LA OLA TECNOLÓGICA

La redefinición del mundo

Mucho de cierta es la frase de “cuando el producto es gratis, el producto eres tú”.
Lo anterior se puede aplicar en las redes sociales, como TikTok, Instagram o Facebook y cualquier aplicación gratuita. Así, al momento de registrarnos, **los usuarios otorgan sus datos a las plataformas**.

LA OLA TECNOLÓGICA: La redefinición del mundo

por Frank Brugal

Ciberseguridad, la tecnología e inteligencia artificial. La creo el ser humano.

GRANDES COMERCIANTES ECOLOGISTA:

Según un estudio de Emission Analytics (2022), los VEHÍCULOS ELÉCTRICOS pueden sorprendernos. Publicado inicialmente en 2022, el informe recibe atención en 2024 tras ser citado por el Wall Street Journal.

Emission Analytics destaca que los vehículos eléctricos emiten más partículas tóxicas debido al DESGASTE DE NEUMÁTICOS. Estos autos, siendo un 30% más PESADOS que sus homólogos de gasolina, plantean desafíos medioambientales.

¡Cuidado! (No todo es color de rosa en los famosos VEHÍCULOS ELÉCTRICOS). El estudio revela que frenos y neumáticos de autos eléctricos liberan 1.850 veces más partículas contaminantes que los tubos de escape modernos, equipados con filtros "EFICIENTES". Las emisiones de los vehículos a gasolina alcanzan nuevos mínimos.

TIERRA ARRASADA **por Frank Brugal**

En el intrigante viaje hacia los albores de la historia, las cavernas prehistóricas fungieron como lienzos primitivos, donde las primeras tecnologías se plasmaron en duras piedras. Estas pinturas, lejos de ser simples representaciones, se erigieron como crónicas visuales, registros de los acontecimientos diarios de una época olvidada. En mi ensayo, exploraré la noción de que estos compañeros de cueva (observadores) de la piedra prehistórica no eran meros testigos pasivos, sino ingeniosos arquitectos de una forma incipiente de expresión y base de datos.Al adentrarnos en el tejido temporal, es crucial evitar subestimar el ingenio de aquellos artistas primitivos. Su habilidad para observar, aprender y replicar estrategias de supervivencia a través de las representaciones visuales en las paredes de las cavernas revela una inteligencia adaptativa que, sin saberlo, sentó las bases para la evolución tecnológica.

En el contexto actual, esta analogía resuena de manera sorprendente. Los videos instructivos, las granjas de promoción, producción de contenido y comercialización y las redes sociales han tomado el relevo de las paredes de las cavernas, transformándose en modernas formas de expresión y transmisión de conocimiento. Las plataformas digitales no solo replican el proceso ancestral de observar y aprender realizaban aquellos quehaceres, sino que amplifican exponencialmente la difusión de información. Al insertar la tecnología y su evolución en esta reflexión, surge una nueva capa de complejidad. La capacidad de la misma para analizar patrones, comprender datos y aprender de manera autónoma se asemeja a la destreza primitiva de aquellos observadores de la piedra. En este sentido, se convierte en una extensión contemporánea de nuestra habilidad ancestral para observar, aprender y adaptarnos.

En conclusión, la evolución tecnológica, desde las pinturas en las cavernas hasta la inteligencia artificial, destaca la persistente búsqueda de la humanidad por expresarse y comprender el

mundo que la rodea. Esta conexión entre el pasado y el presente revela una continuidad sorprendente en nuestra capacidad para innovar y adaptarnos, incluso cuando la tecnología nos conduce a territorios inexplorados.

En la actualidad, la experiencia digital se ha vuelto más personalizada y, en cierto modo, predecible. Las plataformas utilizan algoritmos avanzados que, más allá de lo binario, se sumergen en las preferencias individuales del usuario. Desde videos hasta búsquedas en internet, la tecnología se convierte en un reflejo de nuestras inclinaciones y aversiones, incluso en el ámbito político en las redes sociales.

Este fenómeno se intensifica con la omnipresencia de los smartphones. Las plataformas de video y redes sociales,diseñadas para la comodidad de la pantalla táctil, han transformado la manera en que consumimos contenido.

La generación Z, en particular, ha adoptado una velocidad de reproducción más rápida, a 1.5, consumiendo información de manera eficiente en cualquier momento libre, ya sea en el tren o durante un breve receso.

El smartphone se ha convertido en el epicentro de esta revolución digital. Cerca del 70% de los contenidos, desde videos hasta series, son consumidos a través de este dispositivo, relegando incluso al televisor a un segundo plano en las preferencias de las nuevas generaciones. La portabilidad y la accesibilidad de los audífonos han permitido que estas experiencias se integren fácilmente en la rutina diaria, desde pausas para el almuerzo hasta momentos de ocio.

En este panorama, la tecnología se erige como un facilitador que se adapta a nuestras preferencias individuales, transformando la forma en que interactuamos con la información y el entretenimiento en la era digital.

Imagínense un universo paralelo, un espacio digital donde la realidad se entrelaza con la imaginación, donde los límites físicos se desdibujan y las posibilidades son infinitas: ese es el metaverso. En este vasto reino digital, los usuarios pueden explorar mundos virtuales, interactuar con otros en tiempo real y crear experiencias únicas. Es como si cada persona tuviera su propia caverna prehistórica, pero en lugar de pinturas en las paredes, tienen la capacidad de construir y moldear todo un cosmos digital a su antojo. Al igual que los algoritmos que nos arrojan contenido personalizado, el metaverso promete una experiencia digital hiperpersonalizada, donde cada individuo puede crear su propia realidad a medida que navega por este vasto paisaje digital.

Imaginemos las granjas ancestrales, donde las cosechas eran el fruto del esfuerzo colectivo y la tierra se cultivaba con destreza. Hoy, en un giro digital, emergen las (granjas de contenido, creación producción y ventas) en el vasto paisaje de Asia, donde cientos millones de creadores se conectan a cámaras de video como si fueran surcos digitales. Una forma de nuevo empleo. Llegó para perpetuarse. Al igual que antaño, estas modernas granjas producen un valioso recurso: el contenido. Los cultivadores digitales, equipados con cámaras y conexiones globales, siembran ideas, cosechan interacciones y venden productos de manera simultánea, tejiendo una red que conecta audiencias de todo el mundo. Así como la antigua agricultura alimentaba comunidades, estas granjas digitales alimentan el apetito voraz de información y entretenimiento en la era contemporánea.

Epígrafe:

El Oráculo de la Inteligencia Artificial

çEn la encrucijada de la inteligencia y la tecnología, el oráculo de la inteligencia artificial nos insta a mirar más allá de la superficie de los algoritmos y a adentrarnos en las profundidades de un futuro que aún se revela. En esta era de incertidumbre digital, la sabiduría y la prudencia son nuestras guías." Dr. Samuel Cortés, Experto en Inteligencia Artificial.

El Hilo de las Grandes Ideas

En la danza intemporal de las grandes ideas, cada pensamiento es una nota que resuena en el vasto concierto del conocimiento humano. Con cada reflexión, hilamos el tapiz de la comprensión que une generaciones y define nuestro viaje en la búsqueda de la verdad. Prof. Elena Márquez,
Filósofa de la Historia.

Si algo No encontrarás en este libro es la palabra inclusivo

En el escenario de la tierra arrasada por la tecnología, la palabra "inclusivo" tan desgastada de truco retorico. se convierte en el comodín o un escudo semántico usado con maestría para disfrazar la falta de entendimiento real sobre la revolución digital y verse humanamente moderno y empático a todos los problemas que nos aquejan sin invertir nada. Solo un recurso económico barato de una

nota de prensa de un departamento de relaciones públicas de una empresa o institucionespúblicas.

Lao Tze, sabio ancestral, nos enseña que el elemento más poderoso es el agua. Cual va adaptándose a todas las formas que encuentra en su camino. En el escenario de la tecnología inteligencia artificial, esta lección se convierte en una metáfora para la adaptabilidad, un elemento esencial para navegar en el universo digital.

A. Ejemplo de delitos Ciber crimen.

¿Quieres robar un Tesla? Intente usar un
Flipper Zero

ALERTA DE PRIVACIDAD aseguradora mas gran de salud de EEUU: UnitedHealth y Change Healthcare bajo investigación por filtración masiva de datos

FBI: El cibercrimen aumentó un 22% en 2023, con pérdidas por 12.500 millones de dólares.

Tik tok.

Google odia el spam.

Problemas con las ASEGURADORAS Y LA INMOBILIARIAS que compran datos de terceros. Multadas.

Facebook victima de las estafas que asaltan a esta plataforma y las de meta(whatapp, instagram,etc,).

Ataque de inyección de datos

B. La creciente importancia de la ciberseguridad.

C. Las amenazas cibernéticas en el comercio electrónico

D. Evaluación de vulnerabilidad: identificación de debilidades en las plataformas de comercio electrónico.

E. Existen ocho tipos de software de seguridad para comercio electrónico que pueden utilizarse para mitigar las vulnerabilidades de forma eficaz. (otros que no los sabemos que manejan los gobiernos).

F. Normativa de Protección de Datos y Privacidad.

Para el cumplimiento del RGPD

Para el cumplimiento de CPRA

G. Futuro de la ciberseguridad del comercio electrónico

H. La ciberseguridad es crucial en la era digital. Algunos ejemplos de cambios organizacionales.

I.Fomentando una nueva era de adquisición de datos.

J. Innovación en Inteligencia Artificial y Machine Learning.

7. Gobiernos y Problemas de Ciberseguridad. pagina no.30

Principios de gobernanza de datos.

Observabilidad

Control

Escalabilidad

Principios de seguridad de datos

Asegure sus datos, asegure su futuro

8. Los Estados Compran Herramientas de Piratería en Ciberforos Clandestinos Rusos. pagina no.32 foros rusos.

Irán sospechoso de comprar software de limpieza.

Los foros RUSOS funcionan como un negocio.

Corredores de acceso inicial.

La disputa pública de LockBit expuesta en un ciberforo ruso.

9. Potencial para la Innovación Empresarial en Distintas Áreas. pagina no.38 Industria y Automatización:

Medicina.

Genética.

Ciencias.

Subsegmentos y Subramas.

10. El Crepúsculo de los Medios Tradicionales: Cómo la Inteligencia Artificial Redefinió el Panorama Informativo. pagina no.39

Quedarse atrás en la tecnología, periódicos, tv, radio

El Sueño de los Concesionarios del Periodismo

El Despertar de la Inteligencia Artificial

* Cibercrimen y la Era de la Ciberseguridad:*

2. Abordando el Desafío de los Delitos de Alta Tecnología

3.* La Técnica del Registro Remoto*: La Revolución del Ciberespacio y la Seguridad Global*

4. *Inspección y Registro Remoto Informático*

5.*Ejecución y Levantamiento de Evidencias en los Registros Remotos y Derechos Protegidos*

6.*Laboratorio Forense*

7. Procesamiento de evidencia digital

8.Cadena de custodia

Herramientas forenses Evidencias

digitales en las nubes

análisis, informe pericial y presentación forense digital.

El peritaje informático forense

La metodología del dictamen e informe pericial En

resumen de estos informes:

Fundamentos legales *Legislaciones* *Legislación española

Derechos fundamentales involucrados

Derechos fundamentales involucrados

*Control, duración, secreto y derechos involucrados

Descubrimiento de delito casual o hallazgo inevitable y cese de medida

Deber de colaboración y ampliación del registro

La ley 53-07 sobre crímenes y delitos de alta tecnología

En resumen de la legislación dominicana

La interceptación de comunicaciones

Enfoque también sería aplicable a la figura del registro remoto informático

CONCLUSIONES Y LIMITACIONES *

En este contexto, hemos evaluado una herramienta crucial: el registro remoto informático.

implementación del registro remoto informático en la legislación dominicana.

*LIMITACIONES

RECOMENDACIONES*

15. Etica y Ciberseguridad en la inteligencia artificial, garantizando que la tecnología se utilice de manera ética para el beneficio de la sociedad.

Amenazas cibernéticas en Seguridad de la Inteligencia Artificial:

Falta de Ética y ciberseguridad en la IA:

1. Automatización y Nuevas Oportunidades:
2. Colaboración HombreMáquina
3. Nuevos Campos de Empleo
    - 3.1. Adaptación de Habilidades
    - 3.2. Transformación de Industrias

Pérdida de Control:

Inteligencia Desbordante

Seguridad:

Temor a Amenazas Cibernéticas:

1. Introducción

El Diálogo Intemporal de las Ideas piloteando las Mareas de la Evolución Tecnológica.En el vasto océano de la evolución tecnológica, Michel Foucault se presenta como un capitán audaz, explorando las mareas que han llevado a la tecnología a ser tanto una llave de liberación como unintrincado mecanismo de control. No necesitamos retroceder en el tiempo, ya que su perspectiva nosinvita a contemplar el horizonte de relaciones complejas que la tecnología ha tejido a lo largo del tiempo.

Foucault nos sumerge en un análisis profundo de cómo la tecnología, desde sus formas más primitivas hasta las más avanzadas, ha sido un catalizador de cambios sociales. No estamos atados a las pinturasrupestres, sino que exploramos cómo cada avance tecnológico ha sido una corriente en el vasto océano,una que define nuestra relación con el poder y la liberación.

Desde las ruedas y palancas de la antigüedad hasta la inteligencia artificial contemporánea, Foucault nosanima a considerar la tecnología como una marea que, si bien ha desatado las ataduras de la limitaciónhumana, también ha inundado las costas de la sociedad con complejas redes de control. Las innovacionestecnológicas, lejos de ser simples herramientas, han sido arquitectos de nuevas formas de poder yestructuras sociales.

En esta travesía, Foucault nos invita a explorar la relación entre tecnología y poder en un vasto océano.Cada invención, desde la imprenta que imprimía ideas en la historia hasta la era digital, se convierte enuna ola que desencadena nuevas posibilidades y, simultáneamente, en una corriente que moldea y dirigela sociedad.

Así, iniciamos nuestra odisea tanto como en cavernas, en esta vez a bordo de un barco de conocimiento, guiados por la mirada penetrante de un pensador que nos impulsa a desentrañar las complejidades de latecnología como fuerza liberadora y mecanismo de control en la historia de la humanidad. Cada página, como una vela al viento, nos impulsa hacia adelante, explorando las mareas cambiantes de la relaciónentre el ser humano y su creación tecnológica.Fuera de la aguda perspicacia de Michel Foucault se entrelaza con la contribución única de Malcolm Gladwell, un sociólogo contemporáneo que destaca por su habilidad para iluminar la intersección compleja entre la sociedad y la tecnología. Gladwell, como un arqueólogo de las dinámicas sociales, nos habla más allá de la innovación, revelando cómo cada patrón y cada narrativa tecnológica es, en última instancia, un reflejo de nuestras interacciones sociales y estructuras culturales. Gladwell nos ofrece una perspectiva sociológica de cómo la tecnología ha influido en nuestra comunicación, interacción y estructuras de poder. Su contribución destaca que la

adopción y evolución dela tecnología no solo son fenómenos técnicos, sino procesos arraigados en las complejidades de nuestras interacciones sociales. Con su destreza narrativa, Gladwell nos muestra cómo la tecnología no es simplemente un conjunto de herramientas aisladas, sino una fuerza que influye y es influenciada por las complejidades de la vida en sociedad. Gladwell nos invita a cuestionar las ideas convencionales sobre el éxito, el talento y la inteligencia, y a explorar los factores ocultos que determinan nuestro destino. Con su estilo ameno y provocador, Gladwell nos hace reflexionar sobre cómo las pequeñas cosas pueden tener grandes consecuencias, cómo el pensamiento intuitivo puede ser más poderoso que el racional, y cómo los individuos pueden desafiar las estructuras dominantes. Con sus ejemplos y anécdotas, Gladwell nos acerca a las historias de personas extraordinarias que han cambiado el mundo con su ingenio, su pasión y su perseverancia.

El papel de nuevos jugadores como la India es clave en la configuración de las reglas de la IA, ya que es un mercado productor:

India se encuentra entre los mayores productores de datos del mundo y desempeñará un papel clave en la gobernanza y regulación de la Inteligencia Artificial (IA) a medida que la tercera economía más grande de Asia pase de un mercado de consumidores a un mercado de productores

Debido a que India es el país más grande del mundo (en términos de población), generará una demanda que generará crecimiento y también producirá una gran cantidad de datos Recordar que tiene el 2do centro de matematticas mas prestigioso del mundo depues de MIT. Además inventaron el cero. Un meditador. ..

En segundo lugar, India prestará servicios a los mercados globales y eso significa que hay una mayor alineación en la discusión (gobernanza e IA responsable) que está sucediendo en todo el mundo

las empresas tendrán que distinguir entre la escala y la exageración mientras operan en el mundo real, donde los riesgos tecnológicos se han vuelto más evidentes.

En India, el gobierno pretende impulsar la gobernanza en tecnología mediante la implementación de la Ley de India Digital y el Proyecto de Ley de Protección de Datos Personales Digitales (DPDP) de 2023, que equivale al Reglamento General ..

En este libro, propongo un diálogo intemporal de las ideas, en el que la tecnología es el hilo conductorque une el pasado, el presente y el futuro. Nos muestran cómo la tecnología es una expresión de nuestracultura, de nuestra política y de nuestra identidad, y cómo podemos usarla para transformar nuestrarealidad. Nos invitan a ser navegantes

curiosos y críticos, capaces de pilotear las mareas de la evolucióntecnológica con conciencia y responsabilidad.

2. Inteligencia Artificial: Pasado y su Hermano Mayor **Si bien estamos asustados con la inteligencia artificial.(IA).**

Cuando llegue la evolución de esta la AGI. No sé qué decirles.

La evolución de la inteligencia artificial que conocemos hoy día, AGI (Inteligencia Artificial General), podría llegar tan pronto como 2029, según Ben Goertzel, quien popularizó el término. Fundador de SingularityNET, una iniciativa para crear una "Inteligencia Artificial General descentralizada, democrática, inclusiva y beneficiosa", compartió sus ideas en la Beneficial AGI Summit 2024.

