. Para ello se utilizan herramientas en línea para monitorear sitios web, redes sociales, foros, bases de datos científicas y, especialmente, bases de datos de patentes.

Esta vigilancia tiene como objetivos:

1. **Identificar tendencias emergentes: Monitorear innovaciones en diferentes sectores permite anticipar tecnologías y avances futuros.**
2. **Seguir a la competencia: Permite conocer los movimientos y estrategias de empresas competidoras mediante la observación de sus solicitudes de patentes y lanzamientos de productos.**
3. **Detectar oportunidades y amenazas: Ayuda a las empresas a identificar áreas tecnológicas en las que invertir, así como posibles riesgos, como saturación de mercado o competencia intensa en una tecnología específica.**

El análisis de patentes es una técnica central en la vigilancia tecnológica ya que los soportes de una patente contienen información detallada sobre los principios técnicos de una invención, los problemas que resuelve, y la estructura técnica de su funcionamiento.

Al analizar las patentes en el contexto de vigilancia tecnológica, se pueden lograr varios objetivos:

- Predecir desarrollos tecnológicos

Dado que las patentes se registran antes de que un producto salga al mercado, su análisis permite anticipar futuros lanzamientos de tecnologías.

- Evaluar el estado de la tecnología

El análisis de patentes revela las áreas de innovación y estancamiento, proporcionando un mapa del avance tecnológico en un campo específico.

- Identificar patrones de inversión

Las solicitudes de patentes pueden indicar en qué tecnologías están invirtiendo tiempo y recursos empresas e instituciones.

Relación entre Internet, vigilancia en línea y análisis de patentes

Internet y la vigilancia en línea son esenciales para acceder y analizar bases de datos de patentes de forma eficiente. Las plataformas en línea, combinadas con herramientas de minería de datos, inteligencia artificial y aprendizaje automático, permiten analizar grandes volúmenes de patentes y extraer patrones de innovación y tendencias de mercado con rapidez.

En el contexto de la vigilancia en línea, el análisis de patentes en un se convierte en una estrategia poderosa dentro de la vigilancia tecnológica, aprovechando la disponibilidad de información digital para generar una ventaja competitiva en el mercado.

4.7 Vigilancia tecnológica en Redes Sociales

En este punto debemos diferenciar las redes sociales de las comunidades sociales.

- Una red social es una estructura social compuesta por nodos, que generalmente son individuos u organizaciones [16]. Estos nodos están conectados por uno o más tipos de interdependencia, como valores, puntos de vista o ideas. Las redes sociales no se centran en un lugar, sino en los individuos que participan en ellas. Se autoorganizan, tienen una dinámica aleatoria y están controladas por el usuario.

- Las comunidades sociales suelen estar impulsadas por un tema u objetivo específico, controladas por guías o moderadores y con una arquitectura organizativa. Pueden estar limitadas a un lugar o ámbito particular.

La IA de NotebooKLM nos ha proporcionado un resumen donde destacamos lo presentado el siguiente video:

Video

Video 4.2. Las redes sociales y las comunidades sociales

Hemos definido hasta el momento que una vigilancia tecnológica implica el monitoreo sistemático de información relevante en áreas de innovación, tecnología y desarrollo, y las redes sociales son una fuente rica y dinámica de información. Esas redes sociales y las comunidades sociales facilitan:

1. **Identificación de tendencias**

Las redes sociales son ideales para captar tendencias emergentes en tecnología y mercados. Plataformas como Twitter, LinkedIn, y Reddit permiten rastrear:

- Etiquetas populares (#AI, #IoT, ...)
- Publicaciones de expertos e innovadores
- Debates en comunidades especializadas

2. **Seguimiento de expertos y empresas**

Al seguir a líderes de opinión, startups, e instituciones en plataformas como LinkedIn y Twitter, puedes mantenerte actualizado sobre:

- Nuevas tecnologías
- Publicaciones de investigaciones
- Anuncios de patentes o productos

3. **Monitorización en tiempo real**

Las redes sociales permiten acceder a información en tiempo real, ideal para estar al día con:

- Noticias tecnológicas relevantes
- Avances de la competencia
- Conferencias o lanzamientos globales (ej.: CES, WWDC)

4. **Escucha social**

Herramientas de social listening como Hootsuite o Brandwatch analizan publicaciones y conversaciones en redes sociales para:

- Detectar necesidades del mercado
- Evaluar percepciones sobre una tecnología
- Identificar posibles nichos de innovación

5. **Uso de grupos y foros**

Los grupos y los foros concentran la información sobre conceptos específicos:

- Reddit tiene subreddits tecnológicos como r/technology, r/Futurology
- Grupos de LinkedIn sobre tecnología ofrecen información y networking
- Facebook o X (Twitter) pueden contener grupos o listas de temas especializados

6. **Limitaciones y desafíos**

Interactuar con las redes sociales y las comunidades sociales implica vencer las siguientes limitaciones y desafíos:

- Ruido informativo: Filtrar información relevante es complejo

- Sesgos y desinformación: Hay contenido poco confiable o influido por intereses comerciales
- Acceso limitado: Algunas discusiones avanzadas pueden no estar abiertas o ser superficiales

Estrategias para optimizar el uso de redes sociales en vigilancia tecnológica sabiendo que son un complemento poderoso para la vigilancia tecnológica, siempre que se usen con herramientas adecuadas y un enfoque crítico:

- Define objetivos claros como detectar nuevas patentes en IA
- Utiliza herramientas como Google Alerts, Feedly, o Social Mention para automatizar búsquedas
- Integra la información con otros métodos de vigilancia (bases de datos científicas, reportes de mercado)

Finalizamos afirmando que las redes sociales son una fuente rica y dinámica de información.

4.8 Analítica Avanzada y Aprendizaje Automático

La analítica avanzada y el aprendizaje automático son herramientas poderosas que, combinadas, ofrecen un enorme potencial para mejorar la eficiencia, la precisión y la toma de decisiones en diversos campos

La vigilancia tecnológica (VT) se centra en identificar, recopilar, analizar y difundir información estratégica sobre tecnologías emergentes, tendencias del mercado y actividades de investigación.

Cuando se combina con la Analítica Avanzada y el Aprendizaje Automático (AA), se crea una poderosa sinergia que amplifica las capacidades de predicción, detección y toma de decisiones estratégicas [17].

Relación de las disciplinas Analítica Avanzada y Aprendizaje Automático

La combinación de vigilancia tecnológica, analítica avanzada y aprendizaje automático permite pasar de un enfoque reactivo a uno proactivo, donde las organizaciones pueden no solo seguir el ritmo del cambio tecnológico, sino también adelantarse a él.

1. **Analítica Avanzada en la Vigilancia Tecnológica**

Manejo de grandes volúmenes de datos: La VT requiere procesar información proveniente de múltiples fuentes (publicaciones científicas, patentes y redes sociales entre otras.). La analítica avanzada permite extraer patrones relevantes y estructurar datos no procesados.

- Identificación de tendencias: Utiliza modelos predictivos para anticipar desarrollos tecnológicos basados en el análisis de publicaciones históricas, inversiones en I+D, y adopción en el mercado.
- Segmentación y priorización: Clasifica tecnologías o áreas de interés según su impacto potencial, etapa de desarrollo o relevancia para una organización.

2. **Aprendizaje Automático en la Vigilancia Tecnológica**

   El aprendizaje automático potencia la vigilancia tecnológica mediante la automatización y el aprendizaje continuo. Algunos de ellos:

   - Procesamiento del Lenguaje Natural (PLN)
     - Extrae información de documentos científicos, artículos y bases de datos.
     - Realiza análisis semántico para identificar relaciones entre conceptos tecnológicos.
   - Sistemas de recomendación
     - Sugiere tecnologías o desarrollos relevantes basados en datos previos.
     - Facilita la personalización de resultados para usuarios o sectores específicos.
   - Modelos de predicción
     - Prevé la evolución de una tecnología basándose en datos históricos.
     - Detecta posibles disrupciones tecnológicas o mercados emergentes.

- Detección de señales débiles
    - Identifica patrones que podrían pasar desapercibidos, como menciones marginales de una tecnología que podría convertirse en disruptiva.

Beneficios de la Integración

1. **Automatización**: Reduce el tiempo necesario para realizar análisis complejos
2. **Precisión**: Mejora la detección de tendencias y oportunidades relevantes
3. **Escalabilidad**: Permite analizar un volumen masivo de información en tiempo real
4. **Adaptabilidad**: Los modelos pueden ajustarse continuamente con nuevos datos

La combinación de vigilancia tecnológica, analítica avanzada y aprendizaje automático permite pasar de un enfoque reactivo a uno proactivo, donde las organizaciones pueden no solo seguir el ritmo del cambio tecnológico, sino también adelantarse a él.

4.9 Las patentes, la Inteligencia Artificial y la Automatización

Con lo presentado hasta el momento hemos definido que la vigilancia tecnológica es un proceso estratégico que busca identificar, analizar y utilizar información relevante sobre tecnología, competidores y tendencias del mercado para tomar decisiones informadas. En este contexto, la relación entre patentes, inteligencia artificial (IA) y automatización juega un papel fundamental [18].

Video

Video 4.3. Las patentes, la Inteligencia Artificial y la Automatización

1. Patentes y Vigilancia Tecnológica

En la era de la IA, las bases de datos de patentes han crecido exponencialmente, lo que hace necesaria la automatización en el análisis ya que son una fuente clave de información en vigilancia tecnológica, reflejan innovaciones técnicas protegidas legalmente. Su análisis permite:

- Detectar tendencias tecnológicas: Identificar áreas emergentes de desarrollo y nichos de innovación
- Mapear la competencia: Conocer qué están desarrollando otras empresas o investigadores
- Prevenir infracciones: Evitar conflictos legales por violaciones a derechos de propiedad intelectual

2. **Inteligencia Artificial aplicada a la Vigilancia Tecnológica**

A pesar de los debates controversiales que genera la IA consideramos que ella facilita y amplifica el alcance de la vigilancia tecnológica en varios aspectos:

- Extracción y análisis de datos masivos

La IA puede procesar grandes volúmenes de información de bases de datos de patentes y artículos científicos, identificando patrones y correlaciones.

- Procesamiento de lenguaje natural (NLP)

Herramientas basadas en IA pueden interpretar y clasificar textos técnicos complejos en distintos idiomas, agilizando la revisión de patentes.