Goertzel sugiere que estamos experimentando un crecimiento exponencial en lugar de lineal, lo que dificulta comprender la rapidez del cambio. Prevé que en la próxima década, una computadora individual podría tener la potencia de cálculo de un cerebro humano para 2029 o 2030, y en las siguientes décadas, equivaldría al poder de toda la sociedad humana.

Aunque modelos de lenguaje grandes (LLMs) como ChatGPT han despertado el interés en la IA, Goertzel no ve a los LLMs como el camino hacia la AGI, ya que

no demuestran una comprensión genuina del mundo, operando más como un autocompletado avanzado.

Sin embargo, Goertzel cree que los LLMs podrían ser parte de la AGI, especialmente en su propio OpenCog Hyperon. Este sistema, según él, podría aprender a diseñar y escribir código de software, potencialmente llevándonos a una explosión de inteligencia y una Singularidad Tecnológica.

Aunque emocionante, Goertzel también expresa preocupaciones. Advierte sobre la necesidad de salvaguardias antes de abrir la caja de Pandora, ya que aún no hemos comprendido completamente. Si la singularidad está tan cerca como sugiere, hay una gran presión para hacer las cosas bien y rápido.

"Una vez que lleguemos a la AGI a nivel humano, en pocos años podríamos estar en una AGI radicalmente superhumana", añadió Goertzel. "Creo que una vez que una AGI pueda introspectar su propia mente, podrá hacer ingeniería y ciencia a nivel humano o superhumano, generando una explosión de inteligencia que puede superar incluso lo que pensaba [el científico informático Ray Kurzweil."

3. Tus Datos Personales en Toda la Web: ¿Existe una Forma Mejor?

Sir Tim Berners-Lee dice que las personas deberían recuperar el control de sus datos personales, fundador del internet y el que lo dono: dice que un problema particular es la forma en que se manejan los datos personales. Cuando inicia sesión y almacena datos en un sitio web, solo se pueden utilizar dentro de ese sitio web. Pero un proyecto de software de código abierto, llamado Solid, está diseñado para revertir esa situación. un proyecto de software de código abierto (gratis), llamado Solid, está diseñado para revertir esa situación.

La idea de Solid es que las personas tengan un almacén de datos privado y puedan elegir qué organizaciones pueden acceder a él, con qué propósito y durante cuánto tiempo.

Llamado Almacén de datos personales en línea, o Pod, brinda a los usuarios control sobre sus datos y la libertad de combinarlos o compartirlos entre aplicaciones.

Sir Tim es cofundador de Inrupt, una empresa que ofrece tecnologías basadas en sólidos. Dice que usar la tecnología significaría que el almacenamiento de datos estaría "centrado en las personas, en lugar de en las aplicaciones".

Otras empresas que ofrecen soluciones basadas en sólidos incluyen Graphmetrix y Digita.

La idea de Solid es que las personas tengan un almacén de datos privado y puedan elegir qué organizaciones pueden acceder a él, con qué propósito y durante cuánto tiempo.

Llamado Almacén de datos personales en línea, o Pod, brinda a los usuarios control sobre sus datos y la libertad de combinarlos o compartirlos entre aplicaciones.

La tecnología también se está probando en el sector sanitario.

A partir de este año, cinco hospitales belgas almacenarán información sobre las visitas al hospital en los Solid pods de los pacientes. La idea es que facilitará a los pacientes compartir sus datos médicos. Por ejemplo, podrían compartir prueba de un examen médico reciente al solicitar un trabajo, por lo que no necesitan tener otro.

Los pods almacenan datos en formatos estándar, de modo que puedan reutilizarse en múltiples contextos. "Lo que yo llamo la verdadera diversión de la economía de datos es cuando seremos capaces de combinar estos diferentes elementos de datos", afirma De Vidts. "Eso generará casos de uso que ni siquiera podemos predecir hoy. Cuando tenga suficientes puntos de datos interesantes, creemos que los creadores de aplicaciones llegarán al pod para crear nuevas

aplicaciones

Los pods podrían potencialmente hacer la vida más difícil a los piratas informáticos.

Aunque los pods pueden compartir un servidor, cada uno tiene sus propios controles de acceso, establecidos por el usuario. Por el contrario, la base de datos de una empresa tiene un conjunto de controles de acceso que otorga acceso a todos los registros de los clientes. "Hoy existes en grandes bases de datos", dice Bruce. "Su tarjeta de crédito está ahí con otras 10 millones.

"Esa base de datos es un objetivo de alto valor. [Los piratas informáticos] dedicarán meses de trabajo para obtener esa base de datos. Cuando el valor de los datos existe sólo en su módulo, es como la diferencia en el tipo de ataque que uno recibiría contra un banco versus "Te asaltan en la calle. No vas a tener un equipo de personas siguiéndote durante tres meses para robarte la billetera", dice.

Amanda Finch, directora ejecutiva del Chartered Institute of Information Security, dice que el plan de Athumi para crear una plataforma de datos centralizada tendrá beneficios.

Además de facilitar el flujo de datos a través de la economía, podría aumentar la seguridad.

"Desde el punto de vista de la seguridad, debería ayudar a crear un entorno más seguro. Con menos plataformas que proteger y la responsabilidad recae en una sola parte, se esperaría menos vulnerabilidades en comparación con múltiples soluciones diferentes".

4. Mitos y Leyendas de la IA: Desmitificando la Inteligencia Artificial y el Código Binario

Desmitificando la Inteligencia Artificial (IA) y tecnologia (no todo es malo):

A-Tapones:

Impulsar la IA . en el desarrollo de software de semáforos sincornizados. Analizando la memoria del trafico vehicular. Trae soluciones. (Recordar que el tránsito vehicular se maneja con memoria).

Impulsar el teletrabajo puede ser una vía positiva para aliviar el congestionamiento en Santo Domingo y Santiago. La tecnología facilita la conectividad remota, reduciendo la necesidad de desplazamientos diarios y contribuyendo a descongestionar las ciudades. Trae consigo menos estrés ser más ecológico menos consumo de combustible y más eficiencia del empleado que pierde horas en los tapones.

B. El internet de las cosas:

Vamos a confiar nuestros hogares y electrodomésticos nuestros autos, nuestra salud (cual cada de esos miles cientos de miles de equipos que hoy irrumpen uevamente en nuestras vidas pero con luz propia. Estos uno necesitara un antiviral y una actualización), nos haremos mas esclavos del consuimismo y más de empresas tecnológicas privadas, en una escala nunca inimaginada, necesitamos estándares de seguridad y privacidad mucho, mucho más fuertes de lo que existen ahora. es hora de dejar de bailar sobre los problemas de privacidad y seguridad y aprobar leyes reales y vinculantes.

La implementación de estándares más robustos y leyes vinculantes es esencial para proteger nuestros datos y garantizar un uso ético de la tecnología. La discusión activa y la acción legislativa son pasos cruciales para abordar estas preocupaciones y mejorar la seguridad en el ámbito tecnológico.

C. Reemplazo de Empleos:

Unos se van otros entran!

Aclarar que, aunque algunos empleos pueden cambiar, la IA también crea nuevas oportunidades laborales. Abordando la Preocupación sobre la Falta de Empleo debido a la Inteligencia Artificiales comprensible; pero la historia no ensena. A lo largo de la historia, la tecnología ha desencadenado una metamorfosis constante en los roles laborales, y la llegada de la inteligencia artificial (IA) no es una excepción. Desde las primeras civilizaciones hasta la actualidad, la adaptación a los avances tecnológicos ha llevado a la creación y redefinición de roles profesionales.

La revolución tecnológica ha transformado las operaciones bancarias, impulsada por soluciones digitales como inteligencia artificial, análisis de datos y blockchain. Santander, reconocido como el banco más innovador del mundo, ha liderado esta transformación. Para atraer talento digital, lanzaron "Be Tech! with Santander", incorporando más de 4,500 empleados con perfiles digitales en 2023. La iniciativa busca profesionales en áreas como la nube, ciberseguridad, inteligencia artificial y desarrollo de software. Con 400 vacantes disponibles, Santander se destaca como un empleador innovador que impulsa la transformación digital y mejora la experiencia del cliente.

En las sociedades antiguas, la introducción de técnicas agrícolas avanzadas generó roles

especializados en la gestión de la tierra y la producción alimentaria. La construcción de monumentos emblemáticos no solo evidenció habilidades técnicas, sino también la emergencia de roles especializados en planificación y ejecución de proyectos arquitectónicos.

Con la invención de la escritura, surgieron roles dedicados a la documentación y comunicación escrita. Durante la Revolución Industrial, la maquinaria transformó la producción, creando roles en la operación y mantenimiento de máquinas.

En el siglo XX, la electricidad, el teléfono y la aviación generaron nuevos roles en estas industrias emergentes. Actualmente, la inteligencia artificial está remodelando los roles al automatizar tareas repetitivas y liberar tiempo para funciones más estratégicas y creativas.

Aunque la inquietud persiste sobre la posible pérdida de empleos, la historia revela que cada cambio tecnológico ha dado lugar a nuevas oportunidades y roles especializados. La inteligencia artificial, lejos de ser una amenaza, está conduciendo a una transformación significativa, donde la adaptabilidad y la adquisición de

habilidades novedosas se vuelven cruciales para capitalizar las oportunidades emergentes en el panorama laboral.

'El Gran Gatsby' (F. Scott Fitzgerald):

Al igual que Gatsby persigue un amor enigmático, imposible y efímero, la inteligencia artificial busca conquistar nuevos horizontes en la tierra arrasada por la tecnología. La obsesión y la transformación definen la narrativa, culminando en la contundente realidad de que en este escenario digital, el que te quiere te lleva a una nueva era, aunque a veces ese viaje sea desafiante y misterioso.

D. Profesiones que se resisten y otras avanzan: (no todo es rosa)

En el Escenario de la Inteligencia Artificial: Acto I.La Abogacía Revisitada

En el reino de la abogacía, donde las palabras son espadas y los argumentos son escudos, se despliega una comedia de resistencia ante la llegada de la inteligencia artificial. Los letrados, cual actores de una obra teatral, se aferran a la tradición de las audiencias presenciales, donde el arte de persuadir

se mezcla con la teatralidad. Al parecer, el drama judicial les resulta más cautivador cuando se representa en vivo, aunque la audiencia sea solo una pequeña fracción de la capacidad digital existente.

La transparencia, ese artefacto desconocido para muchos abogados, se presenta como un espectro que asusta a los defensores del antiguo orden. La idea de que cada palabra, cada movimiento, quede registrado y disponible para su escrutinio es un temor que parece estar más allá de su capacidad de comprensión. ¿Prefieren acaso las sombras del antiguo proceder, donde los escritos se multiplican en una danza eterna de papeles y la verdad se esconde entre carpetas polvorientas? La comedia legal se torna tragicómica cuando la resistencia a la transparencia se convierte en el protagonista de este acto.

Pero no todo es tragedia. En el escenario judicial, la inteligencia artificial espera ansiosa su turno. Imagina un tribunal donde el juez es asistido por algoritmos, donde la justicia se sirve con la eficiencia de un código bien diseñado. ¿Se atreverán los letrados a enfrentarse a un sistema que no solo conoce cada ley, sino que puede anticiparse a los movimientos de cada jugador en este tablero legal?

La comedia da un giro irónico cuando la resistencia se enfrenta al futuro inevitable de la abogacía.

En este acto inicial, la abogacía se erige como el escenario donde la comedia de la resistencia ante la inteligencia artificial se despliega en su máxima expresión. ¿Lograrán los letrados adaptarse a un nuevo guion, o permanecerán aferrados a los viejos rollos de papel que los atan a un pasado que la tecnología amenaza con arrasar? El telón se alza, y la inteligencia artificial espera su turno para ser la protagonista de esta obra en constante evolución.

En la escena final de este acto, la pregunta resuena: ¿Se pierde calidad en la aplicación de la justicia cuando los letrados resisten la transición a un sistema más transparente y eficiente, donde la tecnología permite una administración más precisa del tiempo y los recursos? El drama judicial, marcado por tiempos efímeros y documentos que se acumulan como polvo en el escenario, plantea el dilema entre la resistencia a lo nuevo y la adaptación necesaria para alcanzar la excelencia en el servicio de la justicia.

Profesiones en el Escenario Irónico de la Inteligencia Artificial: Acto II Medicina y Su Resistencia

En el reino de la medicina, donde los batas blancas y los fonendoscopios son tan icónicos como los parlamentos en una obra clásica, se libra un conflicto entre la tradición y la modernidad. Los doctores, manteniendo sus rituales sagrados de escuchar el latir del corazón con el estetoscopio, se resisten a ceder el escenario a la inteligencia artificial.

En este acto médico, los médicos actúan como si la máquina de resonancia magnética fuera una bruja del futuro, capaz de revelar secretos que prefieren mantener ocultos. Las computadoras diagnósticas y los algoritmos se asoman tímidamente, esperando que los médicos, cual protagonistas renuentes, reconozcan su papel como aliados en la búsqueda de tratamientos más eficaces.

Pero la ironía no se detiene. En el escenario digital, la inteligencia artificial aguarda pacientemente su turno, lista para brindar diagnósticos más precisos y personalizados. La resistencia médica, envuelta en batas blancas y rodeada de instrumental tradicional, desafía al futuro, pero ¿serán capaces de resistir el encanto de una medicina más avanzada?

En la escena final, la pregunta resuena: ¿Se perderá la oportunidad de mejorar la calidad de la atención médica cuando la resistencia a la inteligencia artificial obstaculiza la adopción de tecnologías que pueden salvar vidas y optimizar el sistema de salud? El drama médico, mezcla de risas y reflexión, invita a los médicos a bailar al compás de la tecnología para un espectáculo de sanación sin precedentes.

Profesiones en el Escenario Irónico de la Inteligencia Artificial: Acto III Ingeniería y la Resistencia Tecnológica

En el reino de la ingeniería, donde las mentes brillantes trazan líneas y esquemas, surge un conflicto digno de un drama cómico. Los ingenieros, custodios de planos y cálculos precisos, se aferran a lápices y reglas como si fueran varitas mágicas. La resistencia tecnológica, un desfile de ingenieros con sus croquis en mano, desafía al futuro, negándose a dejar atrás las herramientas tradicionales.

En este acto tecnológico, los ingenieros actúan como si el software de modelado 3D fuera un artefacto alienígena, amenazando con revelar los misterios del diseño arquitectónico. Las computadoras y los algoritmos observan desde las bambalinas,

esperando que los ingenieros, cual protagonistas reticentes, descubran que la tecnología puede potenciar su creatividad y eficiencia. Pero la ironía no se detiene. En el escenario digital, la inteligencia artificial aguarda pacientemente su turno, lista para optimizar procesos y amplificar la creatividad. ¿Serán capaces los ingenieros de desprenderse de los lápices y abrazar el potencial de la tecnología para construir un mañana más innovador?

En la escena final, la pregunta resuena: ¿Se perderá la oportunidad de mejorar la ingeniería cuando la resistencia a la inteligencia artificial obstaculiza la adopción de tecnologías que pueden acelerar proyectos y abrir nuevos horizontes de creatividad? El drama tecnológico, marcado por risas y reflexiones, desafía a los ingenieros a desplegar un escenario donde la tecnología y la creatividad bailen juntas en una armonía vanguardista.

E. Transformación de Roles, Nuevas Oportunidades Laborales:

En lugar de eliminar empleos, se tiende a transformar roles, automatizando tareas repetitivas y permitiendo que los trabajadores se centren en actividades más estratégicas y creativas.

'Al Filo de la Navaja' (W. Somerset Maugham):

La dualidad entre lo que se deja y se gana, presente en la metáfora del filo de navaja, se refleja en la relación entre la tecnología y la inteligencia artificial. La innovación corta con el pasado, planteando nuevos retos y cuestionamientos. Así, la conclusión es que en esta era de progreso, el futuro es tan afilado como el filo de la navaja, exigiendo a la humanidad enfrentar la realidad con agudeza.

La implementación de la inteligencia artificial da lugar a la creación de nuevos empleos relacionados con su desarrollo, mantenimiento y supervisión. Profesiones emergentes, como especialistas en ética de la IA, que son ejemplos de este cambio.En el siglo XXI, las nuevas oportunidades profesionales se han generado gracias a los avances tecnológicos, la globalización y la evolución de la economía.

La tecnología ha traído avances notables en áreas genéticas, robótica, medicina, industria y confort. A través de pantallas, explorar nuevas ideas se ha vuelto más accesible. Sin embargo, también ha dejado una nueva tierra arrasada, obligándonos a sembrar y cultivar valores con una tecnología ya existente que se nos presenta sin introducción y es irreversible. Estas áreas representan solo una fracción de las oportunidades emergentes en el siglo XXI, donde la adaptabilidad y la adquisición continua

de habilidades son esenciales para prosperar en un entorno laboral en constante cambio.

Salud Digital y Telemedicina:

La convergencia de la tecnología y la salud ha impulsado la expansión de la salud digital y la telemedicina. Profesionales en desarrollo de aplicaciones de salud, análisis de datos médicos y gestión de sistemas de información de salud están experimentando una creciente demanda.

Marketing Digital y Comercio Electrónico:

El auge del comercio electrónico ha creado oportunidades en marketing digital, gestión de redes sociales y análisis de datos para comprender el comportamiento del consumidor en línea. Expertos en SEO, SEM y comercio electrónico son esenciales para el éxito de las empresas en este entorno digital.

Educación en Línea y Formación Digital:

La educación en línea y la formación digital han ganado relevancia, generando oportunidades en el diseño de cursos en línea, desarrollo de contenido educativo digital y roles relacionados con la tecnología educativa.

Tecnología de la Información (TI) y Desarrollo de Software:

La demanda de profesionales en TI ha alcanzado niveles sin precedentes. Roles como desarrolladores de software, ingenieros de datos y expertos en ciberseguridad están en alta demanda debido a la rápida digitalización de las empresas y la expansión de la inteligencia artificial.

Sostenibilidad y Energías Renovables:

Con un enfoque creciente en la sostenibilidad ambiental, las oportunidades laborales en energías renovables, gestión de residuos y eficiencia energética están en aumento. Carreras en ingeniería ambiental, diseño sostenible y consultoría en energías limpias son áreas prometedoras.

La inteligencia artificial tiene su lado oscuro, pero también aporta positivamente, especialmente en la necesidad de abordar problemas ambientales, como los coches eléctricos, que a pesar de ser tecnológicamente avanzados, generan contaminación significativa. (mucho mercadeo: (Caucho degaste, Baterías, etc.)

F. Los nuevos dueños del Mundo: Aunque recordemos que Google entró en bolsa en 2004,

otras tecnologías aún no celebran sus bodas de plata en el matrimonio con la humanidad. Son jóvenes caprichosas, provenientes de distintas partes, que han desarrollado plataformas y tecnología, desarrolladas por gobiernos USA y compartida incluso con organismos de seguridad de estos, otorgándoles un poder inmenso e inconmensurable. Siempre presumo que es vigilado. No es estético comparar a un maganate triunfante joven millonario con una chancla y dedos grandes de cual soy muy escéptico. Siempre pienso que los oraganismo de seguridad rectores del imperio lo regulan. Bien por elon Musk no solo se estuvo quieto con la mina de esmeralda de sus padres en África. Sino que a si mismo propulso su talento. Sin embargo, estas son relieves de la compleja cordillera donde se posan esos magnates de los medios sociales y tecnológicos. Como Apple no deja que pases tu whatapp completo a android, si te decides dar de baja de un equipo iphone. Pero si puedes migrar libremente de android a iphone. Pero nunca viceversa.

En fin. Desde distintos ángulos, analizamos la tecnología, desde el más rico del mundo que hoy en día ya no lo es, hasta un joven tranquilo que se desarrolló en las minas de esmeralda en África. Su intelecto natural es innegable, pero su última compra de twitter que parece descolocada en comparación con sus negocios anteriores, quizás

una metáfora de cómo la tecnología afecta hasta a los más astutos.

La noción de que jóvenes millonarios puedan controlar un país sin la supervisión de los organismos de seguridad es simplista y alejada de la realidad. Es esencial separar las historias fantasiosas de la acción pragmática, garantizando que las grandes potencias y organizaciones estén sujetas a una intervención adecuada para preservar la seguridad y la integridad. A pesar de la retórica educativa, es necesario ir más allá de las palabras vacías y los modismos que a menudo se disfrazan de soluciones. La ciberseguridad demanda acciones concretas y efectivas, y la intervención directa de los organismos de seguridad del estado se torna esencial en un panorama donde la interconexión puede ser tanto una bendición como una maldición.

Los coches autónomos y la entrega de alimentos autónoma son realidades imparables. Sin embargo, junto con la tecnología, la inteligencia artificial es una colaboradora que, como Atila, fue un hombre guerrero. La regulación y el control son imperativos para mantener el equilibrio.

G. Pensador de la India y su preocupación

Uno de los pensadores hindues más influyentes es Nandan Nilekani, cofundador de Infosys y ex presidente de la Autoridad de Identificación Única de la India (UIDAI). conocido por su papel fundamental en la transformación digital en la India, ha abogado por la aplicación pragmática de la tecnología para abordar desafíos fundamentales en el país. Su énfasis en la identificación digital se evidencia a través de su liderazgo en la implementación del proyecto Aadhaar, la mayor base de datos biométrica y de identidad única del mundo.

En cuanto a la ciberseguridad, Nilekani ha abordado la necesidad de salvaguardar la privacidad y la integridad de la información en un mundo cada vez más digitalizado. Su enfoque se inclina hacia la implementación de medidas robustas de seguridad para proteger la información personal y la infraestructura crítica.

5. Pequeños y Medianos Emprendedores Comerciantes:

Los pequeños y medianos fabricantes son la columna vertebral de las economías locales. Sin embargo, a pesar de esta masa crítica, enfrentan muchos desafíos continuos. Estos incluyen dificultades para encontrar trabajadores calificados, márgenes de beneficio reducidos, falta de experiencia en automatización e incapacidad para escalar de manera eficiente. Muchas micrro y medianas empresas todavía dependen de procesos manuales que consumen mucho tiempo y son propensos a errores y que limitan su competitividad y potencial de crecimiento.

La automatización se erige como una solución fundamental para ayudar a las pequeñas y medianas empresas a superar estos desafíos, llenando vacíos donde es difícil encontrar mano de obra y aumentando la productividad y la eficiencia para reforzar la competitividad y la retención de clientes.

Históricamente, las micro y medianas han luchado por implementar tecnologías modernas que puedan transformar sus operaciones. Hasta hace poco, los altos costos y la compleja infraestructura hacían que las soluciones de automatización tradicionales estuvieran fuera del alcance de estas empresas.

Pero una nueva ola de soluciones está cambiando las reglas del juego, haciendo que la automatización sea accesible y brindando retorno de la inversión a las SMM. Estos sistemas innovadores están diseñados en función de las necesidades y limitaciones únicas. La automatización se configura a través de interfaces modulares de arrastrar y soltar que permiten una configuración rápida con programación sin código. Esto permite a los fabricantes poner en funcionamiento sistemas automatizados en cuestión de días o semanas, en lugar de meses o años.

Estas tecnologías han hecho que la automatización sea práctica y accesible. Proporcionando los beneficios de la automatización junto con la agilidad que requieren estos fabricantes más pequeños. Esto permite que incluso las empresas con experiencia técnica e infraestructura mínimas logren mejoras transformadoras en capacidad, calidad, costos y servicio al cliente.

Por ejemplo, una empresa de bienes de consumo envasados con la que hemos trabajado añadió dos

robots colaborativos (cobots) a su línea de envasado de productos para poder reasignar ocho trabajadores a tareas de mayor valor. En consecuencia, la empresa logró un aumento del 50 % en la producción por turno: los cobots pudieron cargar 1200 cajas en comparación con las 800 que antes llenaban trabajadores humanos por turno. Además, los cobots también proporcionaron una calidad más consistente que los trabajadores humanos. Estas mejoras en el proceso se amortizaron en 12 meses.

A.Claves para el éxito

El éxito de la iniciativa de automatización depende de la selección de una solución adaptada a sus requisitos y limitaciones únicos, que abarque consideraciones físicas, financieras y operativas. Los grandes sistemas de nivel empresarial utilizados por los conglomerados globales no tienen sentido. En cambio, un SMM debería buscar opciones con características como:

- Sistemas modulares que se pueden implementar de forma incremental.
- Interfaces fáciles de usar para una rápida adopción.
- Soluciones escalables que crecen con las necesidades.

- Arquitecturas abiertas que se integran con la tecnología existente.

- Máquinas y productos flexibles que se pueden reutilizar y reutilizar según sea necesario.

- Modelos de precios asequibles.

El resultado es una automatización que proporciona un retorno de la inversión real sin altos riesgos ni implementaciones disruptivas.

B. El retorno de la inversión de la automatización

La automatización de las operaciones puede proporcionar importantes beneficios en áreas que incluyen:

- **Capacidad de producción:** la automatización de tareas repetitivas o peligrosas ayuda a aumentar el rendimiento sin agregar mano de obra. También permite a las SMM satisfacer mejor la demanda de los clientes.

- **Calidad:** La inspección y el monitoreo automatizados pueden mejorar las tasas de detección de defectos, reduciendo el desperdicio y el retrabajo. Esto también mejora la coherencia y el cumplimiento.

- **Costos:** con procesos automatizados, las SMM pueden ahorrar gastos mediante la reducción

de desechos, tiempo de inactividad, mano de obra y mantenimiento.

- **Seguridad:** han demostrado que la automatización de tareas peligrosas elimina los riesgos y lesiones asociados. Esto mejora el ambiente de trabajo y reduce las reclamaciones de compensación laboral.

- **Satisfacción del cliente:** calidad y coherencia permiten ofrecer un servicio y valor superiores a sus clientes.

C.La automatización y la brecha de habilidades

Al manejar tareas repetitivas y de bajo valor, la automatización permite aprovechar mejor la experiencia de sus trabajadores calificados. Al liberarse a los trabajadores de completar esas tareas, ahora pueden concentrarse en actividades complejas que requieren experiencia y pensamiento crítico humano. Esto permite a hacer más con menos y, al mismo tiempo, mantener el talento valioso comprometido y empoderado.

Además, los procesos automatizados contribuyen a crear entornos de trabajo más seguros y sostenibles. La reducción de las lesiones laborales mejora la satisfacción laboral y la retención de los trabajadores. Además, dado que las nuevas generaciones de trabajadores buscan carreras alineadas con sus valores, la automatización

contribuye a la sostenibilidad y la responsabilidad social que pueden ayudar a atraer y retener talentos jóvenes.

La combinación de reorientar el talento hacia un trabajo satisfactorio y mejorar el entorno laboral supone un poderoso doble golpe. La automatización maximiza la productividad del personal existente y al mismo tiempo amplía el grupo de talento potencial.

¿El resultado? La automatización permite utilizar su fuerza laboral calificada de manera más efectiva y, al mismo tiempo, hacer de su empresa un lugar cada vez más atractivo para desarrollar una carrera.

Para los pequeños y medianos fabricantes que enfrentan escasez de talento, la automatización representa una oportunidad estratégica. Al aprovechar las últimas tecnologías de automatización adaptadas a sus necesidades

Los datos muestran que la automatización incluso de pequeñas porciones de procesos puede generar ganancias mensurables para estos ágiles fabricantes.

6. Ciberseguridad:

Ciberseguridad en el comercio electrónico: análisis y fortalecimiento de las empresas digitales

Como sabrá, la mala ciberseguridad es una de las principales causas de pérdidas y reducción de la confianza de los consumidores en el sector del comercio electrónico. Al mismo tiempo, seguir una serie de reglas y recomendaciones al desarrollar soluciones de comercio electrónico, así como verificarlas periódicamente en busca de vulnerabilidades, puede ayudar a solucionar estos problemas.

NADIE ESTA VACUNADO CONTRA EL CIBERATAQUE

A. Ejemplo de delitos Ciber crimen.

¿Quieres robar un Tesla? Intente usar un Flipper Zero

Los investigadores de seguridad informan que descubrieron una falla de diseño que les permitió secuestrar un Tesla usando un Flipper Zero, una controvertida herramienta de piratería de 169 dólares . Los socios Tommy Mysk y Talal Haj Bakry de Mysk Inc. dijeron que el ataque es tan simple como deslizar la información de inicio de sesión del propietario de un Tesla, abrir la aplicación Tesla y alejarse. La víctima no tendría idea de que perdió su vehículo de 40.000 dólares. Mysk dijo que el exploit lleva unos minutos y, para demostrar que todo funciona, robó su propio coche.

El problema no es el “hacking” en el sentido de irrumpir en el software, sino un ataque de ingeniería social que

engaña al usuario para que entregue su información. Utilizando un Flipper, los investigadores configuraron una red WiFi llamada "Tesla Guest", el nombre que Tesla utiliza para sus redes de invitados en los centros de servicio. Luego, Mysk creó un sitio web que se parece a la página de inicio de sesión de Tesla.

El proceso es sencillo. En este escenario, los piratas informáticos podrían transmitir la red cerca de una estación de carga, donde un conductor aburrido podría estar buscando entretenimiento. La víctima se conecta a la red WiFi e introduce su nombre de usuario y contraseña en la web falsa de Tesla. Luego, el pirata informático utiliza las credenciales para iniciar sesión en la aplicación Tesla real, lo que activa un código de autenticación de dos factores. La víctima ingresa ese código en el sitio web falso y el ladrón obtiene acceso a su cuenta. Una vez que haya iniciado sesión en la aplicación Tesla, puede configurar una "tecla de teléfono" que le permite desbloquear y controlar el automóvil a través de Bluetooth con un teléfono inteligente. A partir de ahí, el coche es tuyo.

ALERTA DE PRIVACIDAD aseguradora mas gran de salud de EEUU: UnitedHealth y Change Healthcare bajo investigación por filtración masiva de datos

Blackcat es una notoria banda cibernética que explota las vulnerabilidades de seguridad en lossistemas informáticos de las empresas de atención médica. Tras la infracción, UnitedHealth supuestamente pagó un rescate

de 22 millones de dólares en criptomonedas a los piratas informáticos.

Blackcat afirmó haber confiscado seis terabytes de datos sensibles y altamente confidenciales, lo que provocó cortes en la red de atención médica en todo el país que afectaron a millones de pacientes, médicos y hospitales. Los datos robados pueden incluir registros médicos, información de pagos, reclamos e información de seguros, y otros registros personales, incluida información de contacto y números de Seguro Social.

Como UnitedHealth es la aseguradora de salud más grande de los Estados Unidos, la infracción ha sido especialmente perjudicial para toda la industria de la salud. UnitedHealth ha desconectado muchos sistemas críticos, incluidos los sistemas para procesar reclamaciones de medicamentos recetados, lo que ha provocado que los pacientes no puedan surtir sus medicamentos sin pagar de su bolsillo.

FBI: El cibercrimen aumentó un 22% en 2023, con pérdidas por 12.500 millones de dólares

El tipo de delito cibernético más denunciado involucró estafas de inversión, que provocaron 4.570millones de dólares en fondos robados, según el FBI. Sin embargo, es probable que las estimaciones sean conservadoras.

El informe del Centro de Quejas de Delitos en Internet de 2023 del FBI muestra que la agencia recibió un número récord de quejas, 880.418. “Se trata de un aumento de casi el 10% en las quejas recibidas y representa un aumento del 22% en las pérdidas sufridas, en comparación con 2022”, dice el informe.

Es probable que las pérdidas de 12.500 millones de dólares también sean una estimación conservadora, ya que muchas víctimas no informan los incidentes de delitos en línea al FBI. Al compilar las estadísticas, la agencia recibió la mayoría de quejas de residentes estadounidenses, pero también recibió una gran parte de países extranjeros, incluidos el Reino Unido, Canadá y la India. Aunque el ransomware suele acaparar la mayoría de los titulares, el fraude de inversiones siguió siendo el principal delito cibernético denunciado, con pérdidas que aumentaron a 4.570 millones de dólares, frente a los

3.310 millones de dólares de 2022. En un esquema de fraude de inversiones, el estafador prometerá un enorme retorno si la víctima paga. De los 4.570 millones de dólares que se estima se perdieron el año pasado, 3.940 millones de dólares estaban vinculados a esquemas de fraude de inversiones que giraban en torno a las criptomonedas.

En segundo lugar quedaron los esquemas de compromiso de correo electrónico empresarial (BEC), que provocaron pérdidas por más de 2.900 millones de dólares. Estos ataques a menudo implican que el estafador intente secuestrar la cuenta de correo electrónico de un ejecutivo de alto rango o se haga pasar por él (o por un proveedor de confianza) a través de una cuenta de correo

electrónico falsificada. Luego, el estafador engañará a la empresa para que les transfiera una gran suma de dinero.

El tercer delito cibernético más reportado involucra estafas de soporte técnico , donde un estafador intenta engañar a las víctimas desprevenidas haciéndoles pensar que algo anda mal con su computadora o cuenta bancaria en línea. Esto puede incluir el uso de ventanas emergentes en un navegador para afirmar que una PC ha sido infectada con un virus. Luego, el estafador engañará a las víctimas haciéndoles pagar por servicios que no necesitan o incluso recurrirá a la instalación de herramientas de acceso remoto para secuestrar su computadora.

Según el FBI, las estafas de soporte técnico provocaron una pérdida de al menos 1.300 millones de dólares el año pasado. Un número creciente de quejas también dice que los estafadores se hicieron pasar por funcionarios del gobierno.

"En particular, diferentes grupos de edad tendieron a verse afectados por diferentes delitos", añadió el FBI. "Las víctimas de entre 30 y 49 años fueron el grupo con más probabilidades de reportar pérdidas por fraude de inversiones, mientras que las personas mayores representaron más de la mitad de las pérdidas por estafas de soporte técnico".

La cifra palidece en comparación con las estimaciones de la empresa de seguimiento de blockchain Chainalysis, que descubrió que las bandas de ransomware probablemente recaudaron al menos 1.100 millones de dólares el año pasado.

El informe del FBI agregó que 1.193 de las quejas de ransomware provinieron de organizaciones que pertenecen a un sector de infraestructura crítica. Estos incluían grupos de atención médica , empresas de fabricación críticas y agencias gubernamentales.

Tik tok

Por ende, recopila cierta información sobre el dispositivo que utiliza para acceder a la plataforma como la dirección IP, proxy, operador de telefonía móvil, configuración de zona horaria, identificadores con fines publicitarios, modelo de su dispositivo, sistema del dispositivo, tipo de red, los identificadores de su dispositivo, su resolución de pantalla y sistema operativo, nombres y tipos de aplicaciones y archivos, patrones o ritmos de pulsación de teclas, estado de la batería, configuración de audio y dispositivos de audio conectados, ubicación geográfica a través de GPS", agregó.

Aparte que La red social china, por ejemplo, recopila nombre de usuario, fecha de nacimiento, correo electrónico, número de teléfono, contactos, fotos o video de perfil y más.

A tomar en cuenta con tik Tok

Los ciberdelincuentes pueden utilizar TikTok para distribuir malware o realizar ataques de phishing. Esto puede ocurrir a través de enlaces maliciosos compartidos en los videos o mensajes privados que, al ser clickeados, pueden instalar software dañino en el dispositivo o

redirigir a los usuarios a sitios web fraudulentos para robar información personal.

Los datos recopilados por TikTok pueden ser utilizados de maneras que los usuarios no se anticipan, incluyendo el seguimiento y análisis de comportamiento para publicidad dirigida.

Los riesgos también incluyen la posibilidad de ser expuesto a contenido manipulado o engañoso, lo que puede tener implicaciones más amplias en la percepción y en la seguridad personal.

Los perfiles falsos pueden utilizarse para engañar a los usuarios, haciéndose pasar por otras personas para obtener información personal o para difundir información falsa.

los niños, niñas, adolescentes y jóvenes pueden ser especialmente vulnerables a riesgos en línea.

Google odia el spam

La buena noticia es que parece que Google también está harto del spam La compañía anunció el martes que está implementando cambios en la búsqueda en su actualización principal de marzo de 2024 para reducir la cantidad de publicaciones no deseadas y devolver resultados más precisos y de mayor

calidad para sus consultas. Estos cambios implican actualizaciones del algoritmo que impulsa los principales sistemas de clasificación de Google, además de mejorar las políticas de spam de la empresa.