- Predicción de tendencias

Algoritmos de machine learning analizan datos históricos para prever futuros desarrollos tecnológicos y un ejemplo de ello son las plataformas como PatentSight y Derwent Innovation usan IA para analizar la calidad e impacto de patentes, facilitando decisiones estratégicas.

3. **Automatización en Vigilancia Tecnológica**

La automatización complementa la IA, permitiendo:

- Monitoreo continuo

Sistemas automatizados revisan regularmente bases de datos, reportando nuevas publicaciones de interés.

- Alertas personalizadas

Configurar filtros para recibir notificaciones cuando surgen patentes en áreas específicas.

- Gestión eficiente

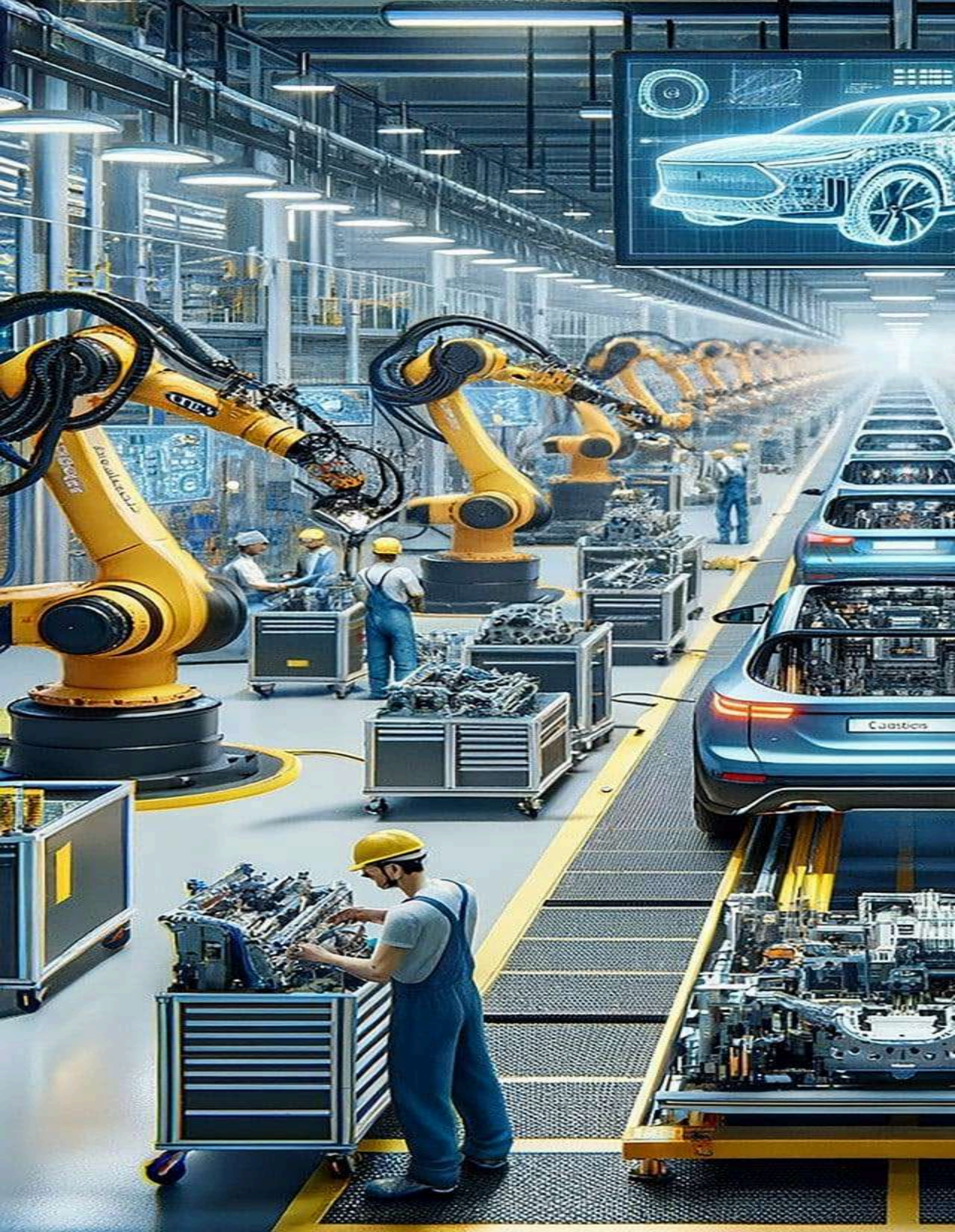
Integrar datos de diferentes fuentes en una única plataforma, reduciendo el esfuerzo manual.

Interacciones clave de las patentes, la Inteligencia Artificial y la Automatización

Surge el cuestionamiento: ¿Debe una invención generada por IA ser patentable? Este debate impacta la protección de innovaciones automatizadas.

La IA para combatir plagio o infracciones: Algoritmos comparan diseños o códigos para identificar similitudes que puedan violar patentes existentes.

Impacto de las patentes en la IA: El uso de IA está condicionado por patentes previas, lo que puede influir en el acceso a herramientas y algoritmos clave para una vigilancia tecnológica.




CAPÍTULO V
Vigilancia e inteligencia competitiva en el ámbito empresarial

Introducción

Este capítulo explorará cómo la vigilancia, cuando se aplica de manera ética y legal en el ámbito empresarial, puede transformarse en inteligencia competitiva. Se discutirán temas como el monitoreo de competidores, el análisis del mercado y las tendencias de la industria, la vigilancia tecnológica, la identificación de riesgos y oportunidades legales y regulatorias, y la evaluación de la cadena de suministro y socios comerciales. Además, se abordarán las consideraciones éticas y legales al realizar la vigilancia en el ámbito empresarial.

5.1 Vigilancia Tecnológica e Inteligencia Competitiva en el Ámbito Empresarial

En un entorno empresarial cada vez más dinámico y globalizado, la capacidad de adaptarse y anticiparse a los cambios es esencial para el éxito organizacional. La Vigilancia Tecnológica (VT) y la Inteligencia Competitiva (IC) han emergido como disciplinas clave para permitir a las empresas no solo sobrevivir, sino prosperar en este contexto.

Estas herramientas estratégicas permiten a las organizaciones monitorear su entorno, anticipar movimientos de competidores, identificar oportunidades tecnológicas y minimizar riesgos, todo ello fundamentado en la recopilación y análisis sistemático de información relevante.

Vigilancia Tecnológica: Un Pilar de Innovación

La Vigilancia Tecnológica (VT) es un proceso sistemático de observación y análisis del entorno tecnológico. Su objetivo es identificar desarrollos y tendencias emergentes que puedan afectar la competitividad de una empresa.

Según Zaintek [19], la VT no solo se enfoca en la tecnología per se, sino también en cómo estas tecnologías pueden ser adoptadas e implementadas para crear ventajas competitivas.

Video

Video 5.1. La VT: un pilar de innovación empresarial

Un sistema de VT eficaz no solo monitorea avances tecnológicos, sino que también examina cómo estos avances están siendo utilizados por competidores y otros actores clave en la industria.

Esto permite a las empresas anticipar la dirección del mercado y ajustar sus estrategias en consecuencia. Por ejemplo, el monitoreo de patentes y publicaciones científicas puede revelar innovaciones emergentes que aún no han sido ampliamente adoptadas, proporcionando a la empresa una oportunidad de ser pionera en su implementación.

5.2 Inteligencia Competitiva: Comprendiendo el Entorno de Negocios

La Inteligencia Competitiva (IC) se centra en la recopilación y análisis de información sobre los competidores y el entorno de mercado. Como lo señala INTEC (2009), la IC permite a las empresas anticiparse a los movimientos de sus competidores, identificar cambios en las preferencias de los consumidores y adaptarse a las nuevas regulaciones que puedan afectar su industria.

La IC incluye la observación de los competidores, pero va más allá al analizar también otros factores del entorno, como cambios políticos, sociales y económicos que puedan influir en el mercado. Este análisis integral permite a las empresas desarrollar estrategias que no solo respondan a la competencia actual, sino que también se anticipen a cambios futuros en el entorno empresarial.

5.3 Proceso de Implementación de la VT e IC

Implementar un sistema de VT e IC requiere seguir un proceso estructurado que asegure la eficacia y relevancia de la información recopilada. [20] [21]

El proceso generalmente sigue las siguientes fases, lo podemos seguir en la siguiente presentación:


PROCESO DE IMPLEMENTACIÓN
Implementar un sistema de VT e IC requiere seguir un proceso estructurado que asegure la eficacia y relevancia de la información recopilada.
ANTERIOR
SIGUIENTE

5.4 Impacto en la Competitividad Empresarial

El impacto de la VT e IC en la competitividad empresarial es significativo. Estas herramientas permiten a las empresas no solo anticiparse a los cambios y minimizar riesgos, sino también fomentar la innovación al identificar nuevas oportunidades de negocio.

Un sistema bien implementado de VT e IC puede mejorar la capacidad de la empresa para tomar decisiones estratégicas informadas, lo que a su vez fortalece su posición competitiva en el mercado.

Además, la VT e IC facilitan la colaboración interna y externa, promoviendo una cultura de innovación y adaptabilidad dentro de la organización. La capacidad de integrar la información obtenida a través de estos procesos en la toma de decisiones es clave para asegurar la competitividad y el éxito a largo plazo de la organización.

Para concluir [22] [23] [24], podemos expresar que La Vigilancia Tecnológica y la Inteligencia Competitiva son componentes esenciales para la estrategia empresarial en el entorno globalizado actual. Al implementar un sistema robusto de VT e IC, las empresas pueden anticiparse a los cambios, minimizar riesgos, aprovechar nuevas oportunidades y tomar decisiones estratégicas informadas. Estas disciplinas no solo fortalecen la competitividad empresarial, sino que también impulsan la innovación y la sostenibilidad a largo plazo.

5.5 Implicaciones éticas y legales en la empresa

La Vigilancia Tecnológica (VT) y la Inteligencia Competitiva (IC) implican la recopilación, análisis y utilización de información de diversas fuentes para apoyar la toma de decisiones estratégicas en las organizaciones.

Sin embargo, estos procesos no están exentos de implicaciones éticas y legales que deben ser cuidadosamente consideradas para evitar riesgos y asegurar el cumplimiento normativo, veamos un avance de lo que visualizaremos en el capítulo VI al respecto de esas implicaciones:

5.5.1 Implicaciones Éticas en el ámbito empresarial

1. **Privacidad y Protección de Datos**

La VT e IC pueden involucrar la recolección de datos sensibles o personales. Es crucial que las empresas aseguren que la recopilación de esta información se realice de manera ética, respetando la privacidad de los individuos y cumpliendo con las normativas de protección de datos, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea [25].

2. **Transparencia y Honestidad**

Las prácticas de VT e IC deben llevarse a cabo con transparencia y honestidad. Las organizaciones deben evitar prácticas de espionaje industrial o cualquier forma de obtención de información que implique engaño o manipulación. Esto incluye el uso de información bajo licencias restrictivas o el acceso no autorizado a sistemas de información [26].

3. **Confidencialidad y Uso Responsable de la Información**

La información obtenida a través de VT e IC debe ser manejada con la máxima confidencialidad, especialmente cuando se trata de información sensible o de propiedad de otras organizaciones. Las empresas deben establecer políticas claras sobre cómo se manejará y utilizará esta información, asegurando que no se viole la confianza de las fuentes [27].

5.5.2 Implicaciones legales en el ámbito empresarial

AL igual que los campos éticos, existen tres campos legales implicados:

1. **Cumplimiento de Leyes de Propiedad Intelectual**

Al utilizar información obtenida mediante VT e IC, las empresas deben asegurarse de no infringir leyes de propiedad intelectual, como el uso indebido de patentes, derechos de autor o marcas registradas. El uso de esta información debe realizarse respetando las licencias y los derechos de los titulares de la propiedad intelectual [28].

2. **Normativas Antimonopolio y de Competencia**

Las empresas deben ser cautelosas para no cruzar la línea entre la competencia justa y las prácticas anticompetitivas. Las leyes antimonopolio prohíben prácticas que restrinjan la competencia, como la colusión o el intercambio de información sensible entre competidores, lo que podría ser una tentación al manejar grandes volúmenes de información competitiva [29].

3. **Regulaciones Internacionales**

En un entorno globalizado, las empresas que operan en múltiples jurisdicciones deben estar atentas a las diversas regulaciones internacionales que puedan afectar sus prácticas de VT e IC.

Esto incluye el cumplimiento de normativas específicas de cada país en relación con la protección de datos, la privacidad y la propiedad intelectual [30].

Implicaciones éticas

Las implicaciones éticas y legales de la Vigilancia Tecnológica y de la Inteligencia Competitiva son fundamentales para garantizar que estos procesos se realicen de manera responsable y dentro del marco legal.

Con fundamento en dicho marco legal, se concluye que las empresas deben establecer políticas claras y realizar auditorías regulares para asegurarse de que sus prácticas cumplen con las normativas aplicables y respetan los principios éticos. Esto no solo protege a la organización de posibles sanciones legales, sino que también promueve una cultura empresarial basada en la integridad y el respeto.


CAPÍTULO VI
Implicaciones éticas y legales de una vigilancia tecnológica

Introducción

Este capítulo aborda las implicaciones éticas y legales de la vigilancia tecnológica, incluidos los debates sobre la privacidad, la seguridad y el derecho a la libertad de expresión. Se discutirán las leyes y regulaciones existentes en diferentes países y cómo estas afectan a la vigilancia tecnológica.

6.1 ¿Qué se denomina ética?

La ética puede definirse como la rama de la filosofía que se ocupa del estudio racional de la moral, la virtud, el deber, la felicidad y el buen vivir. La ética es un conjunto de acciones del bien y del mal y, por otro lado, la ciencia es el conjunto de conocimientos de cualquier materia que obedece a leyes postulados y es comprobable mediante un método científico.

Si a lo anterior le adicionamos que la tecnología es el conjunto de conocimientos técnicos que permiten diseñar y crear bienes y servicios que facilitan la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de la humanidad.

Cuando combinamos la ética con la ciencia y la tecnología tenemos un mundo de posibilidades y dilemas éticos, es en este punto donde debemos analizar las implicaciones de esta definición que planteamos.

La ética en la vigilancia tecnológica se fundamenta en aquellos principios y normas que orientan la conducta de quienes llevan a cabo esta actividad, garantizando que se realice de forma responsable y con respeto hacia los derechos de todas las partes involucradas.

6.2 Principios éticos de una vigilancia

Veamos a continuación algunos de los principios éticos más importantes [31] :

- Transparencia: Es esencial ser claro y abierto respecto a los métodos y fuentes de información utilizados, lo que incluye informar a las partes interesadas sobre cómo se recopila y emplea la información.
- Confidencialidad: Proteger la información sensible y respetar la privacidad de personas y organizaciones es crucial. La información recopilada no debe ser usada de manera que perjudique a terceros.
- Legalidad: Cumplir con todas las leyes y normativas aplicables es fundamental. Esto abarca el respeto a los derechos de propiedad intelectual y la abstención de prácticas como el espionaje industrial.
- Integridad: Actuar con honestidad y evitar la manipulación o distorsión de la información. La información debe ser presentada de manera precisa, objetiva y sin sesgos.
- Responsabilidad Social: Considerar el impacto que las actividades de vigilancia tecnológica pueden tener en la sociedad y el medio ambiente. Las decisiones derivadas de esta información deben promover el bienestar colectivo y no solo el interés propio.

En el ámbito de la inteligencia competitiva, estos principios éticos adquieren una relevancia adicional, ya que la información obtenida puede influir de manera significativa en las estrategias y operaciones de una empresa.

La ética en la inteligencia competitiva asegura que las prácticas sean equitativas y no dañen la reputación ni los intereses de otras organizaciones, fomentando una competencia justa y responsable, veamos esos principios básicos en un video realizado con AI.

Video

Video 6.1. Principios éticos de una vigilancia

6.3 Privacidad y confidencialidad en la vigilancia tecnológica

Uno de los desafíos más comunes al abordar los conceptos de privacidad y confidencialidad en el contexto de la vigilancia tecnológica es que a menudo se tiende a fusionarlos, dificultando su distinción. En la literatura sobre el tema, es usual que se enfatice la protección de la información recopilada sin dar suficiente atención a cómo el equipo de vigilancia maneja la interacción con las fuentes de información o trata asuntos de invasión de la privacidad.

Asimismo, frecuentemente el desarrollo del contrato realizado para una vigilancia expresan que las publicaciones o informes incluyan secciones dedicadas a la "confidencialidad" de los datos obtenidos, mientras que la **"privacidad"** es mencionada solo tangencialmente, si acaso se aborda. Por ejemplo, el informe **Improving Access to and Confidentiality of Research Data**[1] del Consejo Nacional de Investigación de Estados Unidos [National Research Council] dedica un capítulo entero a la confidencialidad de los datos, mientras que la privacidad se trata superficialmente en varias secciones.

En una vigilancia tecnológica o mejor dicho en cualquier proceso ético, es fundamental reconocer que el "respeto a la privacidad de las personas involucradas" y la "protección de la confidencialidad de la información" son dos principios éticos relacionados pero distintos.

Desde un punto de vista ético de ambos principios, diferenciarlos es crucial, ya que afectan de manera diferente a las personas implicadas en el proceso de vigilancia tecnológica y conllevan distintas implicaciones en cuanto a su impacto y consecuencias.

6.4 Seguridad en el contexto de la propiedad intelectual de la vigilancia tecnológica

Esta seguridad en el contexto de la propiedad intelectual implica proteger las obras y creaciones de los autores contra el uso no autorizado, la piratería y el robo. Esto incluye la implementación de medidas tecnológicas como los sistemas de gestión de derechos digitales (DRM) para controlar el acceso y uso de las obras protegidas. Sin embargo, estas medidas pueden generar controversias, ya que a veces restringen el acceso legítimo y el uso justo de las obras.

[1] https://nap.nationalacademies.org/catalog/9958/improving-access-to-and-confidentiality-of-research-data-report-of

6.5 Libertad de Expresión

Normalmente escuchamos esta frase cuando se trata de medios de comunicación masivos, pero para una vigilancia tecnológica la libertad de expresión es un derecho fundamental y debe ser protegido incluso en el contexto de la propiedad intelectual. Los debates se centran en cómo equilibrar la protección de los derechos de autor con el derecho de los individuos a compartir información y expresar sus ideas. Las leyes de propiedad intelectual no deben sofocar la creatividad ni restringir el acceso a la información y la cultura.

6.6 Conflictos entre la privacidad, la seguridad y la libertad de expresión en una vigilancia tecnológica

Analizar el conflicto entre la protección de la propiedad intelectual y los derechos fundamentales en el ámbito digital, es un proceso necesario para evitar infringir las leyes que los regulan.

Dichos análisis exploran la tensión que surge entre la necesidad de proteger los derechos de autor y la libertad de expresión, el acceso a la información y la privacidad en especialmente en Internet. Se examinan las estrategias implementadas para combatir la piratería digital, como las medidas tecnológicas de control, la responsabilidad de los proveedores de acceso a Internet y la intervención judicial, y se analizan sus implicaciones en términos de derechos fundamentales.

Invitamos al lector a complementar lo aquí expresado leyendo el documento de la **Fundación Telefónica**[2] sobre lo debatido.