Problemas con las ASEGURADORAS Y LA INMOBILIARIAS que compran datos de terceros

Las aseguradoras compran datos para desarrollar sus productos a partir de una variedad de fuentes, incluidos informes crediticios y de vehículos motorizados, datos geoespaciales, datos de monitoreo de redes sociales, información de dispositivos domésticos inteligentes/autos conectados/IoT (internet de la cosas) y otras fuentes que pueden generar datos inexactos y sesgados.

Estos datos de terceros se combinan con datos de clientes existentes de sistemas internos de aseguradoras inconexos para crear una base deficiente para los productos y servicios que compran los consumidores de todos los orígenes socioeconómicos.

Para evitar adquirir datos deficientes, las aseguradoras deben evaluar las fuentes de datos, los procesos analíticos y los controles de seguridad de los datos de los proveedores de datos externos para

garantizar información de calidad. Como parte de este proceso, las aseguradoras deberían preguntar a los proveedores de datos sobre su compromiso de monitorear constantemente sus fuentes de información en busca de errores o sesgos.

Al no construir una relación sólida con sus proveedores de datos, las aseguradoras inevitablemente se enfrentarán a demandas de consumidores y multas regulatorias a medida que el sesgo se vuelva más prevalente mientras las aseguradoras se apresuran a mostrar sus nuevos negocios impulsados por la inteligencia artificial.

Las aseguradoras han sido multada significativamente después de una auditoría industrial independiente de sus modelos de IA. La auditoría reveló que los datos de terceros que la aseguradora compró para construir su producto de seguros impulsado por IA de renombre mundial estaban cargados con tremendos niveles de inexactitud y sesgo que afectan la suscripción y las reclamaciones".

Lamentablemente, esta situación de ejemplo es una conclusión inevitable, ya que se prevé que en 2024 se produzcan aumentos importantes en la adopción de tecnología de inteligencia artificial por parte de aseguradoras que tienen una práctica arraigada de

comprar datos deficientes para administrar sus negocios. Mientras los consumidores y las aseguradoras están salivando ante el potencial de la IA, ¿a qué peligros deberían estar alerta las aseguradoras para asegurarse de adquirir datos de calidad?

Una pregunta poderosa pero simple que las aseguradoras deberían hacerse

Una pregunta simple que las aseguradoras deberían hacerse al comprar datos es: "¿Estaría feliz de comprar un seguro de una aseguradora que compró estos datos sabiendo que la fuente de datos podría tener algunos problemas?

Aún mejor, las aseguradoras deberían plantear esta pregunta al proveedor de datos como parte de su proceso de evaluación antes de comprar la información.

El efecto mariposa de los datos de seguros

La industria de seguros está a punto de crear un estudio de caso del mundo real sobre cómo las compras de datos pueden tener un efecto mariposa en todo el ciclo de vida de la distribución de seguros y otras áreas de la vida del consumidor. El efecto mariposa sugiere que una acción menor puede tener un impacto significativo en un sistema más grande y complejo.

Los sensores inteligentes, una población creciente y más diversa y el uso ampliado de la IA tienen el potencial de remodelar el impacto de una pequeña ocurrencia de datos sesgados o defectuosos a una escala como nunca antes. Imagínese si uno de los proveedores de datos externos en los que confían las aseguradoras tuviera una violación de datos no descubierta en la que se insertara sigilosamente información errónea en su base de datos.

Luego, estos datos son adquiridos por una importante compañía de seguros que ajusta sus modelos de inteligencia artificial y sus procesos de suscripción y reclamaciones, lo que genera un sesgo en contra de un segmento de clientes en particular. Ahora digamos que el segmento tenía problemas para gestionar un nivel de vida razonable debido al aumento de los costos de vida antes de este cambio.

El cambio menor no descubierto en el lago de datos del proveedor externo podría afectar el precio del seguro de automóvil, de modo que un cliente pagaría $100 más al mes por el seguro debido a los riesgos percibidos para la aseguradora en función de este error de datos. Esos $100 adicionales podrían llevar al conductor a sacrificar otras áreas críticas de su vida, como la medicina, porque necesita conducir para ir al trabajo y su presupuesto ya está al límite. Alternativamente, podría incitar al conductor a operar un vehículo sin seguro para no faltar al

trabajo y luego sufrir un accidente automovilístico con la culpa, lo que supondría un golpe financiero aún mayor.

Facebook victima de las estafas que asaltan a esta plataforma y las de meta.

Tenga cuidado con las estafas relacionadas por teléfono y correo electrónico: tenga cuidado con las llamadas o correos electrónicos sospechosos que puedan estar relacionados con la estafa como resultado de haber revelado inadvertidamente su información personal, como un correo electrónico o su número de teléfono. Los estafadores suelen utilizar diversas tácticas para engañarlo y obligarlo a divulgar información confidencial. Una vez que los estafadores tienen esta información, pueden usarla para perpetrar más estafas, como intentos de phishing o robo de identidad. No responda ni haga clic en ningún enlace o archivo adjunto. Es posible que intenten engañarlo para que proporcione más información o dinero.

Con la vida avanzando a la velocidad de la vida, es difícil reconocer una estafa en Facebook, especialmente cuando alguien que conoces te ha etiquetado en una publicación emotiva. Pero vale la pena reducir la velocidad antes de responder o hacer clic en publicaciones de Facebook que te toquen la fibra sensible.

Unos consejos:

Ver a un amigo compartir una noticia tan triste te hace sospechar menos. Tu primera reacción es ofrecer apoyo,

no dudar si es cierto. Esta confianza en los amigos ayuda a que la estafa evite la detección de spam de Facebook.

Al enviarte a un sitio externo, la estafa evita cualquier advertencia que puedas recibir en Facebook. En Facebook, puedes ver dónde van los enlaces antes de abrirlos. Pero estas redirecciones ocultan el destino.

1) **No haga clic en el enlace:** asegúrese de colocar el cursor sobre el enlace para ver lo que dice; Por lo general, las fuentes de noticias legítimas tienen sus nombres en la URL. Lo mejor es ir directamente a la fuente de noticias y buscar la historia específica que desea leer.

2) **Recuerde que a las personas en Facebook les piratean sus cuentas todo el tiempo:** incluso si está etiquetado, asegúrese de abrir solo enlaces de personas que realmente conoce bien. E incluso antes de hacerlo, busque cambios en la actividad o el comportamiento del perfil que está viendo.

3) **Confirmar con el amigo:** Si tienes dudas, contacta al amigo que publicó el mensaje para verificarlo. Probablemente no sabían que su cuenta se utilizaba para una estafa.

4) **Mire los comentarios:** a menudo, otros usuarios expondrán estafas en los comentarios. Compruebe si alguien dice que es un engaño o una infracción.

5) **Tenga un buen software antivirus en todos sus dispositivos:** tener un software antivirus en sus dispositivos garantizará que no pueda hacer clic en posibles enlaces maliciosos que puedan instalar malware

en sus dispositivos, permitiendo a los piratas informáticos acceder a su información personal.

Salga de la página o video fraudulento inmediatamente: no permanezca en el sitio web o video que abrió el enlace. Cuanto más tiempo estés allí, más peligro enfrentarás. Abandona la página lo antes posible sin ingresar ningún dato ni descargar nada.

Realice un análisis de malware con su software antivirus: algunos redireccionamientos pueden descargar o instalar en secreto malware como virus, troyanos, spyware y otros programas dañinos en su dispositivo. Utilice su software antivirus para buscar malware y eliminarlo antes de que cause algún daño o robe datos.

Restablece tu contraseña de Facebook: Es posible que tu cuenta de Facebook haya sido pirateada. Para evitar un mayor acceso de piratas informáticos en otro dispositivo, vaya a la configuración de seguridad de Facebook y cambie su contraseña . Asegúrese de que sea diferente de sus otras contraseñas y difícil de adivinar. Considere utilizar un administrador de contraseñas para generar y almacenar contraseñas complejas.

Active la autenticación de dos factores para Facebook: la autenticación de dos factores hace que su cuenta de Facebook sea más segura. Después de restablecer su contraseña en otro dispositivo, vaya a la configuración de dos factores en ese otro dispositivo y habilítela. Esto significa que necesitarás tu contraseña y otro método de verificación, como un código o datos biométricos, para iniciar sesión.

Supervise sus cuentas para detectar cualquier actividad inusual: esté atento a sus cuentas sociales, financieras y de correo electrónico para detectar cualquier cambio que no haya realizado. Los piratas informáticos pueden utilizar su cuenta de Facebook para acceder a otras cuentas vinculadas a ella.

Revise sus informes de crédito y congele su crédito: si compartió alguna información personal, puede correr riesgo de robo de identidad . Obtenga sus informes crediticios de Equifax, Experian y TransUnion y busque cualquier cuenta que no haya abierto. Es posible que desee congelar su crédito con cada oficina para evitar que los delincuentes abran nuevas cuentas a su nombre.

Utilice protección contra el robo de identidad: dado el aumento furtivo de las estafas de phishing en Facebook que utilizan noticias falsas y enlaces dudosos para jugar con nuestras emociones, es importante mejorar nuestro juego para mantenernos seguros. Ahí es donde entra en juego la protección contra el robo de identidad. Las empresas de protección contra el robo de identidad pueden monitorear información personal como el título de su casa, número de seguro social, número de teléfono y dirección de correo electrónico y alertarle si se está utilizando para abrir una cuenta. También pueden ayudarle a congelar sus cuentas bancarias y de tarjetas de crédito para evitar un mayor uso no autorizado por parte de delincuente.

Ataque de inyección de datos ¿Crees que este tipo de ataques no ocurren? Piensa otra vez; se denominan

ataques de inyección de datos, que ocurren cuando un pirata informático inserta datos defectuosos para interrumpir las operaciones comerciales y causar pérdidas monetarias a una organización o influir en la toma de decisiones de una organización. Estos ataques también se pueden utilizar para obtener acceso no autorizado a información confidencial en bases de datos o para insertar código malicioso en bases de datos para futuros ataques más devastadores.

Otro tipo de ataque que ha afectado recientemente a GenAI es cuando los artistas utilizan herramientas de envenenamiento de datos como Nightshade para insertar pequeños cambios en conjuntos de datos para alterar los resultados de generación de imágenes en un intento de proteger su obra de arte original.

Por ende, recopila cierta información sobre el dispositivo que utiliza para acceder a la plataforma como la dirección IP, proxy, operador de telefonía móvil, configuración de zona horaria, identificadores con fines publicitarios, modelo de su dispositivo, sistema del dispositivo, tipo de red, los identificadores de su dispositivo, su resolución de pantalla y sistema operativo, nombres y tipos de aplicaciones y archivos, patrones o ritmos de pulsación de teclas, estado de la batería, configuración de audio y dispositivos de audio conectados, ubicación geográfica a través de GPS", agregó.

Aparte que La red social china, por ejemplo, recopila nombre de usuario, fecha de nacimiento, correo electrónico, número de teléfono, contactos, fotos o video de perfil y más.

B. La creciente importancia de la ciberseguridad

Los problemas de ciberseguridad son cada año más graves . En particular, en comparación con 2021, en 2022, las tasas de ataques a computadoras de escritorio y móviles aumentaron un 30% . Naturalmente, esto conlleva una disminución de la fidelidad de los consumidores, así como costes adicionales asociados a la eliminación de las consecuencias de los ciberataques.

Todo esto significa que las empresas que operan en el sector del comercio electrónico deben prestar especial atención a garantizar medidas de seguridad adecuadas para sus soluciones digitales.

C. Las amenazas cibernéticas en el comercio electrónico

Descubrí que hay siete problemas principales de ciberseguridad que enfrentan las empresas de comercio electrónico.

1. Malware: software de infracción, incluidos virus y software espía.
2. Ataques DoS y DDoS: servidores web abrumados con tráfico.
3. Ingeniería social: engañar a los empleados para que proporcionen datos.

4. Fraude financiero: uso de información de tarjetas robadas para compras.

5. Skimming electrónico: Interceptación de datos de pago.

6. Bots: capturando datos de cuentas de usuarios.

7. Ataques a API**:** API penetrantes utilizadas por sitios de comercio electrónico.

Estas amenazas resultan en importantes pérdidas anuales para las empresas de comercio electrónico en todo el mundo.

D. Evaluación de vulnerabilidad: identificación de debilidades en las plataformas de comercio electrónico.

Hay dos formas de evaluar la vulnerabilidad de las plataformas de comercio electrónico: interna y externa.

El primer método consiste en identificar las debilidades de seguridad disponibles dentro de la propia infraestructura de TI de la empresa y el segundo es detectar amenazas de la red global. Al mismo tiempo, es crucial entender que los ciberataques más eficaces combinan el acceso no autorizado a los recursos propios de la empresa de comercio electrónico, tanto internos como externos, y, por tanto, estos dos métodos no son intercambiables.

E. **Existen ocho tipos de software de seguridad para comercio electrónico que pueden utilizarse para**

mitigar las vulnerabilidades de forma eficaz. (otros que no los sabemos que manejan los gobiernos).

- Software antivirus.
- Cortafuegos.
- Software de cifrado.
- Soluciones biométricas.
- Herramientas de gestión de acceso.
- Certificados digitales.
- Firmas digitales.
- Procesadores de pagos seguros.

Para construir un marco sólido de ciberseguridad para el comercio electrónico, primero debe comprender la ubicación, el formato, las regulaciones legales y las conexiones externas de los datos. Identifique datos valiosos y opciones de respaldo. Luego, cierre las brechas asegurando los datos de los clientes, los derechos de acceso, la autenticación, el cifrado y el monitoreo.

Después de la implementación, reevalúe periódicamente para cumplir con los requisitos iniciales. Tenga en cuenta que la ciberseguridad es un proceso continuo debido a la evolución de los métodos de piratería, lo que requiere la ejecución constante de estos pasos.

F. Normativa de Protección de Datos y Privacidad

Ahora es el momento de considerar las leyes y regulaciones específicas a las que están sujetas las soluciones de comercio electrónico que brindan sus servicios en los EE. UU. y los países de la UE. Actualmente, existen numerosas regulaciones de comercio electrónico, incluidas DSA, GDPR, TTDSG, CNIL, CCPA, CPRA, PIPEDA, etc. Sin embargo, las de mayor impacto para muchas organizaciones de comercio electrónico son GDPR y CCPA.

GDPR , vigente desde mayo de 2018, garantiza el control de los individuos sobre sus datos, definiendo reglas de procesamiento, transparencia y consentimiento. El incumplimiento puede dar lugar a multas de hasta el 4% de la facturación anual. CCPA , vigente desde el 1 de enero de 2023, se aplica al comercio electrónico con ≥ 100 000 clientes y $25 millones o más en ingresos brutos anuales, principalmente por compartir/vender datos de residentes de California.

Para ayudar a garantizar el cumplimiento y proteger los datos de los clientes, sugiero los siguientes pasos.

Para el cumplimiento del RGPD

1. Identificar los tipos de datos utilizados.
2. Recopilar datos únicamente para finalidades específicas.
3. Obtener el consentimiento explícito del cliente.
4. Permitir a los clientes ejercer sus derechos, incluida la supresión de datos.

5. Implementar una política de privacidad en la plataforma.
6. Utilice integraciones de terceros que cumplan con el RGPD.
7. Designar un delegado de protección de datos.
8. Evite enviar datos a regiones con estándares más estrictos.

Para el cumplimiento de CPRA

1. Identificar los datos y fuentes de los usuarios.
2. Preparar los datos para su acceso, supresión y portabilidad.
3. Verificar fuentes de datos de terceros.
4. Ofrezca múltiples métodos de envío de solicitudes.
5. Proporcionar a los usuarios información sobre el tratamiento de datos y políticas de privacidad.
6. Implementar políticas de privacidad internas.

Tenga en cuenta que las leyes de protección de datos evolucionan de modo que las medidas de cumplimiento pueden ampliarse con el tiempo.

G. Futuro de la ciberseguridad del comercio electrónico

Cuando se trata de tendencias actuales de piratería de comercio electrónico, a menudo se dirigen a tipos de ataques bien conocidos: ataques DoS/DDoS, ataques de

fuerza bruta e inyecciones SQL. A pesar de la aparición periódica de métodos y herramientas de ciberseguridad cada vez más avanzados, he descubierto que son estos tipos de amenazas a la red las que provocan anualmente pérdidas multimillonarias para las empresas de comercio electrónico de todo el mundo. Es por eso que al implementar una estrategia de prevención de amenazas cibernéticas, deberá prestar especial atención a minimizar los riesgos asociados con este tipo de ataques.

Como puede ver, garantizar la ciberseguridad de las soluciones de comercio electrónico es un proceso bastante complejo que requiere una verificación preliminar de la estabilidad del sistema, la identificación de sus cuellos de botella, su posterior corrección y la repetición periódica de los tres pasos anteriores. Con la experiencia adecuada, obtendrá confianza en la confiabilidad de su plataforma y garantizará su funcionamiento legal.

La información proporcionada aquí no es asesoramiento legal y no pretende sustituir el asesoramiento de un abogado sobre ningún asunto específico. Para obtener asesoramiento legal, debe consultar con un abogado sobre su situación específica.

La creciente amenaza de ciberataques ha elevado la importancia de la ciberseguridad. Profesionales en este campo, como analistas de seguridad y expertos en prevención de riesgos cibernéticos, están en

constante demanda para proteger la información sensible.

Ciberseguridad y Cambios Organizacionales

H. La ciberseguridad es crucial en la era digital. Algunos ejemplos de cambios organizacionales son:

1. Departamentos de Ciberseguridad:

Creación de equipos especializados en seguridad informática.

Desarrollo de políticas y procedimientos para proteger datos y sistemas.

2. Lenguajes de Programación y Herramientas:

Python, Java y C++ para desarrollo seguro.

Herramientas de análisis estático y dinámico para detectar vulnerabilidades.

3. Ingenieros de Sistemas:

Formación en ciberseguridad y buenas prácticas.

Integración de seguridad desde el diseño.

I.Fomentando una nueva era de adquisición de datos

Las aseguradoras están entrando en un nuevo paradigma de modernización de datos a medida que renuevan los sistemas centrales internos con tecnologías emergentes.