[2] https://telos.fundaciontelefonica.com/archivo/numero085/el-conflicto-entre-propiedad-intelectual-y-derechos-fundamentales/

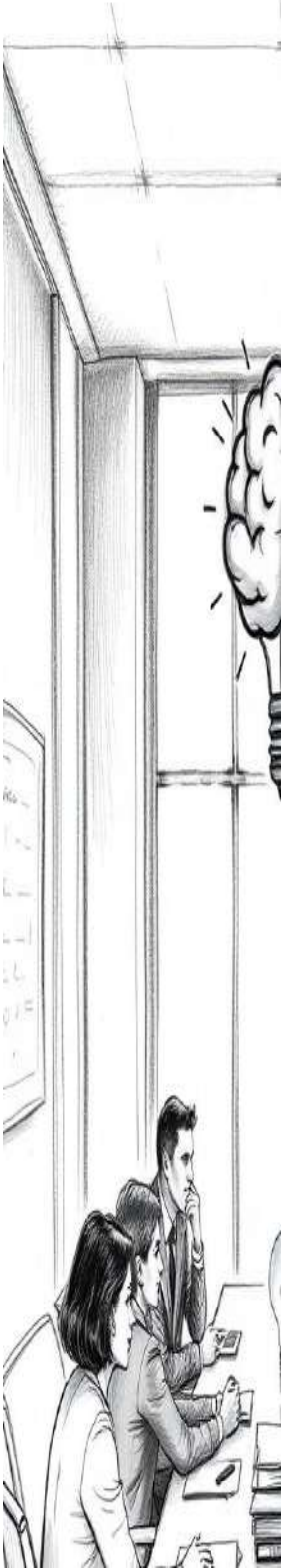
6.7 Los Sistemas P2P y el Desafío a la Responsabilidad por Copyright

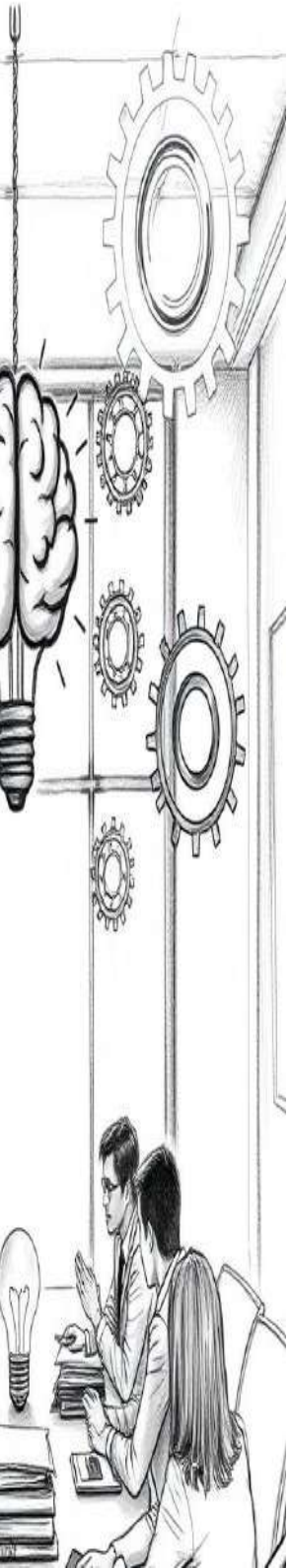
A partir del articulo la IA NotebooKLM de Google expresa que las plataformas de intercambio de archivos descentralizadas, como los sistemas peer-to-peer (P2P), han desafiado las interpretaciones legales tradicionales sobre la responsabilidad por infracción de copyright.

La estructura descentralizada de dichos sistemas dificulta la identificación de los responsables y desdibuja los límites de la responsabilidad indirecta, generando nuevos desafíos legales.

En un principio, los tribunales aplicaron la doctrina Betamax, establecida en el caso Sony de 1985 en EE. UU., la cual eximía de responsabilidad a quienes comercializan productos que pueden usarse tanto para fines legales como ilegales. Esta doctrina buscaba proteger el desarrollo tecnológico, incluso si este desafiaba los derechos de los titulares de copyright.

Otro caso sonado fue el de la **Metro-Goldwyn-Mayer Studios** contra **Groskter** en el año 2005 pues marcó un cambio significativo. En esa sentencia, se declaró responsables por contribución a la infracción a las empresas detrás de los sistemas Morpheus y Kazaa, reduciendo así los requisitos para la responsabilidad de los proveedores de servicios de la Sociedad de la Información. Esta decisión afectó la libertad de información y expresión en internet, ya que impuso mayores restricciones a la operación de sistemas P2P.





La naturaleza descentralizada de los sistemas P2P presenta un obstáculo legal adicional.

A diferencia de plataformas centralizadas como Napster, que fueron clausuradas fácilmente a principios de los 2000, los sistemas P2P alojan los archivos directamente en las computadoras de los usuarios, sin un índice central, lo que dificulta la persecución y cierre de estos servicios por parte de las autoridades.

Un aspecto crucial en este contexto es el debate sobre la responsabilidad de los proveedores de acceso a Internet (ISP) en el intercambio no autorizado de archivos en sus redes. Hasta el momento, no existe una obligación legal para que los ISP monitoreen o filtren el tráfico de archivos protegidos. No obstante, la inclusión de esta responsabilidad en acuerdos internacionales, como el ACTA, ha generado preocupación.

En la Unión Europea, la Directiva 2000/31/CE protege a los proveedores de servicios de una obligación general de supervisar el contenido que transmiten.

Sin embargo, se espera que surja la posibilidad de futuras decisiones del Tribunal de Justicia de la Unión Europea puedan cambiar esta interpretación.

En resumen, las plataformas P2P han planteado interrogantes en cuanto a:

- La aplicabilidad de la responsabilidad indirecta por infracción de copyright

- La necesidad de equilibrar la protección de la propiedad intelectual con la libertad de información y expresión en línea
- El rol y la responsabilidad de los ISP en la lucha contra la piratería.

Estos desafíos legales siguen evolucionando a medida que avanza la tecnología como los debates de hoy en cuanto a la IA y las prácticas de intercambio de archivos se adaptan y se generan con ella.

Conflictos y Equilibrio

El conflicto entre la propiedad intelectual y los derechos fundamentales, como la privacidad y la libertad de expresión, ha sido objeto de intensos debates.

Un ejemplo de ello son las medidas tecnológicas para proteger los derechos de autor, medidas que pueden limitar el acceso a la información y la libertad de expresión. Es crucial encontrar un equilibrio que permita proteger los derechos de los creadores sin vulnerar los derechos fundamentales de los ciudadanos.

6.8 Uso de Tecnología de IA Generativa y sus productos como Propiedad Intelectual

Los titulares de derechos de propiedad intelectual están desarrollando diversas estrategias legales para abordar el uso no autorizado de herramientas de inteligencia artificial (IA) generativa [32] y los productos que esta tecnología genera. Estas estrategias se enfocan en actores clave involucrados en el uso y desarrollo de IA, incluyendo plataformas de IA, usuarios finales y proveedores de infraestructura digital.

Acciones Legales contra Plataformas de IA Generativa: Al igual que en el caso de las plataformas de intercambio de archivos, se han emprendido acciones legales contra desarrolladores de sistemas de IA generativa. Aunque es posible restringir el uso de ciertos sistemas centralizados, las plataformas descentralizadas de IA y los modelos de código abierto presentan un desafío significativo para la regulación y el control.

Medidas para Interrumpir Servicios de IA sin Autorización Judicial: En algunos casos, se han explorado propuestas para la suspensión o cierre de servicios de IA que operan sin las debidas licencias de contenido o que generan productos que infringen derechos de propiedad intelectual, sin necesidad de una autorización judicial previa. Sin embargo, esta medida enfrenta desafíos legales, ya que la intervención directa puede entrar en conflicto con derechos fundamentales como la libertad de expresión y el acceso a la tecnología.

Sanciones a Usuarios Finales por Uso No Autorizado de Productos Generados por IA: En algunos países, se está discutiendo la posibilidad de sancionar a los usuarios finales que utilicen productos generados por IA de forma que infrinja los derechos de propiedad intelectual.

Un modelo similar a la "Ley Hadopi" podría establecer advertencias graduales para los usuarios que persistan en el uso no autorizado de contenidos generados por IA.

¿Qué se denomina ley Hadopi?

Es una ley Francesa que recibe su nombre de la entidad que la administra: la ***Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet*** (Alta Autoridad para la Difusión de Obras y la Protección de Derechos en Internet). Esta autoridad fue creada específicamente para supervisar la implementación de la ley y garantizar la protección de los derechos de autor en el entorno digital.

Dicha ley se implementó en el año 2009 para combatir la piratería en Internet [33], establece un sistema de "tres avisos" para los usuarios que descargan contenido ilegalmente.

El proceso funciona de la siguiente manera:

- Primer aviso: El usuario recibe un correo electrónico advirtiéndole que ha sido detectado descargando contenido ilegal.
- Segundo aviso: Si el usuario continúa descargando contenido ilegal, recibe una carta certificada.
- Tercer aviso: Si el usuario persiste, puede enfrentarse a sanciones que incluyen multas y la suspensión de su conexión a Internet.

La ley ha sido objeto de controversia y debate, ya que algunos la consideran una medida necesaria para proteger los derechos de autor, mientras que otros la ven como una violación de la privacidad y la libertad en Internet. No obstante, este tipo de sanciones plantea preocupaciones éticas y legales, especialmente si no cuentan con la intervención judicial adecuada.

Una legislación al respecto debería considerar:

1. **Vigilancia y Obtención de Datos Personales en el Uso de IA**

La vigilancia del uso de IA para identificar a quienes infringen derechos de propiedad intelectual podría implicar la recolección y tratamiento de datos personales, como direcciones IP y patrones de uso. Esta vigilancia podría ser realizada tanto por los titulares de derechos como por autoridades designadas. Sin embargo, la vigilancia masiva es controvertida y ha sido criticada por organismos de protección de datos en la UE por considerarse una intrusión en el derecho a la privacidad.

2. **Responsabilidad de los Proveedores de Infraestructura de Red**

Aunque aún no se ha implementado legalmente, se ha discutido la posibilidad de responsabilizar a los proveedores de infraestructura digital (ISP) por el uso no autorizado de productos de IA generativa en sus redes.

Lo anterior podría implicar que los ISP supervisen, filtren o bloqueen el tráfico de datos que involucre productos generados por IA que infrinjan derechos de propiedad intelectual. Esta medida, sin embargo, requeriría modificaciones legales en la UE y otros territorios, ya que actualmente la Directiva 2000/31/CE prohíbe imponer una obligación general de control sobre el tráfico de Internet a los ISP.

3. **Desafíos en el Equilibrio Legal**

Estas estrategias reflejan la complejidad de proteger los derechos de propiedad intelectual sin comprometer otros derechos fundamentales, como la libertad de expresión, el derecho a la privacidad y el acceso a la innovación tecnológica.

Encontrar un equilibrio adecuado en el uso de IA generativa y sus productos sigue siendo un desafío legal y ético que evoluciona con los avances tecnológicos en el entorno digital [34].

6.9 Consideraciones éticas en la implementación de la IA en la vigilancia tecnológica

Estas consideraciones no varían mucho con respecto a las descritas en el numeral 6.2, veamos:

1. **Privacidad de Datos**

La recopilación y el análisis de datos obtenidos de la vigilancia plantean preguntas sobre quién tiene acceso a esta información y cómo se utiliza. El consentimiento informado y la transparencia son cruciales en este contexto.

2. **Equidad e Inclusividad**

La IA tiene el potencial de amplificar las desigualdades existentes si los algoritmos se entrenan con datos sesgados o si los recursos de IA no están equitativamente distribuidos.

3. **Autonomía del ejecutor de la vigilancia tecnológica**

El uso de IA para el seguimiento del comportamiento de la vigilancia y su ejecutor y la personalización de la misma puede, en algunos casos, limitar la autonomía de quienes realizan el proceso al restringir las opciones de aprendizaje del ejecutante.

4. **Responsabilidad y Rendición de Cuentas**

Cuando las decisiones de mejoramiento son tomadas o asistidas por algoritmos, la responsabilidad y rendición de cuentas pueden volverse menos claras, lo que plantea preocupaciones éticas.


CAPÍTULO VII
Protegiéndose en la era digital

Introducción

Este capítulo ofrece consejos y estrategias sobre cómo protegerse de la vigilancia tecnológica y mantener la privacidad en la era digital. Se discutirán temas como la ciberseguridad, el cifrado y la importancia de la educación digital.

7.1 La protección de los datos en la historia

La protección de la información ha evolucionado significativamente a lo largo de la historia, adaptándose a los avances tecnológicos y a las necesidades de la sociedad. En el siguiente video diseñado con Invideo ai presentamos un resumen de los hitos más importantes en este sentido:

Video

Video 7.1. La protección de datos en la historia

Es importante que hablemos de la protección de la Privacidad y confidencialidad, la seguridad y la libertad de expresión en la era digital antes y después de la IA:

7.2 Protección en la era digital

La Era Digital que hoy vivimos esta caracterizada por el acceso masivo a internet, la expansión de las redes sociales y el uso generalizado de dispositivos inteligentes. Esta digitalización de nuestras vidas nos brinda enormes beneficios, desde el acceso instantáneo a la información hasta la capacidad de conectarnos con personas en cualquier parte del mundo.

Sin embargo, la digitalización también trae consigo riesgos significativos, especialmente en términos de privacidad y seguridad. La protección de los datos personales, la prevención de ataques cibernéticos y la educación en prácticas seguras en línea se han vuelto imprescindibles para todos. Veamos:

1. **La Importancia de la Seguridad de Datos**

El concepto de seguridad de datos se refiere a la protección de información contra accesos no autorizados, destrucción o modificación. A medida que se utiliza y almacena más información en línea, proteger los datos personales se vuelve una necesidad vital. Las empresas, los gobiernos y los individuos deben tomar medidas para asegurar que la información se maneje de forma segura.

Las medidas descritas incluyen el uso de contraseñas fuertes, la autenticación de dos factores y la encriptación de información confidencial. La protección de datos personales no solo se relaciona con la privacidad de un individuo, sino también con la protección de sus activos y su reputación.

2. **Ciberseguridad: Un Reto Constante**

El crecimiento de las amenazas cibernéticas, como el malware, el phishing y los ataques de denegación de servicio, ha puesto en alerta a todo tipo de usuarios y organizaciones.

La ciberseguridad es un campo en constante evolución que busca prevenir ataques y responder rápidamente ante posibles brechas de seguridad. Los hackers y los cibercriminales desarrollan técnicas más sofisticadas para acceder a sistemas y robar datos.

La ciberseguridad hoy requiere no solo de tecnologías avanzadas, sino de una capacitación continua y de la sensibilización de todos los usuarios sobre la importancia de proteger sus dispositivos y redes.

3. **Privacidad en la Era de las Redes Sociales**

Las redes sociales son un reflejo de la sociedad actual, donde la gente comparte información personal, opiniones y momentos de su vida cotidiana. Sin embargo, estas plataformas también representan un gran riesgo para la privacidad.

A menudo, los usuarios no son conscientes de cuánto de su información personal está disponible públicamente y de cómo esta puede ser utilizada con fines maliciosos o comerciales sin su consentimiento.

La configuración de privacidad, la conciencia de los permisos y la comprensión de los términos de servicio de las redes sociales son herramientas esenciales para protegerse en un entorno digital donde la información fluye rápidamente.

4. **Legislación y Derechos Digitales**

El aumento de los riesgos de privacidad y seguridad ha llevado a los gobiernos a implementar leyes y regulaciones para proteger los datos de los ciudadanos. Reglamentos como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Privacidad del Consumidor de California en los Estados Unidos son ejemplos de esfuerzos para asegurar que las empresas manejen de manera responsable la información personal.

Estas leyes no solo protegen a los individuos, sino que también exigen a las empresas ser más transparentes y responsables sobre el manejo de los datos que recopilan.

La protección en la era digital es un aspecto fundamental de la vida moderna. A medida que la tecnología sigue evolucionando, también lo harán los riesgos asociados. Adoptar medidas de seguridad, educarse sobre los derechos digitales y mantenerse informado sobre las buenas prácticas en ciberseguridad son pasos esenciales para proteger nuestra privacidad y seguridad en línea. En última instancia, la protección en la era digital es una responsabilidad compartida entre usuarios, empresas y gobiernos.

7.3 Protección en la era de la inteligencia artificial

La era digital ha transformado la vida cotidiana, facilitando el acceso a la información, las comunicaciones y los servicios en línea.

Sin embargo, junto con los beneficios, también se presentan riesgos, especialmente en términos de seguridad y privacidad.

En ese contexto, la inteligencia artificial (IA) emerge como una herramienta poderosa para fortalecer la protección digital, aunque también plantea nuevos desafíos. Explorar el rol de la IA en la seguridad y la privacidad digital nos permite comprender mejor cómo aprovechar esta tecnología para crear un entorno en línea más seguro, las principales características de dicho rol:

1. **La IA como Aliada en la Seguridad Digital**

La IA se utiliza para fortalecer la ciberseguridad mediante técnicas de detección y respuesta en tiempo real a amenazas. Algoritmos de aprendizaje automático permiten a los sistemas de IA identificar patrones sospechosos y comportamientos anómalos que podrían indicar un intento de ataque, como intentos de phishing o malware. Además, la IA ayuda a mejorar la autenticación de usuarios a través de tecnologías avanzadas, como el reconocimiento facial y de voz, lo que agrega una capa adicional de seguridad.

2. **Inteligencia Artificial y Privacidad, un Equilibrio Delicado**

Si bien la IA puede mejorar la seguridad, también presenta desafíos significativos para la privacidad. Muchas aplicaciones de IA requieren grandes volúmenes de datos para su entrenamiento y funcionamiento efectivo, lo que plantea preocupaciones sobre el manejo y almacenamiento de información personal. Este apartado podría explorar cómo los sistemas de IA pueden diseñarse para proteger la privacidad de los usuarios mediante técnicas como el aprendizaje federado y la anonimización de datos, que buscan equilibrar la seguridad con el respeto a la privacidad.

3. **La IA y la Automatización de los Ataques Cibernéticos**

A medida que la IA se utiliza en la defensa digital, también se convierte en una herramienta accesible para los cibercriminales, quienes pueden automatizar y sofisticar sus ataques. La IA puede utilizarse para realizar ataques más difíciles de detectar, como campañas de phishing personalizadas o manipulación de redes sociales mediante bots inteligentes.

Es importante complementar lo descrito hasta el momento con el detallar algunos de los riesgos emergentes y la necesidad de sistemas de seguridad que estén preparados para enfrentar ataques potenciados por IA.

4. **Legislación y Ética en el Uso de IA para la Protección Digital**

La expansión de la IA en el ámbito de la seguridad digital ha llevado a legisladores y expertos a trabajar en normas que regulen su uso ético y legal. Esa legislación se puede profundizar en cómo las regulaciones como el Reglamento General de Protección de Datos (GDPR) y la reciente legislación sobre IA en la Unión Europea, buscan garantizar que las herramientas de IA se utilicen de manera responsable y respetuosa de los derechos de privacidad de los individuos.

De lo descrito en los numerales anteriores podemos expresar que la inteligencia artificial tiene el potencial de revolucionar la protección en la era digital, pero requiere un uso cuidadoso y ético para equilibrar la seguridad y la privacidad. Si bien es una herramienta poderosa para la defensa cibernética, también presenta riesgos que deben gestionarse mediante regulaciones, buenas prácticas y educación. Aprovechar la IA para mejorar la seguridad digital sin comprometer la privacidad es uno de los grandes retos y oportunidades de nuestra era.


CAPÍTULO VIII
Una experiencia académica de vigilancia tecnológica

Una experiencia en la academia

En este capítulo se describe la manera como se realizó una vigilancia tecnológica para buscar la categorización de un grupo de investigación del Instituto Tecnológico Metropolitano.

8.1 El grupo GNOMON-ITM

El informe "Informe de vigilancia e inteligencia competitiva con enfoque prospectivo" describe las actividades de investigación y desarrollo del grupo GNOMON-ITM. Este informe menciona dos líneas de investigación principales:

1. **Gestión del conocimiento y nuevas tecnologías para la educación**

Esta línea se centra en la aplicación de tecnologías de la información y la comunicación (TIC) en la educación y en cómo estas pueden mejorar los procesos de enseñanza y aprendizaje. El enfoque de esta línea se divide en dos perspectivas:

- Proyectos de Desarrollo Tecnológico 4.0 (PDT) para el sector Educativo

Esta perspectiva busca desarrollar soluciones tecnológicas que puedan ser aplicadas a la educación, utilizando tecnologías de la Industria 4.0. Ejemplos de esto son el diseño de plataformas de aprendizaje en la nube y el desarrollo de recursos didácticos basados en realidad aumentada.

- Investigación sobre impactos de las tecnologías 4.0 en la educación

Esta perspectiva se centra en analizar cómo la aplicación de las tecnologías de la Industria 4.0 a la educación impacta las prácticas educativas y cómo se pueden diseñar proyectos de investigación para abordar estos impactos.

2. **Innovación Educativa**

Esta línea se enfoca en el diseño e implementación de nuevas estrategias didácticas y pedagógicas, con el objetivo de mejorar la calidad de la educación. Esta línea también se divide en dos perspectivas:

- Proyectos de innovación educativa (PiE)

Esta perspectiva busca desarrollar nuevas estrategias didácticas y pedagógicas que respondan a las necesidades de talento humano de la Industria 4.0. Esto implica la creación de recursos educativos que permitan a los estudiantes desarrollar las habilidades y competencias necesarias para prosperar en un entorno laboral cada vez más digitalizado.