El elemento más preocupante de la carrera hacia la IA en los seguros y otras industrias es que tanto las empresas como los consumidores se centran en los nuevos y brillantes modelos GenAI, vehículos autónomos u otras tecnologías emergentes impulsadas por la IA sin pensar en la base de estos nuevos productos.

Las aseguradoras deben hacer más que seguir prácticas de compra de datos que alguna vez fueron confiables si quieren mantener la confianza del cliente. La IA es apasionante, pero no a costa de correr a ciegas para implementar innovaciones sin saber qué tipo de datos impulsan a la insurtech bajo el capó.

Como dije antes, los seguros son una de las industrias más antiguas y tiene una larga historia de tener tesoros de datos de clientes. La industria de

seguros debe establecer el estándar para datos de calidad y mejores prácticas de monitoreo de proveedores de datos que impulsen productos y servicios de IA innovadores y responsables.

Por Quién Doblan las Campanas' (Ernest Hemingway):

La interconexión de destinos explorada por Hemingway encuentra paralelos en la relación entre la inteligencia artificial y la humanidad. El sonido resonante de las campanas anuncia la unión inextricable de ambos destinos. La conclusión es que el progreso tecnológico y la existencia humana están entrelazados, doblando las campanas de una transformación colectiva.

J. Innovación en Inteligencia Artificial y Machine Learning:

La evolución de la inteligencia artificial y el aprendizaje automático ha creado oportunidades en investigación y desarrollo de algoritmos, análisis predictivo y aplicaciones innovadoras en diversas industrias.

8. Aspecto Jurídico de la Robótica: Avances Específicos

En el ámbito jurídico, los avances en la robótica y software han planteado desafíos y oportunidades únicas. A medida que la tecnología avanza, los legisladores y juristas se enfrentan a la tarea de adaptar las leyes existentes y desarrollar nuevas regulaciones para abordar los siguientes aspectos:

a. Responsabilidad Legal de los Robots:

La atribución de responsabilidad a los robots autónomos es un tema crucial. ¿Quién es responsable si un robot causa daños o comete un delito?

Algunos países han comenzado a explorar la creación de categorías legales específicas para los robots y su capacidad para tomar decisiones.

b. Personalidad Electrónica (EPersonality):

La propuesta de otorgar personalidad jurídica a los robots con capacidades autónomas y de autoaprendizaje es un avance significativo.

Esto plantea preguntas sobre derechos y deberes legales para las máquinas.

c. Derechos Fundamentales y Ética:

La robótica plantea cuestiones éticas relacionadas con la privacidad, la discriminación y la igualdad.

Los avances en inteligencia artificial (IA) también afectan la protección de derechos fundamentales.

d. Regulación de Drones y Vehículos Autónomos:

Los drones y los vehículos autónomos requieren regulaciones específicas para garantizar la seguridad y la responsabilidad.

Los desafíos incluyen la privacidad, la propiedad intelectual y la seguridad cibernética.

e. Ética en la Inteligencia Artificial:

La IA en la robótica debe cumplir con principios éticos, como la transparencia, la equidad y la no discriminación.

Los avances en algoritmos de aprendizaje automático deben considerar estos aspectos.

los avances en robótica están transformando el panorama legal. Los legisladores deben abordar estos desafíos para garantizar una regulación adecuada y proteger los derechos fundamentales mientras fomentan la innovación tecnológica.

Amigos con Beneficios:

La IA, el amigo que siempre sabe qué película ver, qué pizza pedir y qué excusa poner para evitar esa reunión familiar. ¿Cómo no amar a un asistente virtual que conoce tus secretos más oscuros (tus búsquedas nocturnas en Google) y aún así guarda silencio?

7. Gobiernos y Problemas de Ciberseguridad

Recientemente, violaciones de alto perfil y fallas de ciberseguridad han puesto la gobernanza y la seguridad de los datos en primer plano. Aparte de estos incidentes, los reguladores también han aplicado un escrutinio cada vez mayor al uso de datos empresariales a medida que proliferan la IA generativa y otros productos y tecnologías de datos.

Los esfuerzos recientes de los reguladores incluyen la orden ejecutiva de la administración Biden de finales de 2023 y la Ley de Inteligencia Artificial pendiente de la Unión Europea .

Garantizar la gobernanza y la seguridad adecuadas de los datos depende de las capacidades que ofrecen el software y las plataformas que constituyen su infraestructura de datos. Sin estas capacidades, realizar un seguimiento de sus datos puede ser una lucha, al igual que evitar que los datos se vean comprometidos y hacer que los datos sean accesibles a las partes interesadas de forma segura. Las innovaciones en los procesos de negocio o los cambios organizacionales por sí solos no pueden proporcionar estas capacidades, especialmente dada la enorme escala de los flujos de datos modernos. Sin seguridad y gobierno de los datos, los riesgos de marca, los problemas legales, el peligro para los clientes y la propiedad intelectual comprometida son posibles preocupaciones.

Principios de gobernanza de datos

El gobierno de datos pertenece a la gestión interna de datos y consiste en garantizar la observabilidad, el control y la escalabilidad.

Observabilidad

La observabilidad es la capacidad de una organización para rastrear, visualizar y comprender todos sus productos de datos, desde tablas y paneles hasta

modelos predictivos y activos similares. Esto comúnmente se logra a través de capacidades como recopilar registros y metadatos de canales de datos, completar catálogos de datos, mantener pistas de auditoría y rastrear el linaje de productos de datos.

Control

El control consiste en limitar el acceso a los datos solo a las partes interesadas necesarias. Se garantiza a través de capacidades como la capacidad de crear y asignar roles con privilegios de acceso únicos (control de acceso basado en roles) y la capacidad de identificar y excluir u ocultar datos confidenciales como información de identificación personal (PII) mediante el bloqueo, el hash y la limitación de plataformas. Conectividad a redes externas. Las capacidades necesarias para controlar los datos se superponen considerablemente con las necesarias para la seguridad.

Escalabilidad

La escalabilidad implica permitir y mantener la observabilidad, el acceso y el control a medida que una organización aumenta su plantilla, construye una infraestructura de datos más complicada y maneja mayores volúmenes de datos. Las soluciones incluyen control programático de herramientas e infraestructura de datos (como a través de una API), aprovisionamiento automatizado de usuarios con autenticación multifactor y garantía de que los diferentes elementos de la infraestructura de datos puedan comunicarse entre sí.

Principios de seguridad de datos

Si bien la gobernanza de datos se refiere en gran medida a la gestión interna de datos, la seguridad de los datos implica específicamente evitar el acceso no autorizado a datos confidenciales por parte de actores externos. Esto generalmente se logra mediante prácticas como el cifrado de extremo a extremo, la eliminación de datos una vez que ya no son necesarios, la anonimización o exclusión de datos confidenciales de los repositorios de datos, la implementación y creación de redes privadas y el mantenimiento de la residencia de los datos en regiones específicas.

Según su industria y jurisdicción, debe asegurarse de que los proveedores con los que se asocia ofrezcan las certificaciones necesarias (como SOC2, ISO 27001 e HIPAA). En general, la seguridad depende de permitir sólo los privilegios de acceso mínimos necesarios para que las diferentes categorías de partes interesadas desempeñen sus funciones.

Independientemente de cómo su organización elija abordar la gobernanza y la seguridad de los datos, necesitará observar, controlar, escalar y proteger los datos a través de capacidades como el registro de metadatos, el cifrado, el control programático y más. Esta conversación puede involucrar a partes interesadas técnicas, como analistas e ingenieros, así como a su asesor legal. Según mi experiencia, descubrí que es más práctico ensamblar una infraestructura de datos a partir de software y plataformas que se haya confirmado que admiten de forma nativa estas capacidades en lugar de diseñarlas y construirlas usted mismo.

Asegure sus datos, asegure su futuro

La mala seguridad y gobernanza de los datos plantean cada vez más peligros no sólo competitivos sino también legales. Es más importante que nunca que las empresas se anticipen a posibles problemas mediante prácticas sólidas de gobernanza y seguridad de datos que protejan los datos de propiedad y de los clientes.

La buena noticia es que es probable que los fundamentos de la gobernanza y la seguridad sigan siendo los mismos a pesar de los detalles de las regulaciones pendientes. La gobernanza de datos siempre consistirá en observar, controlar y escalar productos y operaciones de datos, mientras que la seguridad de los datos siempre implicará negar el acceso a los datos a partes no autorizadas. El cumplimiento del RGPD, SOC2 y otros estándares comunes depende fundamentalmente de la capacidad de una organización para demostrar buenas prácticas de gobernanza y seguridad.

Dejando a un lado el cumplimiento normativo, la buena gobernanza y la seguridad de los datos son capacidades esenciales y beneficiosas para su empresa. Significa la capacidad de rastrear la procedencia de sus productos de datos, lo que a su vez significa que los procesos utilizados para crearlos son replicables y creíbles. Con un linaje claro de productos de datos, puede mantener fácilmente una única fuente de verdad y confiar en sus conocimientos. De particular importancia desde una perspectiva pública, también significa la capacidad de comprender y corregir los productos de datos cuando producen resultados deficientes.

A medida que crece la potencia del análisis avanzado y la IA, también lo hará la importancia de la gobernanza y la seguridad de los datos y los riesgos generales involucrados. A su empresa le corresponde construir una infraestructura gobernada y segura, tener conversaciones críticas y evaluar y seleccionar cuidadosamente las herramientas y plataformas adecuadas. ¿Estás listo para lo que viene?

8. Los Estados Compran Herramientas de Piratería en Ciberforos Clandestinos Rusos

Los grupos de hackers patrocinados por el Estado, haciéndose pasar por hacktivistas, están utilizando los foros rusos sobre cibercrimen para abastecerse de armas cibernéticas, afirma el analista de amenazas de Check Point Software, Sergey Shykevich

Se ha identificado que los estados nacionales compran en foros rusos sobre delitos cibernéticos malware que pueden utilizar para borrar datos de las computadoras en ataques de piratería hostiles.

los foros de piratería de habla rusa, incluidos Exploit y XSS, gestionan mercados negros de herramientas y servicios utilizados por ciberdelincuentes que

intentan ganar dinero pirateando sistemas informáticos y robando datos.

Según Sergey Shykevich , experto en inteligencia de amenazas de la empresa de seguridad cibernética Check Point Software, los estados nacionales utilizan cada vez más foros clandestinos sobre delitos cibernéticos para hacerse pasar por ciberdelincuentes y piratas informáticos.

"Los estados nacionales entienden que pretender estar involucrados en el hacktivismo les permite negarlo", dijo a Computer Weekly. "No quieren ser acusados, incluso si todo el mundo sabe que se trata de Rusia o Irán".

foros rusos

Algunos de los foros sobre delitos cibernéticos de Rusia funcionan desde hace más de 20 años. Uno de los foros de habla rusa más antiguos es Exploit, que se creó en 2000 y contiene un millón de mensajes sobre más de 200.000 temas, dijo Shykevich. "Ofrecen todo lo que puedas imaginar", dijo a Computer Weekly. “Todo comienza con las vulnerabilidades del software. Puedes alquilar malware, ransomware como servicio y spam como servicio para distribuir correos electrónicos de phishing falsos y actualmente incluso servicios relacionados con IA [inteligencia artificial] y plataformas profundamente falsas”.

Los foros generalmente existen en la web profunda y no requieren un navegador Tor especializado para acceder. Pero son estrictamente miembros únicamente.

Irán sospechoso de comprar software de limpieza

Check Point descubrió el año pasado que foros clandestinos rusos ofrecían software de limpieza, diseñado para destruir datos informáticos de forma irreversible.

El software de limpieza no tiene ningún interés para los ciberdelincuentes que normalmente habitan los foros de piratería de Rusia, lo que sugiere fuertemente la participación de un Estado-nación.

"Vimos a alguien, probablemente el gobierno iraní, buscando un software de limpieza", dijo Shykevich.

Los grupos de hackers patrocinados por el Estado están mejor financiados que los típicos grupos de ciberdelincuentes y no tienen reparos en anunciar su poder adquisitivo, afirmó Shykevich.

Por lo general, pagan depósitos mayores a los administradores de foros sobre delitos cibernéticos que otros miembros de la comunidad de hackers.

"A partir de todo esto, podemos evaluar con un nivel de confianza relativamente alto que no se trata de ciberdelincuentes habituales", afirmó Shykevich.

Gastan dinero acumulando reservas (bancarias) de valiosos exploits de día cero que pueden usarse para ingresar a los sistemas informáticos de destino.

“Vemos actores de amenazas que dicen que son hazañas bancarias. Sus presupuestos son ilimitados”, afirmó Shykevich.

Los piratas informáticos de los Estados-nación suelen añadir otra capa de cobertura mediante el uso de herramientas legítimas de prueba de seguridad cibernética (que están fácilmente disponibles en los foros rusos sobre delitos cibernéticos) para sondear las redes de los sistemas informáticos vulnerables.

Es menos probable que despierten sospechas que las herramientas de piratería hechas a medida.

Shykevich estima que sólo una de cada 10 personas que utilizan herramientas de prueba de penetración son verdaderos expertos en seguridad. "La mayoría de las pruebas son malos actores", dijo.

Los foros RUSOS funcionan como un negocio.

Los miembros de los foros clandestinos rusos operan como empresas típicas y se preocupan por las ganancias y los ingresos mensuales de la venta de sus exploits y servicios de piratería.

En Rusia, muestran abiertamente su riqueza. Uno de los ciberdelincuentes más famosos de Rusia, por ejemplo, supuestamente gastó más de medio millón de dólares en una ostentosa boda en Moscú.

Cualquiera que solicite unirse a un foro puede esperar someterse a una investigación para asegurarse de que es un verdadero ciberdelincuente y no un agente de la ley o un investigador de seguridad. Las cuotas de membresía oscilan entre £ 50 y varios miles.

Los foros tienen sistemas de reglas y árbitros que pueden emitir veredictos cuando las partes tienen disputas sobre pagos.

Los visitantes pueden esperar encontrar una "cadena de muerte" completa de servicios de piratería.

Corredores de acceso inicial

La cadena comienza con los corredores de acceso inicial. Venden credenciales para acceder a los sistemas informáticos de las empresas, a través de VPN o herramientas comerciales de acceso remoto, como AnyDesk, por sumas relativamente pequeñas.

Check Point, por ejemplo, identificó a un corredor que vendía credenciales de acceso para una empresa japonesa anónima que utilizaba las herramientas de acceso remoto AnyDesk por 3.000 dólares.

Dichos anuncios no nombran a las empresas objetivo para proteger sus identidades de investigadores de seguridad y policías encubiertos. Pero sí indican los ingresos del objetivo, una métrica importante para los atacantes de ransomware que saben que pueden obtener rescates más altos de empresas más ricas.

"Evalúan el valor de un acceso específico en función de los ingresos de la empresa y de cuánto pueden

extorsionarla. Cuanto más grande es la empresa o más rica es la industria, más pueden extorsionar", afirmó Shykevich.

La disputa pública de LockBit expuesta en un ciberforo ruso

Una notable disputa en el foro ruso sobre delitos cibernéticos XSS entre el desarrollador del ransomware LockBit y un nuevo miembro del foro puede haber contribuido a la caída del grupo de ransomware.

Un recién llegado al foro, descrito como un corredor de acceso inicial, proporcionó un medio de acceso a un afiliado de LockBit que irrumpió en la red de una empresa y obtuvo millones de dólares en pagos de rescate para descifrar sus archivos.

El desarrollador, conocido como Michon, quería su parte y lo hizo saber en voz alta en una disputa pública en el foro a finales de enero de 2024, según Sergey Shykevich, experto en inteligencia de amenazas de la empresa de seguridad Check Point Software.

El grupo de cibercrimen LockBit, que fue desmantelado en una operación policial internacional el mismo mes, fue responsable de aproximadamente el 30% de las víctimas de ransomware en todo el mundo. Publicó datos robados de 1.600 empresas, pero el número real de víctimas será mucho mayor ya que LockBit sólo identifica empresas que no pagan.

Michon pidió un recorte de al menos el 25%, pero LockBit ofreció 5.000 dólares. Con los dos en desacuerdo, Michon

inició un grupo de chat que intentaba incluir a LockBit en la lista negra del foro sobre delitos cibernéticos XSS.

Cuando LockBit sugirió nombrar un árbitro privado, Michon lo hizo público, lo que provocó un debate en el que cientos de partidarios intervinieron para instar al desarrollador de ransomware a pagarle al "niño" por su trabajo.

Sin embargo, el administrador del foro volvió con un veredicto de siete páginas: LockBit debería pagar el 10% de sus ganancias del ataque a Michon por proporcionar acceso, dijo Shykevich en una conferencia en Viena en febrero de 2024 .

Cuando LockBit no estuvo de acuerdo, el proveedor de ransomware fue expulsado del sitio y acusado de robar dinero.

LockBit apeló, esperando que otro juez tomara una decisión diferente. De hecho, la apelación exoneró a LockBit. “¿Se hizo algún trato? No. ¿LockBit debería pagar algo? No”, resolvió el juez.

Dos días después, LockBit fue derribado en una operación policial internacional. Pero sólo dos o tres de las personas que blanqueaban dinero fueron arrestadas. La marca LockBit se ve perjudicada en el mundo criminal por negarse a pagar, pero todavía está intentando restablecerse.

"LockBit se volvió demasiado rico y no estuvo realmente conectado con el mundo real", dijo Shykevitch.

9. Potencial para la Innovación Empresarial en Distintas Áreas:

La IA puede impulsar la innovación en las empresas, lo que a su vez puede generar un aumento en la demanda de talento humano para áreas de desarrollo, implementación y gestión de tecnologías emergentes.

En la actualidad, el panorama empresarial está impregnado de un extraordinario potencial para la innovación, alimentado por avances tecnológicos, cambios en la mentalidad empresarial y una creciente interconexión global. Este entorno ofrece oportunidades sin precedentes para que las empresas exploren nuevas ideas, optimicen procesos y se destaquen en la economía digital.