- Investigación sobre los retos del diseño de PiE

Esta perspectiva analiza los desafíos que se presentan al diseñar e implementar proyectos de innovación educativa en el contexto de la Industria 4.0.

Ambas líneas de investigación del grupo GNOMON-ITM se enfocan en la intersección entre la tecnología y la educación, buscando aprovechar el potencial de la Industria 4.0 para mejorar los procesos de enseñanza y aprendizaje y formar a los estudiantes para los desafíos del futuro.

8.2 Resumen

Vamos a describir el texto que representa el informe de vigilancia tecnológica e inteligencia competitiva realizado por el grupo Gnomon ITM sobre las líneas de investigación en educación 4.0.

El informe analiza las posibles aplicaciones de tecnologías de la industria 4.0 como la inteligencia artificial, la robótica, la Internet de las cosas y los gemelos digitales en la educación. Los autores exploran las necesidades en **I+D** en cada campo, buscando identificar posibilidades prospectivas en relación con las áreas de investigación del grupo Gnomon ITM. Además, el informe también incluye una revisión de la literatura sobre el tema, con el objetivo de identificar las tendencias actuales y futuras en la innovación educativa.

8.3 El enfoque de la vigilancia

El enfoque de la vigilancia tecnológica es un proceso sistemático y continuo que tiene como objetivo identificar oportunidades y amenazas del grupo de investigación, se utilizaron dos enfoques para analizar las posibilidades prospectivas de **I+D** en el contexto de la Industria 4.0 y la educación:

1. **Problematización investigativa**

Este enfoque se centra en identificar y categorizar posibles preguntas de investigación que sean relevantes para cada línea de investigación del grupo GNOMON ITM.

Se buscó entender cómo los campos tecnológicos de la Industria 4.0 podrían impactar las prácticas educativas y cómo se pueden diseñar proyectos de investigación para abordar estos impactos.

2. **Prospectiva tecnológica**

Este enfoque se centra en identificar las posibilidades de desarrollo tecnológico (PDT) que pueden surgir de la aplicación de la Industria 4.0 al sector educativo. Se busca analizar cómo las tecnologías 4.0 pueden utilizarse para crear proyectos de innovación educativa (PiE) que respondan a las necesidades de talento humano en la Industria 4.0.

Estos dos enfoques se complementan para ofrecer una visión completa de las posibilidades de I+D en el contexto de la Industria 4.0 y la educación.

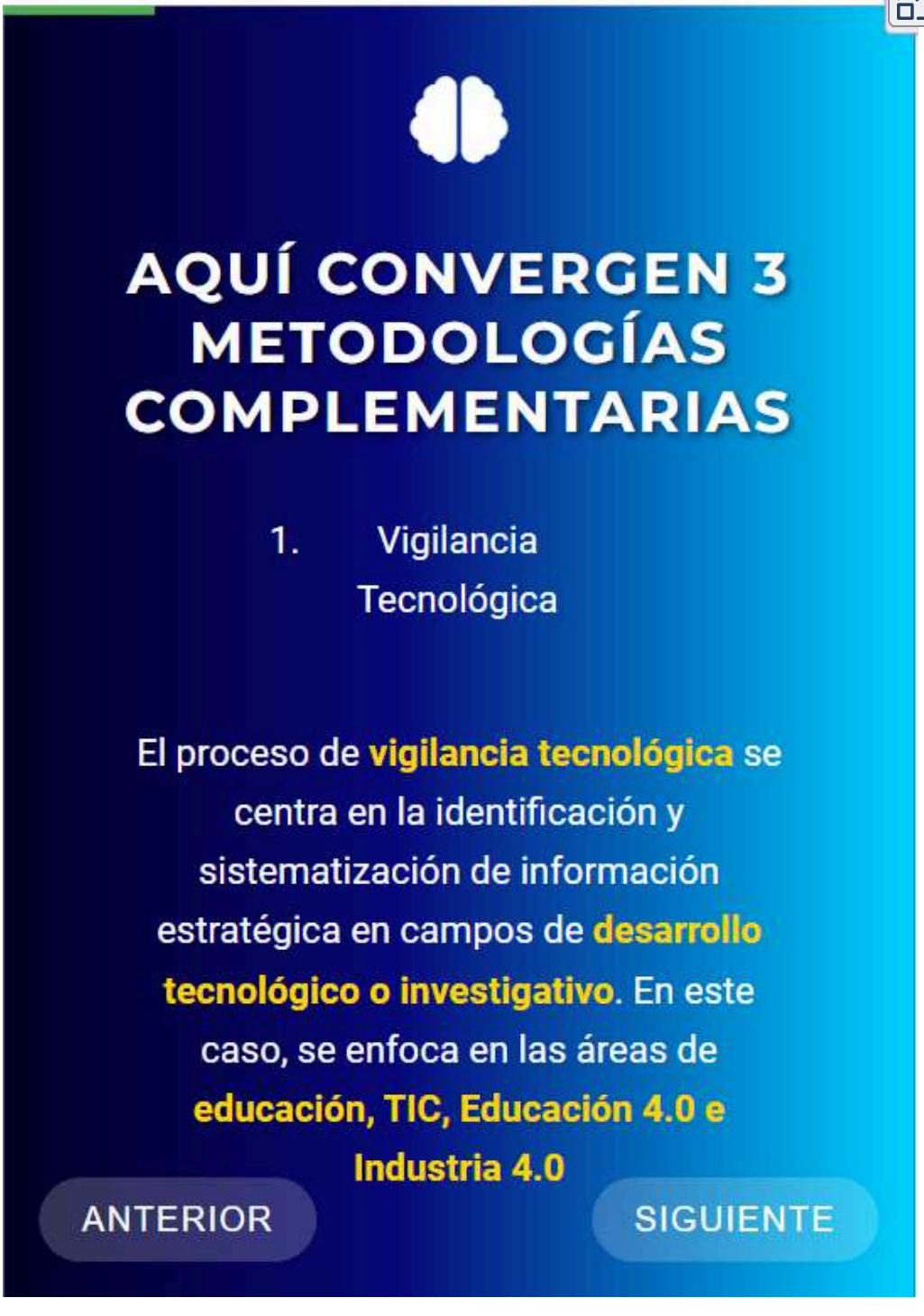
El informe de la vigilancia realizada propone analizar cada campo tecnológico de la Industria 4.0 desde la perspectiva de la problematización investigativa y la prospectiva tecnológica. Por ejemplo, en el campo de Big Data, la problematización investigativa se centraría en cómo analizar los datos generados por los procesos de aprendizaje mediados por la tecnología, mientras que la prospectiva tecnológica se enfocaría en el diseño de plataformas para el procesamiento de información educativa en la nube.

8.4 Metodología de la vigilancia realizada

La metodología empleada combina elementos de vigilancia tecnológica, bibliometría e inteligencia competitiva, con el objetivo de identificar información estratégica en el campo del desarrollo tecnológico e investigativo.

Herramientas Utilizadas

El informe menciona el uso de software para el análisis bibliométrico, como SciMAT, aunque no se describe en detalle su aplicación. También se elaboraron tablas y gráficos para la presentación de los resultados. En la siguiente presentación se ilustra la metodología empleada:


AQUÍ CONVERGEN 3 METODOLOGÍAS COMPLEMENTARIAS
1. Vigilancia Tecnológica
El proceso de vigilancia tecnológica se centra en la identificación y sistematización de información estratégica en campos de desarrollo tecnológico o investigativo. En este caso, se enfoca en las áreas de educación, TIC, Educación 4.0 e Industria 4.0
ANTERIOR
SIGUIENTE

La vigilancia tecnológica permitió identificar las principales tendencias en la investigación y el desarrollo tecnológico en las áreas de interés, así como las posibles aplicaciones de la Industria 4.0 a la educación. El análisis prospectivo permitió identificar áreas estratégicas de I+D para una Educación 4.0

8.5 Elementos identificados en la vigilancia tecnológica del Grupo GNOMON-ITM

La metodología aplicada en el desarrollo de la vigilancia tecnológica del Grupo GNOMON-ITM permitió identificar diversos elementos clave en relación a la Industria 4.0 y su impacto en la educación, veamos:

- Tendencias en publicaciones científicas

El análisis bibliométrico de las bases de datos Scopus, ScienceDirect, EBSCOhost y Web of Science permitió identificar las principales tendencias en publicaciones científicas relacionadas con la Industria 4.0 y la educación.Se analizaron palabras clave, ecuaciones de búsqueda, tipos de documentos, autores y áreas temáticas para determinar las áreas de mayor interés y actividad investigativa.

- Factores críticos que afectan la disponibilidad de tecnologías y conocimiento

Se identificaron factores como la disponibilidad de tecnologías 4.0 y el acceso a la información investigativa como elementos que pueden influir en el desarrollo de la Industria 4.0 y su aplicación en la educación.

- Relación entre la I+D del grupo GNOMON y la Industria 4.0

La inteligencia competitiva permitió analizar la relación existente entre las líneas de investigación del grupo GNOMON y la Industria 4.0. [11-13] Este análisis permitió identificar las áreas de mayor sinergia y las oportunidades de colaboración entre el grupo y la industria.

- Oportunidades de investigación y desarrollo tecnológico

El análisis de la información recopilada, incluyendo el análisis prospectivo, permitió identificar posibilidades de trabajo investigativo y de desarrollo tecnológico en el campo de la Industria 4.0 y la educación.Esto se enfocó en las dos líneas de investigación del Grupo GNOMON-ITM: Gestión del Conocimiento y Nuevas Tecnologías para la Educación, e Innovación Educativa.

- Mapa de ideas en I+D para las líneas de investigación

Se elaboró un mapa de ideas que visualiza las posibilidades de investigación y desarrollo tecnológico para las líneas de investigación del grupo GNOMON. [1] Este mapa permite guiar las futuras actividades del grupo en relación a la Industria 4.0 y la educación.

En resumen, la metodología aplicada permitió identificar tendencias en publicaciones, factores críticos, relaciones entre la I+D del grupo y la Industria 4.0, así como oportunidades de investigación y desarrollo.

Los elementos descritos y plasmados en el informe final de la vigilancia tecnológica realizada, incluyendo tablas, gráficas, hallazgos del análisis prospectivo y conclusiones, brindan al Grupo GNOMON-ITM una base sólida para la toma de decisiones y el desarrollo de estrategias en el contexto de la Industria 4.0 y su impacto en la educación.