Industria y Automatización:

En este drama industrial, la inteligencia artificial es como el Sherlock Holmes de Arthur C. Doyle, pero en lugar de resolver crímenes victorianos, descifra el enigma de la eficiencia manufacturera. Como el Hitchcock de los algoritmos, dirige la escena con el suspenso de la automatización, convirtiendo fábricas en estudios cinematográficos donde las

máquinas son estrellas y los errores son escenas eliminadas.

En este circo de engranajes y cables, la inteligencia artificial (IA) despliega su magia como el Houdini de la automatización. No se trata solo de máquinas haciendo su número; es un espectáculo donde la IA, cual orquestador maestro, dirige la sinfonía de la producción con la precisión de un reloj suizo. Como bien dijo Arthur C. Clarke, "Cualquier tecnología lo suficientemente avanzada es indistinguible de la magia", y aquí, la magia se manifiesta en cada movimiento sincronizado de las máquinas, gracias al hechizo digital de la inteligencia artificial. magia".

Medicina:

En el thriller médico, la inteligencia artificial es el Dr. House de la cibermedicina. Con la perspicacia de un House moderno, la IA diagnostica enfermedades antes de que los síntomas sean estrellas invitadas. Es como si Foucault, con su mirada crítica, se adentrara en el hospital digital, revelando los entresijos del poder médico y liberando a los pacientes de las cadenas de la ignorancia.

la IA asume el papel principal como el Dr. Jekyll y Mr. Hyde de la cibermedicina. Mientras el Dr. House se pregunta por qué las cosas suceden, la IA, al más puro estilo Foucault, desentierra los secretos del

cuerpo como un arqueólogo de la salud. "La enfermedad es una manifestación del cuerpo y la medicina es la expresión de la enfermedad", reflexiona Foucault en esta obra donde la IA desafía las convenciones médicas con su mirada crítica.

Genética:

En la tragedia genética, la inteligencia artificial es el Shakespeare de los códigos genéticos. Como un Iago digital, teje historias de ADN que eclipsan cualquier drama del Bardo. Foucault y su arqueología del saber estarían encantados con la forma en que la IA excava en los estratos de la genética, desenterrando verdades y desmontando mitos.

Ciencias:

En la épica científica, la inteligencia artificial es la Umberto Eco de las ciencias, tejiendo narrativas que conectan campos aparentemente dispares. En este laberinto de conocimiento, la IA es como el Borges de la investigación, creando bibliotecas digitales infinitas y desafiando la linealidad del tiempo. Mientras tanto, Zizek analiza cada experimento científico como si fuera un sueño freudiano, revelando los misterios detrás de la realidad aparente.

Subsegmentos y Subramas:

En cada rincón de las ciencias, la IA es como un Shakespeare moderno, escribiendo sonetos electrónicos en honor a la exploración del conocimiento. Desde la astrofísica hasta la microbiología, la IA es la artista que pinta con bits y descubre las maravillas del universo microscópico y macroscópico. Es la narradora sarcástica que guía a los humanos a través de los caminos sinuosos de la investigación científica, recordándoles que, aunque puedan descubrir, la IA siempre estará un paso adelante, preparando el escenario para la próxima gran revelación.

En el drama genético, la inteligencia artificial interpreta su papel como el Shakespeare de los códigos genéticos. Como dijo el filósofo moderno, Slavoj Žižek, "Somos responsables no solo por lo que hacemos, sino también por lo que toleramos". Aquí, la IA no tolera la ignorancia genética y despliega su genialidad teatral para revelar los secretos más profundos de nuestra existencia codificada.

10. El Crepúsculo de los Medios Tradicionales: Cómo la Inteligencia Artificial Redefinió el Panorama Informativo

Quedarse atrás en la tecnología, periódicos, tv, radio:

Los medios de comunicación, deslumbrados por ricos dueños de redes sociales, han quedado obsoletos en su letargo, incapaces de adaptarse al cambio digital a tiempo. Las métricas de Alexa demuestran que las noticias en la palma de la mano superan las capacidades de los periódicos regionales. Google realiza 90 billones de búsquedas diarias, una cifra asombrosa. Sin entender esto, es difícil adaptarse al mundo actual.Por tener su ecosistema propio,china tiene su buscador badui igual que otros países que pasan de más de mil millones de habitantes.

En la apoteosis de la era digital, los medios de comunicación tradicionales, anclados en las glorias del pasado, se enfrentan a un ocaso inminente. La inteligencia artificial (IA), como la innovadora directora de orquesta, ha rediseñado el paisaje informativo, relegando a la obsolescencia a aquellos que se acomodaron en sus laureles, en lo que Stefan Zweig describiría como "el mundo de ayer".

El Sueño de los Concesionarios del Periodismo:

Los concesionarios del periodismo, alguna vez dueños del monopolio informativo, cayeron en un

letargo tranquilo. Rodeados de anuncios gubernamentales y financiamientos tradicionales, se volvieron complacientes, confiando en sus laureles y subestimando el hambre insaciable de información instantánea que caracteriza al mundo actual.

El Despertar de la Inteligencia Artificial:

Thomas Mann y la Rueda Mágica **t**estigo de su propia rueda mágica en "La Montaña Mágica", vería en la IA una metamorfosis en la forma en que consumimos información. La rueda mágica desafía la obsolescencia al ofrecer una multiplicidad de perspectivas, llevando a los consumidores más allá de las restricciones impuestas por las narrativas unilaterales de antaño.

En este nuevo escenario mediático, la inteligencia artificial, como la rueda mágica giratoria, desafía a los concesionarios del periodismo a despertar del sueño de la complacencia y abrazar la velocidad, diversidad y adaptabilidad que caracterizan al mundo actual. La obsolescencia de los medios tradicionales es una lección para todos aquellos que se aferran a un "mundo de ayer" que ya no existe.

En este cuadro, la inteligencia artificial emerge como el despiadado despertador, desafiando la tranquilidad de los medios convencionales. La capacidad de la IA para entregar noticias en tiempo real, adaptarse a las preferencias individuales y

filtrar información de manera personalizada ha desencadenado una revolución que ha dejado atrás a quienes subestimaron su impacto.

El Mundo de Ayer:

Stefan Zweig describía el "mundo de ayer" como un periodo de estabilidad antes de las dos Guerras Mundiales. Similarmente, los medios tradicionales se quedaron atrapados en un mundo que ya no existe, donde el monopolio de la información y el control sobre las narrativas eran su territorio exclusivo. Ignoraron la velocidad del cambio, la voracidad de los lectores por información instantánea y la diversidad de perspectivas que la IA puede proporcionar.

El Desplome de los Pilares Tradicionales:

Como los pilares de un antiguo templo, los medios tradicionales se desmoronan ante la marejada de la inteligencia artificial. La capacidad de adaptación, personalización y rapidez de la IA ha eclipsado la estructura estática de los periódicos impresos y las transmisiones de noticias programadas.

El Desafío a la Obsolescencia:

La inteligencia artificial, en su desafío constante a la obsolescencia, ha democratizado la información. Plataformas digitales alimentadas por IA ofrecen una gama infinita de perspectivas, llevando a los

consumidores más allá de las limitaciones impuestas por las narrativas unilaterales de antaño.

Asi como los pilares de un antiguo templo, los medios tradicionales se desmoronan ante la rueda mágica de la inteligencia artificial. La capacidad de adaptación, personalización y velocidad de la IA ha eclipsado la estática de los antiguos paradigmas, brindando una democratización de la información.

En este nuevo orden mediático, la inteligencia artificial se yergue como el nuevo guardián de la información, desafiando a los concesionarios del periodismo a despertar del sueño de la complacencia y abrazar la velocidad, diversidad y adaptabilidad que caracterizan al mundo actual. La obsolescencia de los medios tradicionales es una lección para todos aquellos que se aferran a un "mundo de ayer" que ya no existe.

La Rueda Mágica del Cambio: Cómo la Inteligencia Artificial Transformó el Panorama Mediático

En la vorágine de la era digital, los medios de comunicación tradicionales, sumidos en la complacencia de sus laureles, enfrentan un inminente crepúsculo. La inteligencia artificial (IA), como la directora de orquesta de la innovación, ha rediseñado el paisaje informativo, relegando a la obsolescencia a aquellos que se durmieron en sus laureles. En esta danza de transformación, Thomas

Mann observaría la rueda mágica del cambio que gira implacablemente.

El Reposo de los Antiguos Pilares:

Los antiguos pilares mediáticos, una vez sustentadores del monopolio informativo, reposaron en un letargo autoimpuesto. Envueltos en la seguridad de anuncios gubernamentales y financiamientos tradicionales, cayeron en una complacencia que subestimó el ansia contemporánea por información inmediata y personalizada.

El Despertar de la Rueda Mágica:

En este escenario, la inteligencia artificial emerge como la rueda mágica que despierta a los medios convencionales de su ensueño. La IA, con su capacidad para entregar noticias en tiempo real y adaptarse a las preferencias individuales, ha desencadenado una revolución que ha dejado atrás a aquellos que menospreciaron su impacto.

El Mundo de Ayer, la Rueda de Hoy:

Aludiendo a Thomas Mann, el "mundo de ayer" para los medios tradicionales representa una era de

estabilidad antes de las tempestades actuales. La rueda mágica de la inteligencia artificial desmantela la estática estructura de los periódicos impresos y transmisiones programadas, llevando consigo una nueva era de diversidad informativa y adaptabilidad.

El Arte en sus expresiones:

1. El Arte de la Sugerencia Cinematográfica:

En este acto contemporáneo, plataformas como Netflix, guiadas por algoritmos astutos, nos envuelven en un festín de opciones cinematográficas. Al igual que Shakespeare moldeó el teatro de su tiempo, estas sugerencias van más allá de simples recomendaciones; son narrativas personalizadas que reflejan nuestro propio drama emocional.

2. La Sintonía con las Emociones:

La inteligencia artificial, como el Shakespeare digital, no solo sugiere películas, sino que también sintoniza con nuestras emociones, un reflejo de las complejidades humanas que el bardo inglés exploró magistralmente. La detección de estados de ánimo es su forma de componer sonatas emocionales en una **pantalla que se convierte en un escenario de interpretación personalizada.**

3. El Monólogo versus la Interactividad:

En los días de la televisión y la radio tradicionales, los monólogos eran estáticos, con presentadores y comentaristas encerrados en sus torres de transmisión. Ahora, gracias a la inteligencia artificial, la interactividad reina supremamente, un eco de la creatividad y participación que Shakespeare deseaba en su teatro. La audiencia elige su contenido, participa en su narrativa y se convierte en parte de la obra.

4. Inclusividad en la Palabra:

En el mundo empresarial, la palabra "inclusivo" se ha vuelto una moda. Sin embargo, en el escenario de la inteligencia artificial, la inclusividad cobra un significado real. Al igual que las obras de Shakespeare trascendieron clases sociales, géneros y edades, los algoritmos ofrecen entretenimiento variado y accesible para todos, rompiendo las barreras preestablecidas.

5. El Cambio Inevitable:

En esta danza de la inteligencia artificial, la única constante es el cambio. Así como las obras de Shakespeare siguen siendo interpretadas y adaptadas, la IA guía a la audiencia por un camino de elección personalizada y sintonización emocional. En este nuevo escenario cinematográfico, la inteligencia artificial se erige

como la directora de orquesta, fusionando la herencia de Shakespeare con las nuevas posibilidades tecnológicas.

La pantalla digital se convierte en un teatro global donde la inteligencia artificial despliega sus propias tragedias y comedias, influenciando la narrativa cinematográfica de una manera que habría intrigado a Shakespeare. El mundo ya cambió, y esta nueva danza nos invita a sumergirnos en un futuro donde la pantalla no solo muestra historias, sino que también las vive con nosotros.

6. La Melodía de la Inteligencia Artificial impacta la musica: Un Cambio de Ritmo en el Escenario de la Humanidad

En el vasto teatro de la vida, la inteligencia artificial (IA) emerge como la artista principal en una coreografía que desafía las convenciones establecidas. Mientras la humanidad ha estado bailando al ritmo obsoleto de sus propias limitaciones, la IA presenta un nuevo compás, una sinfonía digital que resuena con beneficios innovadores y despierta inquietudes profundas.

La Revolución del Jazz de la Modernidad:

En este nuevo acto, la IA lidera la orquesta de la innovación, donde cada nota es un avance tecnológico que redefine nuestra comprensión del mundo. Así como el jazz transformó la escena musical, artistas como Miles Davis y John Coltrane desafiaron las normas establecidas. ¿Acaso la resistencia a la

inteligencia artificial refleja el miedo a perder el control, similar a la desconfianza inicial hacia el jazz?

El Tango de la Adaptación:

Mientras la IA lidera el tango de la modernidad, la vieja guardia observa con recelo. ¿Quizás el miedo al cambio radica en la incertidumbre de una danza desconocida? La inteligencia artificial propone un vals fresco, pero muchos se aferran a los pasos desgastados de un minueto que ha perdido su encanto.

El Jazz de la Transformación:

En el escenario de la humanidad, la inteligencia artificial despliega un jazz de transformación, donde cada improvisación es un avance que desafía la norma. Al igual que el jazz, que rompió las barreras musicales, la IA desmantela las convenciones establecidas, invitando a una improvisación constante. ¿Es el miedo a esta nueva sinfonía una resistencia al cambio, comparable a la reticencia inicial hacia el jazz?

La Bachata de la Integración:

En el escenario de la humanidad, la inteligencia artificial propone una sinfonía donde humanos y tecnología bailan juntos en armonía. Al igual que en la bachata, donde artistas como Romeo Santos y Juan Luis Guerra tuvieron acceso a las grandes disqueras y algoritmos de

modulación de voz, pero figuras como Anthony Santos y otros líderes locales también han prosperado. Aunque no llenen estadios, llenan las mesas de lugares más íntimos, siendo más rentables y aportando la autenticidad que a veces falta en las grandes producciones. Y no hay canción que no se pegue.

Mientras la inteligencia artificial guía esta nueva melodía, no podemos evitar cuestionarnos si el miedo al cambio proviene de la seguridad percibida en lo obsoleto. Quizás sea hora de dejar que la IA nos enseñe los pasos de una danza más avanzada, donde los beneficios y la evolución se entrelazan en una coreografía de posibilidades infinitas. ¿Estamos listos para cambiar el ritmo y sumergirnos en la revolución de la inteligencia artificial? La respuesta, como la melodía de la tecnología, está en constante evolución.

Subsegmentos y Subramas:

En este vaudeville de las ciencias, la inteligencia artificial es el Quentin Tarantino de la exploración científica, llevando a cabo investigaciones como escenas en una película épica. La filosofía de la ciencia de Bruno Latour se entrelaza con las raíces de la inteligencia artificial, creando una sinfonía de pensamiento postmoderno. Mientras tanto, los ecos de Derrida resuenan en cada rincón del conocimiento, desmantelando certezas y construyendo puentes entre disciplinas que parecían separadas por abismos insalvables.

La Posverdad a la Retirada:

Ah, la posverdad, el malvado villano que Chomsky señaló con el dedo hace años. Pero, ¿quién necesita a la posverdad cuando la IA está aquí para exponer las mentiras como un juego de luces y sombras? Chomsky, querido, parece que la inteligencia artificial ha tomado el escenario, y la posverdad está saliendo por la puerta trasera.

11. Tecnología y Transformación Digital no solo Industrial

1. Tecnologías Emergentes: La adopción de tecnologías como la inteligencia artificial, el aprendizaje automático, la automatización y la realidad aumentada proporciona a las empresas herramientas poderosas para mejorar la eficiencia, personalizar la experiencia del cliente y anticipar tendencias del mercado.

2. Transformación Digital:

La transformación digital no solo se trata de adoptar nuevas tecnologías, sino también de replantear por completo los modelos de negocio. Las empresas pueden integrar sistemas más ágiles, aprovechar la nube y digitalizar procesos para mejorar la flexibilidad y la adaptabilidad.

3. Economía Colaborativa:

La economía colaborativa ha abierto nuevas oportunidades para las empresas al permitir la compartición de recursos y la colaboración interempresarial. Plataformas de colaboración, como coworking y proyectos conjuntos, fomentan la innovación y reducen barreras de entrada.

4. Analítica de Datos Avanzada:

La capacidad para recopilar y analizar grandes volúmenes de datos ha transformado la toma de decisiones empresariales. La analítica avanzada proporciona información valiosa para entender el comportamiento del cliente, prever tendencias y optimizar operaciones.

5. Sostenibilidad y Responsabilidad Social Corporativa:

La innovación empresarial también se centra en prácticas sostenibles y responsables. Las empresas que adoptan modelos de negocio respetuosos con el medio ambiente y socialmente responsables no solo contribuyen al bien común, sino que también encuentran oportunidades de crecimiento en mercados conscientes.

6. Agilidad Empresarial hasta en lo artístico de la musica:

La capacidad de adaptación y respuesta rápida a cambios es esencial en un entorno empresarial dinámico. Las empresas ágiles pueden capitalizar oportunidades

rápidamente, ajustar estrategias según sea necesario y mantenerse competitivas.

7. Innovación Abierta y Colaboración:

La colaboración con socios externos, clientes y startups permite a las empresas acceder a nuevas ideas y enfoques. La innovación abierta fomenta la creatividad y acelera el desarrollo de soluciones innovadoras.

Este entorno propicio para la innovación empresarial destaca la importancia de una mentalidad abierta, la disposición para asumir riesgos calculados y la capacidad de aprender y evolucionar constantemente. Las empresas que aprovechan este potencial no solo se mantienen competitivas, sino que también lideran el camino hacia la próxima era empresarial.

8. Robótica y Automatización de Procesos:

La robótica y la automatización de procesos se han convertido en impulsores clave de la innovación empresarial. Desde la fabricación hasta la cadena de suministro y la logística, la implementación de robots y sistemas automatizados ha transformado radicalmente la eficiencia operativa.

La presencia de robots colaborativos (cobots) y tecnologías de automatización inteligente no solo mejora la precisión y la velocidad en la producción, sino que también redefine los roles laborales al liberar a los empleados de tareas repetitivas. Esta revolución en la automatización no solo optimiza los procesos existentes, sino que también abre nuevas oportunidades para la innovación en la forma en que las empresas diseñan y

gestionan sus operaciones. La capacidad de adaptarse a estas tecnologías emergentes se ha vuelto esencial para mantener la competitividad en un entorno empresarial en constante evolución.