8.6 El análisis prospectivo

El análisis prospectivo realizado en el informe buscó identificar posibilidades de trabajo de investigación y desarrollo tecnológico en el campo de la Industria 4.0 y la educación. Dicho análisis se enfoca en las perspectivas de las dos líneas de investigación del Grupo GNOMON-ITM y da a conocer lo siguiente:

8.6.1 Línea Gestión del conocimiento

Del informe se pueden inferir algunas áreas potenciales de mejoramiento:

- Impacto de la Industria 4.0 en la Gestión del Conocimiento

La Industria 4.0 introduce nuevas tecnologías y procesos que transforman la forma en que se genera, comparte y utiliza el conocimiento en las organizaciones. Investigar cómo estas tecnologías (como la inteligencia artificial, el internet de las cosas y la analítica de big data) impactan la gestión del conocimiento en el contexto educativo sería un área de investigación relevante.

- Gestión del Conocimiento en la Educación 4.0

La Educación 4.0 se refiere a la transformación digital de la educación, impulsada por las tecnologías de la Industria 4.0. La investigación podría enfocarse en cómo aplicar los principios de la gestión del conocimiento para mejorar la enseñanza y el aprendizaje en entornos educativos digitales.

- Integración de la Gestión del Conocimiento con las Nuevas Tecnologías para la Educación

Explorar cómo las nuevas tecnologías educativas pueden utilizarse para facilitar la gestión del conocimiento en las instituciones educativas. Esto podría incluir el desarrollo de plataformas de aprendizaje en línea que incorporen herramientas de gestión del conocimiento o la investigación sobre el uso de la realidad virtual y aumentada para la formación y el intercambio de conocimientos.

8.6.2 Línea Innovación Educativa

Para la línea de Innovación Educativa, el proceso de vigilancia tecnológica identificaría las posibilidades de investigación a través del análisis prospectivo. Este análisis se basa en la información recopilada y analizada en las etapas previas de la vigilancia tecnológica, las principales son:

- Tendencias en publicaciones científicas

El análisis bibliométrico de bases de datos como Scopus, ScienceDirect, EBSCOhost y Web of Science permite identificar las áreas de investigación emergentes y las tendencias en publicaciones relacionadas con la Innovación Educativa.

- Relación I+D con la Industria 4.0

El análisis de inteligencia competitiva permite identificar cómo la Industria 4.0 está impactando la educación y qué oportunidades de I+D existen en la intersección de ambas áreas, especialmente para la línea de Innovación Educativa.

- Factores críticos

La identificación de factores que pueden afectar la disponibilidad de tecnologías y conocimiento, como el acceso a tecnologías 4.0 y a la información investigativa influye en las posibilidades de investigación.

8.7 Conclusiones del informe

Basándose en la metodología descrita en las fuentes, se pueden inferir algunas conclusiones del informe de vigilancia tecnológica realizado por el Grupo GNOMON-ITM:

1. **Identificación de oportunidades de I+D**

El informe busca identificar oportunidades de investigación y desarrollo tecnológico en el campo de la Industria 4.0 y la educación para el grupo GNOMON-ITM. Esto se logra mediante el análisis de la información científica, las tendencias y el entorno competitivo.

2. **Impacto de la Industria 4.0 en la educación**

El informe analiza la relación entre la Industria 4.0 y la educación, especialmente en las áreas de interés del Grupo GNOMON-ITM: Gestión del Conocimiento y Nuevas Tecnologías para la Educación, e Innovación Educativa. Se espera que el informe arroje luz sobre cómo la Industria 4.0 está transformando la educación y qué oportunidades presenta para la investigación.

3. **Tendencias en investigación y desarrollo**

A través del análisis bibliométrico y de inteligencia competitiva, el informe identifica tendencias actuales y futuras en la investigación y desarrollo de tecnologías 4.0 aplicadas a la educación. Estas tendencias pueden servir como guía para futuras investigaciones del grupo GNOMON-ITM.

Para finalizar podemos expresar que basados en la metodología descrita en las fuentes surgen algunas recomendaciones para el Grupo GNOMON-ITM.

A partir del documento presentado los investigadores del grupo ofrezcan recomendaciones específicas para el Grupo GNOMON-ITM en cuanto a las áreas de investigación y desarrollo tecnológico que deberían priorizar en el contexto de la Industria 4.0 y la educación. Estas recomendaciones se basan en los hallazgos del análisis prospectivo.


EPÍLOGO
Dialogando con un chabot sobre vigilancia tecnológica

9.1 Introducción

Según lo expresa el Diccionario de "Real Academia Española", epílogo de una obra hace referencia a la lo expresado una composición literaria como la presentada en este libro, es una síntesis, compendio o resumen de las reflexiones relacionadas con su tema central, para nuestro caso: la vigilancia tecnológica.

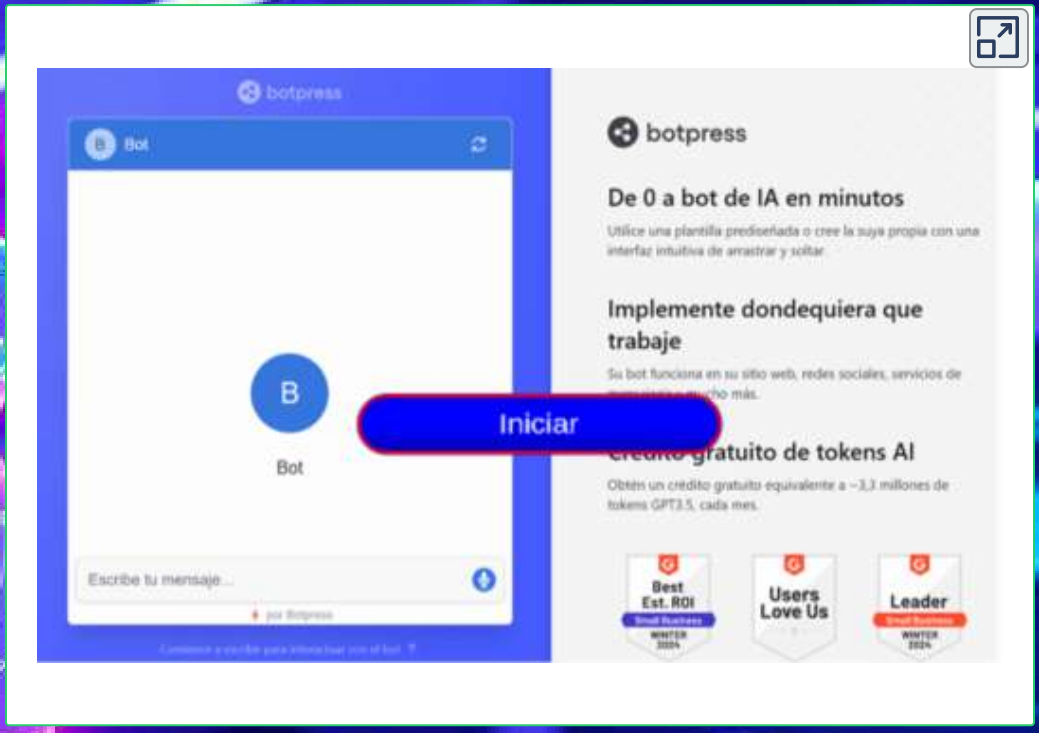
Este epílogo está presentado en forma de chatbot, una herramienta de la era donde la inteligencia artificial toma cada día más ventaja y qué a pesar de ello genera interrogantes pesimistas.

La historia de la IA nos dice que los primeros programas pioneros fueron rudimentarios, pero sentaron las bases para los avances actuales en IA conversacional, entre ellos tenemos:

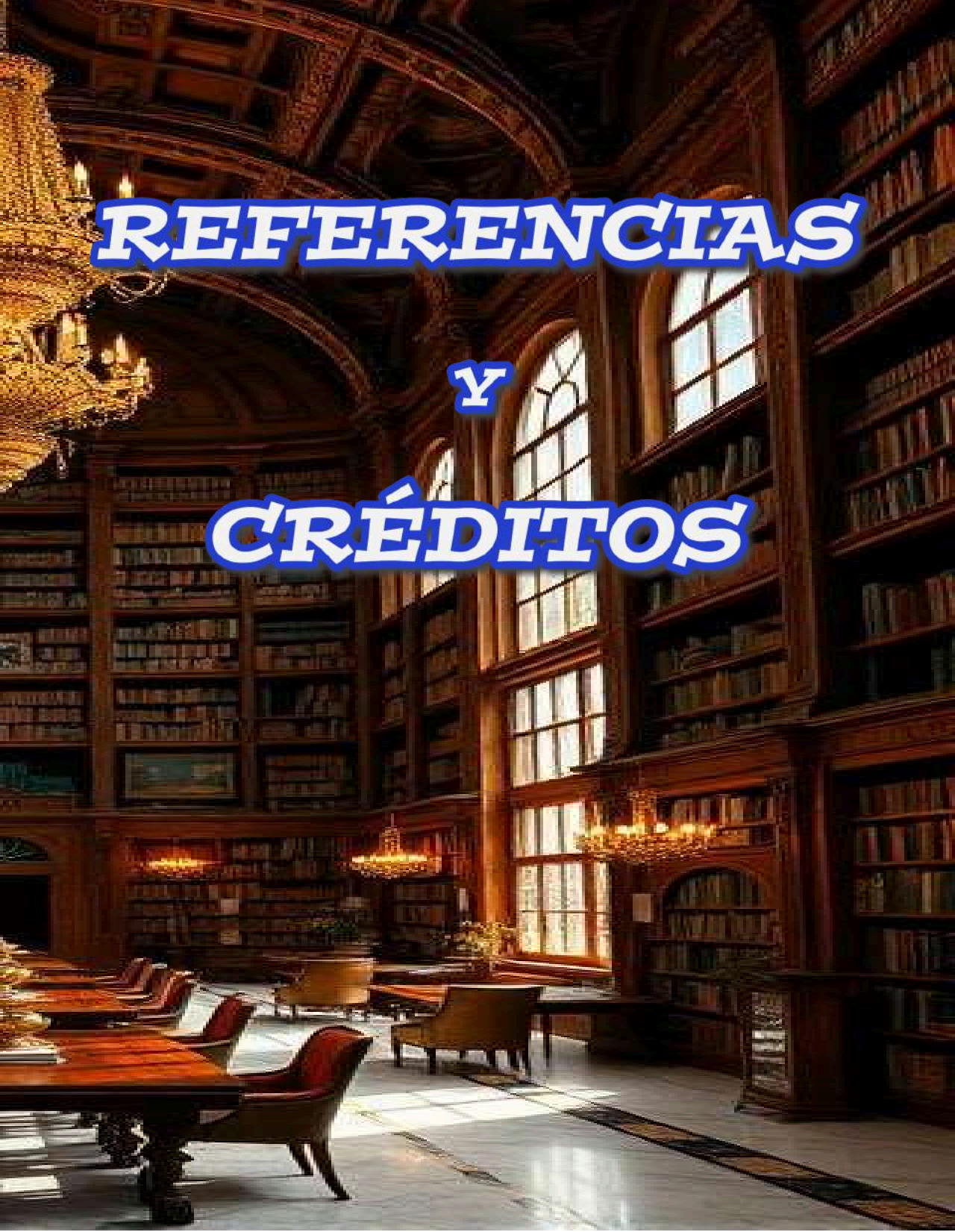
- ELIZA (1966). Desarrollado por Joseph Weizenbaum en el MIT, ELIZA fue uno de los primeros programas en simular una conversación humana. Utilizaba reglas simples de coincidencia de patrones para responder, simulando a un psicoterapeuta.