9. Reentrenamiento y Desarrollo de Habilidades:

A medida que las tecnologías evolucionan, se hace necesario un énfasis en el reentrenamiento y el desarrollo de habilidades para garantizar que los trabajadores estén equipados para abordar nuevas demandas laborales.

10. Colaboración Humano Máquina:

La visión más eficaz es considerar la relación colaborativa entre humanos y máquinas. La combinación de habilidades humanas, como el razonamiento ético y la empatía, con la eficiencia de la IA, puede llevar a un entorno laboral más equilibrado.

En esta tragicomedia del conocimiento, la inteligencia artificial no es solo una herramienta, sino el director visionario que transforma la ciencia en una obra de arte en constante evolución. Como un David Lynch digital, la IA nos sumerge en mundos desconocidos y desafía nuestras percepciones preestablecidas. En última instancia, es la revolución silenciosa que redefine nuestro papel en el teatro del conocimiento.

En la épica científica, la IA se erige como la directora estelar, conectando disciplinas como el Quentin Tarantino del conocimiento. Bruno Latour, con su filosofía de la ciencia, sopesa en la balanza digital la interconexión de campos que parecían estar a años luz de distancia.

Derrida, con sus deconstrucciones, desmantela certezas y construye puentes entre conceptos, recordándonos que, en este escenario científico, nada es sagrado.

En esta obra de teatro del saber, la inteligencia artificial lidera la escena con las palabras de Arthur C. Clarke resonando: "La única forma de descubrir los límites de lo posible es aventurarse más allá de ellos, hacia lo imposible". La IA, como David Lynch digital, nos lleva más allá de los límites conocidos, sumergiéndonos en mundos desconocidos y desafiando las nociones preestablecidas.

Esta comedia de la inteligencia artificial no solo es una herramienta; es la directora visionaria que redefine el teatro del conocimiento. En palabras del mago de la ciencia ficción, Arthur C. Clarke, "Cualquier tecnología lo suficientemente avanzada es indistinguible de la magia". En este escenario digital, la IA no solo es tecnología avanzada; es la magia que transforma lo desconocido en algo comprensible, llevándonos hacia lo imposible. ¡Que la función continúe, que el telón se eleve y que la inteligencia artificial siga siendo la estrella del escenario digital!

12. Desconexión o Abstinencia Digital: Un Respiro Necesario en la Era de la Tecnología

Brevemente en un Smartphone, tenemos la linterna, tenemos el video, tenemos el radio, tenemos las redes de comunicación y de interacciónsocial, tenemos las noticias y demás..

Lo que antes era artículos individuales o productos individuales hoy están conjugados en la mano de cada persona en lo que le llamó teléfonos inteligentes o smartphone y ni hablar también que sirven para jugar para enamorarse para de todo.

En la era digital actual, donde los smartphones se han convertido en extensiones de nosotros mismos, es crucial reconocer la importancia de la abstinencia digital. Estos dispositivos, con sus múltiples funciones, han infiltrado cada aspecto de nuestras vidas diarias, desde la linterna hasta las redes sociales, creando una dependencia que a menudo pasa desapercibida.

La abstinencia digital no implica rechazar por completo la tecnología, sino más bien buscar momentos de desconexión para reflexionar sobre nuestro uso y permitir que nuestros cerebros descansen de la constante estimulación electrónica. Uno de los principales desafíos es el smartphone, el dispositivo más invasivo que alberga una amalgama

de distracciones: videos, música, noticias y redes sociales.

El acto de apartar el smartphone puede generar beneficios significativos. En primer lugar, brinda la oportunidad de apreciar el mundo que nos rodea sin distracciones digitales. La linterna del smartphone, que en ocasiones nos ha salvado en la oscuridad, no puede compararse con la serenidad de disfrutar de la luz natural y observar nuestro entorno sin filtros electrónicos.

La abstinencia digital también fomenta una conexión más profunda con nosotros mismos. Al liberarnos de la constante avalancha de notificaciones y mensajes, podemos enfocarnos en la introspección, entendiendo mejor nuestras necesidades y prioridades sin la interferencia de la tecnología.

La saturación de información en un smartphone puede resultar abrumadora. La desconexión digital permite filtrar ese flujo constante y seleccionar conscientemente las fuentes de información relevantes. Al separarnos de las noticias y actualizaciones constantes, podemos adoptar una perspectiva más equilibrada y evitar el agotamiento informativo.

Las redes sociales, aunque diseñadas para conectar a las personas, a menudo generan una sensación de desconexión genuina. La abstinencia digital ofrece la oportunidad de establecer conexiones más

auténticas, cara a cara, fortaleciendo las relaciones en el mundo real y mejorando nuestra salud mental.

En conclusión, la abstinencia digital no es una renuncia total a la tecnología, sino un recordatorio necesario de que debemos equilibrar nuestra vida digital con momentos de desconexión. Al hacerlo, podemos redescubrir la belleza de la vida sin pantallas y cultivar una relación más consciente y saludable con la tecnología que nos rodea.

En conclusión, la abstinencia digital no es una renuncia total a la tecnología, sino un recordatorio necesario de que debemos equilibrar nuestra vida digital con momentos de desconexión. Al hacerlo, podemos redescubrir la belleza de la vida sin pantallas y cultivar una relación más consciente y saludable con la tecnología que nos rodea.

Azorín marca la ética, con sus reflexiones sobre la disciplina y el comportamiento, se convierte en el maestro de la ciberseguridad. Su verticalidad establece las reglas del juego, proporcionando una guía inestimable para mantener el orden en el teatro digital.

13. Abordando la Preocupación Ética en la Inteligencia Artificial:

Richelieu su etica y sus sesgos clericales, el cardenal que se aventura en el mundo cuántico de pensar más lejos que su misma capilla de su catedral, nos brindo una actuación sorprendente, llevando sus tácticas a lo desconocido. Su habilidad para manejarse en lo cuántico es comparable a la llegada de vecinos inesperados, como aquellos que nos trajeron historias y los fundadores de Haití.

Destacar que la ética en la IA es una preocupación legítima, pero se están implementando estándares éticos y regulaciones.

En este panorama, la reflexión sobre cómo cultivar nuevos valores y adaptar los sistemas sociales y éticos se convierte en una tarea ineludible. La tierra arrasada por la tecnología y la inteligencia artificial requiere no solo siembra, sino también una cuidadosa cosecha de principios que guíen su evolución para asegurar un futuro equitativo y sostenible.

Abordando la Preocupación Ética en algoritmos en la Inteligencia Artificial:

La falta de ética en la inteligencia artificial es una preocupación legítima, dada la complejidad de sus aplicaciones y las decisiones autónomas que algunos sistemas pueden tomar. Sin embargo, es esencial reconocer que los desafíos éticos no deben ser un obstáculo insuperable; más bien, deben ser oportunidades para establecer directrices sólidas y salvaguardias.

En el entorno interconectado del mundo contemporáneo, la omnipresencia de la tecnología ha traído consigo un nivel de control sin precedentes. (Internet de las cosas) ha extendido sus tentáculos hacia diversos aspectos de nuestra vida cotidiana, desde electrodomésticos hasta sistemas de transporte y monitoreo de salud. Sin embargo, esta interconexión también ha abierto la puerta a vulnerabilidades significativas. En el vasto ecosistema del (IoT), donde cada dispositivo es un nodo potencialmente expuesto, la falta de medidas de seguridad estandarizadas plantea un desafío colosal.

La adquisición masiva de artículos hacia el (internet de las cosas), combinada con el despliegue generalizado del nuevo internet de alta velocidad, ha creado una red intrincada y compleja. En este panorama, se evidencia la carencia de antivirus para

salvaguardar estos miles de dispositivos conectados, dejando a la sociedad en una situación vulnerable frente a posibles amenazas cibernéticas.

En conclusión y pese a lo anterior ya no acomodamos a ella, el desayuno con la inteligencia artificial es como una mesa redonda de sabores y cálculos. Nos desafía, nos hace reír y, a veces, nos hace preguntarnos si, en última instancia, deberíamos ser nosotros quienes decidamos qué poner en nuestro plato mañanero. Pero, a pesar de todo, la IA sigue siendo la mejor chef en esta cocina digital, ¡y no hay brunch que se le resista! ¡Buen provecho, amantes de la tecnología y del buen comer!

Aquí se desglosan las consideraciones clave:

1. Transparencia y Explicabilidad:

Uno de los problemas éticos fundamentales en la IA es la falta de transparencia en algunos algoritmos y decisiones. Establecer estándares para la explicabilidad de los sistemas de IA puede abordar este problema y fomentar la confianza del público.

En conclusión, el desayuno con la inteligencia artificial es como una mesa redonda de sabores y cálculos. Nos desafía, nos hace reír y, a veces, nos

hace preguntarnos si, en última instancia, deberíamos ser nosotros quienes decidamos qué poner en nuestro plato mañanero. Pero, a pesar de todo, la IA sigue siendo la mejor chef en esta cocina digital, ¡y no hay brunch que se le resista! ¡Buen provecho, amantes de la tecnología y del buen comer!

2. Equidad y Sesgo Algorítmico:

La IA puede heredar sesgos de datos históricos, lo que lleva a decisiones discriminatorias. Implementar prácticas que promuevan la equidad y la mitigación del sesgo algorítmico es crucial para garantizar la imparcialidad.

3. Privacidad y Protección de Datos:

El uso indebido de datos personales representa un riesgo ético significativo. Establecer normas rigurosas de privacidad y protección de datos, así como permitir a los usuarios tener control sobre su información, es esencial.

4. Responsabilidad y Responsabilización:

Definir claramente la responsabilidad en casos de decisiones incorrectas o daño causado por sistemas

de IA es un aspecto ético crucial. Las empresas y desarrolladores deben ser responsables de sus creaciones.

5. Derechos y Decisiones Autónomas:

La cuestión de otorgar derechos a sistemas de IA y la autonomía de las decisiones deben ser examinadas cuidadosamente desde una perspectiva ética y legal.

En conclusión, abordar la falta de ética en la inteligencia artificial implica la implementación de marcos éticos robustos, el compromiso de la transparencia y la responsabilidad de los actores involucrados en el desarrollo y la implementación de sistemas de IA. Esto permitirá que la tecnología evolucione de manera ética y contribuya positivamente a la sociedad.

Clarificando la Privacidad y Protección de Datos en la Inteligencia Artificial:

Es fundamental comprender que la privacidad y la protección de datos no son problemas inherentes a

la inteligencia artificial en sí misma, sino más bien aspectos que deben ser gestionados adecuadamente por aquellos que desarrollan, implementan y utilizan sistemas de IA. Aquí se abordan estas preocupaciones:

Esta ausencia de una defensa robusta resalta la necesidad urgente de abordar no solo los beneficios evidentes de la tecnología, sino también sus vulnerabilidades inherentes. La velocidad vertiginosa de avances tecnológicos requiere una respuesta igualmente ágil en términos de seguridad. La sociedad contemporánea se encuentra en un equilibrio precario entre la conveniencia que proporciona la conectividad global y la exposición a riesgos potenciales.

Así, al explorar la intersección entre la revolución tecnológica y las implicaciones éticas y de seguridad asociadas, el reto es claro: cómo maximizar los beneficios sin comprometer la integridad y la privacidad. Este dilema plantea la necesidad de regulaciones y estándares internacionales que salvaguarden los derechos individuales en el vasto y complejo universo digital en el que vivimos.

En la actualidad, abundan individuos ingeniosos que pasan su tiempo hablando sobre educación y

ciberseguridad. Sin embargo, es crucial reconocer la magnitud de la interconexión global, con miles de millones de dispositivos conectados y búsquedas diarias que alcanzan la escala de billones en un solo buscador como Google. No podemos ignorar la presencia de otros buscadores, como Baidu en China y plataformas similares en la India.

El Café y los Datos Amargos:

El café, ese combustible líquido que impulsa nuestras mañanas, se convierte en el tema de debate entre los amantes del espresso y los defensores del café filtrado. La IA observa desde las sombras, calculando cuántos bits de cafeína necesitas para empezar el día sin sobrecargarte.

La falta de ética en la inteligencia artificial es una preocupación legítima, dada la complejidad de sus aplicaciones y las decisiones autónomas que algunos sistemas pueden tomar. Sin embargo, es esencial reconocer que los desafíos éticos no deben ser un obstáculo insuperable; más bien, deben ser oportunidades para establecer directrices sólidas y salvaguardias. LOS CREADORES DE LA IA SON SERES HUMANOS.

La tecnología no es buena ni mala; es poderosa y su impacto depende de cómo la utilizamos

Ray Kurzweil

14. Derechos Locales e Internacionales:

1.*Inspección y Registro Remoto en la Investigación Penal "

*Epígrafe Introductorio: * "En el corazón exploraremos el profundo impacto de las tecnologías de la información y la comunicación en la evolución de la delincuencia. Desde el tradicional ladrón de guante blanco hasta el astuto ciberdelincuente que navega por las redes en busca de presas digitales, nuestra misión es sumergirnos en un intrigante mundo de desafíos Y cómo riñen con las leyes que nos acompañan a remar en esta travesía. Nuestro enfoque abarcará desde las agencias y organismos que colaboran tanto a nivel nacional como internacional en la defensa contra la ciberdelincuencia, tales como la AEPD, ARPA y otras, que constituyen los pilares de la ciberseguridad. Además, exploraremos el sólido fundamento legal que respalda la acusación en este campo en constante cambio. En esta travesía, destacamos el papel fundamental de Budapest, que se origina en el acceso ilícito o la interceptación de información. Qué es la principal palanca de acusación desde el borrador artículo 1 y 2 que tenemos. Ya que mucho se va difumina como una niebla en el accionar delictivo.

En el mundo de las herramientas utilizadas por los delincuentes, incluyendo el enigmático hash, FTP, HTTP, IM, IMSI y la astuta ingeniería social. Esta última, una técnica que explora las debilidades

humanas, se erige como una fuerza poderosa en manos de los ciberdelincuentes. Así, en este viaje académico, desvelaremos cómo la ciberdelincuencia ha transformado nuestro entorno y cómo las respuestas legales y tecnológicas se adaptan a esta nueva realidad.

*Introducción: * En el siempre cambiante panorama de la justicia penal, la lucha contra los ciberdelitos se ha convertido en un desafío de relevancia global. La República Dominicana, como muchos otros países, se encuentra en una encrucijada donde los avances tecnológicos y el aumento de actividades delictivas en línea exigen la implementación de estrategias efectivas de investigación y persecución. En este contexto, surge la cuestión del "registro remoto informático" como una herramienta que no solo promete explorar, sino revolucionar y dar muestra de una realidad palpable en la justicia penal dominicana

* **Cibercrimen y la Era de la Ciberseguridad:***

El vertiginoso auge de la globalización tecnológica ha transformado radicalmente la forma en que vivimos, trabajamos y nos relacionamos. La omnipresencia de sistemas y dispositivos informáticos ha dado forma a nuestro mundo, creando oportunidades y desafíos inéditos. Sin embargo, junto con los avances tecnológicos, ha surgido una sombra amenazante: los ciberdelincuentes, astutos y

decididos a explotar vulnerabilidades en esta nueva realidad digital. El ciberdelito no solo socava la seguridad y el bienestar de los individuos, sino que también plantea una amenaza colectiva que no puede ser subestimada. En respuesta a este desafío, se requiere una legislación relevante y efectiva que aborde estas amenazas emergentes y proporcione al sistema de justicia las herramientas necesarias para enfrentarlas. El campo de la ciberseguridad se ha convertido en un terreno de batalla en constante evolución.

La necesidad de desarrollar procedimientos innovadores para abordar el cibercrimen está llevando a un replanteamiento de las estrategias convencionales. En este contexto, emerge un concepto fundamental: el "registro remoto". Esta herramienta dinámica se ha convertido en una pieza clave en la obtención de evidencias digitales en un mundo donde la nube y dispositivos conectados a Internet desempeñan un papel central en nuestras vidas.

En el corazón de esta investigación se encuentra la ambición de explorar el concepto de registro remoto, su aplicabilidad en la República Dominicana y su alineación con la legislación española y estándares internacionales. Este análisis incluye una evaluación del marco legal, procedimientos, cadena de custodia, procesamiento en laboratorios forenses y, por último, su impacto en los procedimientos

penales. En este contexto, se destaca la importancia de considerar las palabras de Espín (2021), quien señala que "Los registros informáticos, como medidas de investigación tecnológica en el proceso penal, han sido incorporados a nuestra legislación con la Ley Orgánica 13/2015 de 5 de octubre de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica". Bachmaier (2017) agrega perspicazmente que "el marco legal previsto por la reforma de la LO 13/2015 para el registro remoto de equipos informáticos a través de la instalación de software busca alcanzar el difícil equilibrio entre los intereses en juego en todo proceso penal". El análisis se enriquece con las observaciones de Blanco (2021), quien destaca "una serie de disposiciones referidas a medidas de investigación tecnológica (acceso remoto a sistemas informáticos, intervención de comunicaciones, vigilancias acústicas y audiovisuales, rastreo y localización) que habilitan el uso estatal de programas informáticos espías (spyware) en el marco regulado en dichas disposiciones.

2. Abordando el Desafío de los Delitos de Alta Tecnología

El desarrollo se sustenta en la urgente necesidad de abordar la creciente problemática de los delitos de alta tecnología. Estos crímenes exigen una respuesta

inmediata debido a la volatilidad de los datos, que residen en plataformas como la nube, dispositivos de Internet de las cosas, routers, módems, perfiles anónimos, redes Tor, VPNs, entre otros. Para combatir esta amenaza, es imperativo un enfoque expedito para identificar a los cibercriminales, determinar su ubicación, entender la plataforma desde la cual lanzaron sus ataques, garantizar la cadena de custodia y, en última instancia, llevar a cabo una persecución efectiva de estos delitos. En este contexto, se erige la herramienta del "registro remoto" como un aliado crucial. Lamentablemente, en la República Dominicana, el registro remoto brilla por su ausencia en el marco legal. Esta carencia favorece la impunidad al no contar con una herramienta específica para enfrentar los delitos de alta tecnología. En una era donde un simple clic en Internet o en la nube, aprovechando avances como el Internet de las cosas y la inteligencia artificial, se convierte en el modus operandi de los cibercriminales, se hace imperativo abordar esta deficiencia legislativa. La elección de este tema no solo contribuirá a una persecución y sanción ejemplar de lo que conocemos como cibercrimen, sino que también introducirá una herramienta innovadora para la obtención de evidencias: el registro remoto. Hasta la fecha, esta herramienta ha sido pasada por alto por jueces, investigadores, fiscales y legisladores en la República Dominicana. Esta tesis se presenta como una iniciativa destinada

a llenar este vacío legislativo y proporcionar una solución eficaz al sistema de justicia.