- PARRY (1972). Creado por el psiquiatra Kenneth Colby, PARRY fue una evolución de ELIZA, diseñado para simular una conversación con una persona con esquizofrenia paranoide. Tenía reglas más complejas y podía mantener una conversación coherente en ciertos temas específicos.


Desde el año 2021 disponemos de Modelos de Deep Learning o desarrollo de redes neuronales profundas y, más recientemente, los transformadores, vamos a lo nuestro:
A partir de una base de datos elaborada con documentos en formato pdf, hemos diseñado nuestro chatbot con las herramientas IA de "Botpress."



Interactivo 9.1. Chatbot de vigilancia tecnológica.


REFERENCIAS
Y
CRÉDITOS

Bibliografía

[1] Strathern, P. (2015). Hume en 90 minutos. Spain: Siglo XXI.

[2] Metamorfosis: 16 Catalizadores Para Una Transformación Radical. (2024). (n.p.): 22 Lions.

[3] Holguin, A. (2020). BREVE HISTORIA: DEL" ALÓ" AL CELULAR. Cuadernos Unimetanos, (41), 69-76.

[4] Aguirre Rosado, K. M. (2023). Uso de drones con reconocimiento facial como mecanismo de control de seguridad en la facultad de ciencias agropecuarias (FACIAG) (Bachelor's thesis, Babahoyo: UTB-FAFI. 2023).

[5] Villegas, F. (2020). Relatividad y el Sistema de Posicionamiento Global (GPS). Revista de investigación de Física, 23(1), 44-47

[6] VASQUEZ, H. G. E., Merchán, A. A., & Siguenza, A. P. (2020). LOS SISTEMAS DE VIGILANCIA EN LA ORGANIZACIÓN: UNA DESCRIPCIÓN HACIA LA ESTRUCTURA DE RED. Revista Pertinencia Académica. ISSN 2588-1019, 4(5), 334-346.

[7] Sánchez, Y. E., & López, J. J. S. (2021). Vigilancia tecnológica como mecanismo de innovación educativa. Publicaciones e Investigación, 15(4).

[8] Bollás Sánchez, R. L., & Valencia Pérez, L. R. (2021). Análisis de los modelos de la vigilancia tecnológica e inteligencia competitiva en proyectos de I+ D+ i.

[9] Macén, A. G. (2021). El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea. Cuadernos de Derecho Transnacional, 13(2), 209-232.

[10] Del Río Portilla, J. A. (2021). El arte de patentar. Spain: Reverte.

[11] Shark, A. R. (n.d.). Technology and Public Management. United Kingdom: Taylor & Francis.

[12] David, F. R. (2003). Conceptos de administración estratégica. España: Pearson Educación.

[13] Gógova, S. (2015). Inteligencia competitiva. España: Ediciones Díaz de Santos.

[14] Inteligencia estratégica del futuro: Pensamiento crítico e interconectado en un mundo global. (2023). España: Siglo del Hombre Editores.

[15] Velayos-Ortega, G., López Carreño, R. (2023). Patentes: Búsqueda y uso bibliográfico. España: Editorial UOC, S.L.

[16] Leal Cardozo, L., Escobar Valencia, M., Mosquera Abadía, H. A., Medina Vásquez, J. E., Mosquera Guerrero, A. (2014). Construyendo la calidad en los ejercicios de prospectiva y vigilancia tecnológica. Colombia: Universidad del Valle.

[17] Bravo, L. E. C., Molano, J. I. R., & López, H. J. F. (2021). Analítica académica: nuevas herramientas aplicadas a la educación. Boletín Redipe, 10(3), 137-158.

[18] Group, W. B. (2016). World Development Report 2016: Digital Dividends. United States: World Bank Publications.

[19] Zaintek (2003). Guía de Vigilancia Tecnológica: Sistema de información estratégica en las pymes. Bilbao: Servicio de vigilancia tecnológica e inteligencia competitiva. Depósito Legal: BI-1042-03. ISBN: 84-7752-348-7.

[20] Modelo de Vigilancia Tecnológica y Competitiva. (2007). Modelos de vigilancia tecnológica e inteligencia competitiva. BAI Agencia de Innovación, Bizkaia.

[21] Inteligencia Económica y Tecnológica. (2002). Guía para principiantes y profesionales. Innovación, Desarrollo y Transferencia de Tecnología, S.A. Comunidad de Madrid – Dirección General de Investigación.

[22] INTEC. (2009). La Inteligencia Competitiva: Factor clave para la toma de decisiones estratégicas en las organizaciones. Fundación madrid para el Conocimiento.

[23] Inteligencia Económica y Tecnológica. (2002). Guía para principiantes y profesionales. Innovación, Desarrollo y Transferencia de Tecnología, S.A. Comunidad de Madrid – Dirección General de Investigación.

[24] PUZZLE. (2005). Inteligencia Competitiva en España y Latinoamérica. Año 4, Edición Nº 16, Marzo-Abril 2005, ISSN 1696-8573.

[25] Tavani, H. T. (2016). Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing (5th ed.). Wiley.

[26] Fleisher, C. S., & Bensoussan, B. E. (2015). Business and Competitive Analysis: Effective Application of New and Classic Methods. FT Press.

[27] Palomares, S., & Serrano, C. (2018). Inteligencia Competitiva: Desarrollo de Capacidades en la Empresa. ESIC Editorial.

[28] Porter, M. E. (2008). On Competition. Harvard Business Press.

[29] OECD. (2015). Competition Law and Policy in Latin America: Peer Reviews of Argentina, Brazil, Chile, Mexico and Peru. OECD Publishing.

[30] Sullivan, D. J. (2014). International Business: Strategy and the Multinational Company. Routledge.

[31] Santana, A., Valera, L. (2022). Ética y seguridad: Aprendizajes y desafíos. Chile: Ediciones UC.

[32] IA generativa: cuestiones de propiedad intelectual. (2024). (n.p.): WIPO.

[33] Responsabilidad de los proveedores del servicio de internet en relación con la propiedad intelectual. (2015). Colombia: Universidad Externado.

[34] La Evolución de la Inteligencia Artificial: de Asistentes Virtuales a Robots Autónomos. (2024). (n.p.): Amazon Digital Services LLC - Kdp.

Créditos de las imágenes

Iconos de lista. Imagen deImagen PNG de es.pngtree.com/

Portada Capítulo I. Imagen creada con tecnología Dalle-E3 de bing

Página 13.Imagen de b0red en Pixabay

Página 19. Imagen de Gordon Johnson en Pixabay

Página 28. Imagen de Alexandra_Koch en Pixabay

Portada capítulo II. Imagen de Gerd Altmann en Pixabay

Portada Capítulo III. Imagen creada con tecnología Dalle-E3 de bing

Página 40. Imagen de Vilius Kukanauskas en Pixabay

Pagina 51. Imagen de Bing

Portada capítulo IV. Imagen de Gianluca en Pixabay

Portada capítulo V. Imagen de Sjjalinn from Pixabay

Portada capítulo VI. Imagen de Bing

Pagina 131. Imagen de Gerd Altmann from Pixabay

Portada capítulo VII. Imagen de Bing

Portada capítulo IX. Imagen de Willi-van-de-Winkel from Pixabay

Imágenes generadas por Polinations con modelo Flux

- Página 14: istory_artificial_intelligence_watercolor.jpg
- Página 38: vigilancia_tecnologica-3D.jpg
- Páginas 48-49: edad_media_pencil-sketch.jpg
- Página 80: productos_competencia_automoviles_pixar_isometric.jpg
- Páginas 92-93: espionaje_digital.jpg
- Página 97: inteligencia_competitiva_watercolor.jpg
- Páginas 106-107: vigilancia_tecnológica_redes_sociales_estilo_disney-3D.jpg
- Páginas 128-129: etica_conocimiento_empresa_pencil-sketch.jpg
- Página 130: consideraciones_eticas_pencil-sketch.jpg

- Página 150: un hacker en la empresa,comic.jpg
- Poster video página 151: cifrado-isometric.jpj
- Página 170: vigilancia_isometric.jpg
- Páginas 175-176: Chatbot3D.jpg
- Páginas 177-178: Chatbot_watercolor.jpg
- Páginas 179-180: chatbot_neón.jpg
- Página 182: biblioteca_moderna.jpg

Créditos de los videos

- Página 28: Los drones de Peter Florea de Pixabay
- Página 30: Vigilancia en línea de 31963655 de Pixabay
- Página 47: Metodología de la vigilancia tecnológica e inteligencia estratégica de Universidad de Antioquia
- Página 89: Ciclo de vida de un producto o innovación creado con Invideo IA
- Página 106: Las redes sociales y las comunidades sociales creado con Invideo IA
- Página 113: Las patentes, la Inteligencia Artificial y la Automatización creado con Invideo IA
- Página 120: La VT: un pilar de innovación empresarial creado con Invideo IA
- Página 133: Principios éticos de una vigilancia creado con Invideo IA
- Página 147: La protección de datos en la historia creado con Invideo IA


DESCARTES
matemáticas interactivas