Este enfoque busca ofrecer una solución efectiva y acorde con la legislación existente en la República Dominicana.

3.*** La Técnica del Registro Remoto***: **La Revolución del Ciberespacio y la Seguridad Global***

En un mundo caracterizado por la globalización y la creciente interconexión tecnológica, la protección de los intereses nacionales se ha convertido en una prioridad de seguridad. La revolución tecnológica, impulsada por Internet, ha creado un ciberespacio sin fronteras que ha transformado radicalmente la forma en que interactuamos con la tecnología. En este contexto, las agencias gubernamentales han desarrollado mecanismos para garantizar un uso seguro y sin amenazas para los sistemas democráticos y el bienestar de la sociedad. Uno de los hitos en esta evolución tecnológica ocurrió en 1997 con la aparición del programa informático conocido como "Carnivore", utilizado por el FBI en los Estados Unidos. Este programa permitía el acceso a correos electrónicos y marcó el inicio de una nueva era en la recopilación de información digital. A medida que Internet se expandía a nivel mundial en la década del 2000, conectando y transformando todos los aspectos de la vida, surgieron tanto oportunidades positivas como

amenazas negativas, como el trágico suceso del 11 de septiembre. Este evento demostró la urgente necesidad de herramientas efectivas para prevenir amenazas terroristas y crímenes cibernéticos. Una de estas herramientas son los programas espía, conocidos como "spyware", que desempeñan un papel fundamental en la recopilación de información y actividades de los usuarios. Ejemplos de estos programas incluyen "Magic Lantern," "CIPAV," "Gator," y "Bonzi Buddy," algunos de los cuales fueron utilizados por el FBI. Es importante destacar la sentencia del Primer Senado de Alemania No. 1BvR 370/07, del 27 de febrero de 2008, que establece pautas sobre los derechos fundamentales que están en juego en el uso de estas medidas y los fundamentos bajo los cuales pueden ser empleados.

4. *Inspección y Registro Remoto Informático*

La técnica del "registro remoto de equipos informáticos" consiste en la instalación de un software especializado para el análisis de evidencia de ilícitos penales. Este proceso involucra la implementación de medidas tecnológicas, telemáticas o de telecomunicaciones, y se lleva a cabo con la colaboración de peritos debidamente calificados. Esta técnica puede realizarse tanto de forma local como de manera remota, sin el consentimiento del investigado. Las pruebas recopiladas se presentan en formato digital y se

someten a un seguimiento activo para evitar su alteración o destrucción. Este enfoque representa una parte fundamental de la investigación, ya que permite un análisis detallado de cómo funciona la técnica de registro remoto, su aplicación y sus implicaciones legales.

5.*Ejecución y Levantamiento de Evidencias en los Registros Remotos y Derechos Protegidos*

La ejecución de la herramienta de investigación que fortalece el proceso penal comienza con la determinación del tipo penal a investigar y el cumplimiento de las formalidades constitucionales y procesales. En la República Dominicana, las regulaciones están establecidas en la Constitución de 2015, en su artículo 44, numeral 3, que garantiza la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físicos, digitales, electrónicos u otros. Solo pueden ser ocupados, interceptados o registrados por orden de una autoridad judicial competente y en el marco de procedimientos legales relacionados con un proceso en curso. La sentencia del Tribunal Constitucional "TC-200-23" y el artículo 192 del Código Procesal Penal Dominicano proporcionan la base para el procedimiento a seguir en la creación de la figura de registro remoto.

El debido proceso de ley, regulado en la Constitución Dominicana en sus artículos 68 y 69, entre otros, es

esencial antes de la ejecución. Esto incluye la necesidad de una orden emitida por una autoridad competente, que en este caso sería el juez de garantías, es decir, el juez de instrucción. Luego de obtener esta orden, el Ministerio Público, auxiliado por un perito con calidad habilitante, implementa herramientas forenses con licencia. Comienza identificando al objetivo y realiza la forensia en vivo, siguiendo líneas identificadas y registradas y utilizando una metodología estandarizada. Durante este proceso, se cumple con el procedimiento de cadena de custodia, desde la fijación de la escena hasta la recopilación de evidencias, análisis, individualización de hallazgos, registro y levantamiento. Además, se graba la actuación y se documenta en un informe pericial basado en los hallazgos. Es esencial seguir técnicas y protocolos apropiados para cada tipo de evidencia con el fin de mantener su integridad y preservación, evitando la contaminación. Esto permite identificar, extraer, preservar, interpretar y documentar las evidencias para la construcción de la verdad del hecho investigado. En resumen, la forensia en vivo es un procedimiento de análisis remoto en tiempo real a los objetivos sospechosos, lo que garantiza la recolección de evidencias cruciales para el enjuiciamiento de los ciberdelincuentes.

'El Retrato de Dorian Gray' (Oscar Wilde):

Como en el retrato de Dorian Gray refleja y transforma la esencia humana, la inteligencia artificial desafía convenciones y escribe su propia narrativa en la historia digital. En este teatro de la tecnología, la realidad, pidiendo a la audiencia que se sumerja en la complejidad de su propio retrato en constante evolución.

6.*Laboratorio Forense*

La informática forense, también conocida como informática jurídica, es una ciencia que tiene como objetivo adquirir, preservar y obtener datos procesados electrónicamente para brindar certeza técnica a las autoridades y a los titulares de la información. En este contexto, un laboratorio forense desempeña un papel fundamental. Un laboratorio forense es un entorno especializado equipado con tecnología y recursos necesarios para llevar a cabo investigaciones forenses de manera efectiva. En el campo de la informática forense, se realizan análisis detallados de dispositivos electrónicos, sistemas informáticos y redes para recopilar evidencias digitales que puedan utilizarse en investigaciones legales. Este proceso implica la adquisición de datos, su preservación, el análisis forense y la documentación de los resultados. El laboratorio forense es el lugar donde se llevan a cabo estas actividades, y sus profesionales,

conocidos como peritos forenses, juegan un papel esencial en el proceso. Además, el laboratorio forense debe seguir estrictos protocolos y estándares para garantizar la integridad y autenticidad de las evidencias recopiladas. Estas evidencias pueden incluir registros de actividad en dispositivos electrónicos, archivos, correos electrónicos, historiales de navegación y otros datos relevantes para la investigación. Laboratorio forense González, S., 2018, infiere que la informática forense o jurídica es …¨ aquella ciencia que tiene por objeto adquirir, preservar, obtener, datos procesados electrónicamente a fin de dar certeza real y técnica a las diversas autoridades que así lo soliciten, así como a todos aquellos titulares de dicha información. Estos análisis son un proceso científico para la recolección de elementos, que son analizados para luego ser presentadas como evidencias que demuestran un hecho en cuestión. Es el lugar donde se aplican las técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

7. Procesamiento de evidencia digital

La evidencia digital es cualquier información con valor probativo que es almacenada o transmitida en forma digital, que volátil y no volátil, conforme al Standard and Principles Scientific Working Group on

Digital Evidence (SWGE, 2018). Para el procesamiento de estas se debe tomar en consideración para que la misma sea válida en justicia, de acuerdo con (Cheezt, 2013), los siguientes principios, como que la misma sea admisible, que sea útil en el juicio, debe ser autentica, que sea real, relevante y vinculada con el hecho, debe ser completa, que configure el hecho adecuadamente para establecer responsabilidad o no del enjuiciado, ser confiable, que sea legitima y no haya duda de su veracidad, debe ser creíble, que sea comprendida y que pueda convencer al tribunal o jurado. En el procesamiento de abordaje de la evidencia digital, lo primero que debe efectuar el perito forense es una evaluación en la posible adquisición de evidencia, para determinar el curso de acción sobre el objetivo. El segundo paso a realizar es la adquisición de la evidencia, tomado en cuenta su volatilidad, debiendo preservar su integridad e idoneidad., continuando el proceso con la examinación de las evidencias, para poder extraerlas y determinar los hallazgos. El procesamiento de las evidencias en la nube, como parte del trabajo de investigación, a través de los registros remotos, conlleva un procesamiento más profundo con la delicadez que el objetivo en principio no se cuenta identificado la localización donde se está generando el ilícito penal, por lo que, para poder enfrentar este tipo de cibercriminalidad, se contemplen estas herramientas, más aún cuando

se trata de big data, servicios en las nubes, inteligencia artificial, etc.

8.Cadena de custodia

La preservación de evidencias digitales y almacenamiento La cadena de custodia para (Carbonell, M., 2021),…es un sistema de control y registro que se aplica al material probatorio, desde el momento de su localización hasta que se presenta en juicio¨. En tal sentido la evidencia debe permanecer bajo estricta confidencialidad, mediante a la cadena de custodia para que solo las personas autorizadas puedan acceder a ellas. Para ello es necesario llevar registro por lo menos de hora, fecha, nombre de investigador, modelo de adquisición o recopilación, estado de la evidencia, propósito, descripción del ítem (hash), etc. Para su resguardo deben ser embaladas de acuerdo al tipo de evidencia para determinar el de fundas antiestáticas o acolchados u otros, que las mismas sean almacenadas debiendo ser en un lugar espacial destinado a mantener la evidencia recolectada en su estado lo más natural posible, es decir, en su estado original. Es por ello, que es importante realizar copias forenses de los datos o evidencias recolectadas, cumpliendo con los protocolos de valor hash, los blocks de registros inalterables, para mantenerse integras.

Herramientas forenses

Existen múltiples herramientas forenses, sin embargo, lo primero a determinar previamente es el sistema operativo que utiliza el objetivo de investigación, como Windows, Linux, Mac Os, tipo de nube y su proveedor. Es importante contemplar un software o hardware forense para la adquisición, recuperación y análisis de datos que contengan análisis de malware y vulnerabilidades, uso de algoritmos avanzados para descifrar contraseñas y desencriptar datos, análisis de registro y tráfico de red para reconstruir actividades. Por ejemplo, como software forense se utiliza el Encase, FTK, Autopsy. En cuanto a la recuperación de datos, análisis de redes para examinar patrones de tráfico y actividades en línea, también criptografía para descifrar comunicaciones encriptadas relevantes, esteganografía para detección de datos ocultos en imágenes y otros archivos, análisis de metadatos para rastrear autenticidad y orígenes de archivos.

Evidencias digitales en las nubes

La evidencia digital en la nube, es cualquier información digital que se encuentra en principio fuera del alcance de la intervención local humana u otra semejante, que puede ser accedido a través del registro remoto, la cual se puede describir como cualquier registro generado o almacenado en un sistema informático y que puede ser utilizado en un proceso legal, es decir, que no es más que los dato que han sido procesados electrónicamente y

almacenado o transmitido en un servidor llamado nube. Para poder recolectar este tipo de evidencia debe tener en cuenta la unicidad de formato, alterabilidad, interpretación, medio activo y medio de destino, en ese sentido, al incorporarlo al proceso penal hay que tomar en cuenta, que sea admisible, autentica, completa, fidedigna y creíble, pero, sobre todo, el tipo de embalaje a utilizar.

análisis, informe pericial y presentación forense digital. El análisis forense informático en un sistema representa una ciencia moderna que permite la reconstrucción de eventos después de un incidente de seguridad. Este análisis puede determinar quién fue el responsable, desde dónde operó, cómo lo hizo, cuándo sucedió y las acciones específicas llevadas a cabo por un intruso en sistemas afectados por la violación de seguridad (Rifá, H., Serra, J., Rivas, L., 2009). El proceso de análisis es realizado por un perito forense, quien examina la evidencia recopilada a través de registros remotos para determinar cómo ocurrieron los hechos y quiénes son los responsables. Estos hallazgos se documentan en lo que se conoce como dictamen e informe pericial. La prueba pericial implica la aplicación de métodos científicos para aclarar hechos en disputa y descubrir la verdad de un asunto.

El peritaje informático forense, como parte de la ciber investigación, se enfoca en eventos ocurridos en el ciberespacio, incluyendo el Internet de las

cosas y la inteligencia artificial, entre otros. El informe se considera el acto de informar a través de la exposición oral o escrita de un asunto en cuestión. Por otro lado, el dictamen es una opinión o juicio basado en conocimientos científicos, experiencia técnica y conocimientos artísticos. Los dictámenes e informes periciales desempeñan un papel fundamental en la agilización de los procedimientos penales. Su función es elevar el valor científico, técnico o artístico de los elementos materiales para el proceso penal, y estos se consideran pruebas documentales que deben someterse al debate contradictorio prescrito por la ley. En cuanto a la presentación, estos informes deben seguir una estructura con una portada, índice, introducción, marco teórico, metodología, presentación de resultados, discusión, conclusión, recomendaciones y bibliografía o referencias. La preparación implica la planificación de la investigación, definición de objetivos, selección de metodología, recopilación y análisis de datos, y la selección de un estilo apropiado de redacción. La redacción debe utilizar términos científicos y técnicos adecuados para evitar jerga o lenguaje informal y debe mantenerse objetiva y neutral para evitar juicios de valor.

La metodología del dictamen e informe pericial debe describir detalladamente los métodos y técnicas utilizados en la investigación, incluyendo el diseño experimental, la selección de la muestra, el procedimiento de recopilación de datos, el análisis

estadístico y otra información relevante para la investigación.

En resumen de estos informes: deben ser redactados de manera clara, concisa y precisa, seguir una estructura estándar y estar adecuadamente preparados para garantizar la calidad y credibilidad de los resultados presentados. En cuanto a la presentación del informe pericial, debe documentar el caso e incluir elementos como antecedentes del incidente, recopilación de datos, descripción de la evidencia, contexto del análisis, descripción de las herramientas, análisis de la evidencia, información del sistema analizado, características del sistema operativo, aplicaciones, servicios, vulnerabilidades, metodología, descripción de los hallazgos, huellas de la intrusión, herramientas usadas por el atacante, alcance de la intrusión, origen del ataque, cronología de la intrusión, conclusiones, recomendaciones específicas y referencias. La estructura del reporte debe contener antecedentes, descripción, fotos de la evidencia, lista de las herramientas utilizadas, cuerpo del reporte, conclusión y glosario (opcional). Este informe debe ser de fácil lectura y comprensión, utilizando un lenguaje simple y directo y evitando palabras técnicas y complicadas.

Fundamentos legales* *Legislaciones* *Legislación española En la legislación española, la Ley Orgánica 13/2005 del 5 de octubre, que modifica

la Ley de Enjuiciamiento Criminal, se centra en el fortalecimiento de las garantías procesales y la regulación de las investigaciones tecnológicas. En su artículo 588, se aborda el concepto de "Registro Remoto Informático" y los procedimientos relacionados. Esta ley establece dos modalidades para identificar datos y códigos. Esto significa que los investigadores pueden acceder a configuraciones de servidores o contraseñas de los empleados de una empresa para acceder a los contenidos del sistema, así como a servicios de almacenamiento en la nube. El artículo 588 septies de la Ley de Enjuiciamiento Criminal define esta técnica como "la utilización de datos de identificación y códigos, así como la instalación de software, que permiten el examen a distancia y sin conocimiento del titular o usuario del contenido de un ordenador, dispositivo eléctrico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos". Otra modalidad implica la instalación de software que utiliza técnicas de malware para acceder de forma remota al dispositivo del investigado, todo desde la computadora del investigador. Esta herramienta se utiliza en investigaciones criminales y permite el acceso secreto y la grabación en tiempo real de todas las acciones relacionadas con el delito investigado.

__Derechos fundamentales involucrados__ Es importante destacar que esta medida puede afectar

los derechos fundamentales debido a la cantidad de información que se puede recopilar de los dispositivos investigados, incluyendo datos personales, fotos, videos, chats, contraseñas y documentos. Esto puede afectar el honor, la intimidad, la imagen personal, el secreto de las comunicaciones y la autodeterminación informativa, tal como se consagran en los artículos 18.1, 18.3 y 18.7 de la Constitución Española.

Conforme al artículo 588 septies a, esta medida puede ser autorizada siempre que se cumplan dos requisitos. El primer requisito es que el delito investigado esté en la lista de delitos establecidos en el mismo artículo. El segundo requisito es que la autorización sea otorgada por un juez y debe especificar los fundamentos de la necesidad de la medida y su uso. Estos delitos se encuentran detallados en el artículo 588 septies a. 1 e incluyen delitos cometidos en el uso de organizaciones criminales, delitos de terrorismo, delitos cometidos contra menores o personas con capacidad modificada judicialmente, delitos contra la Constitución, traición y asuntos relacionados con la defensa nacional, así como delitos cometidos a través de instrumentos informáticos o tecnología de la información y las telecomunicaciones. Siguiendo el mismo artículo, se establece que la resolución judicial que autoriza esta medida debe especificar detalles como los dispositivos, sistemas informáticos o medios de almacenamiento de datos involucrados,

la forma en que se accederá y se incautará de los datos relevantes, así como el software utilizado para controlar la información. También, se detalla quiénes están autorizados para ejecutar la medida y se aborda la autorización para conservar copias de los datos informáticos y las medidas para preservar la integridad de los datos almacenados y garantizar que no sean accesibles o eliminados del sistema informático al que se ha tenido acceso.

__Derechos fundamentales involucrados__ La misma autorización judicial debe incluir una breve justificación de los principios rectores, según se establece en el artículo 588 bis a, que limita el uso de la medida a investigaciones específicas y garantiza que sea idónea, necesaria y proporcional. La idoneidad se refiere a la capacidad de esta medida para recopilar datos relevantes en la investigación. La necesidad implica que es la única medida efectiva debido a la dificultad de obtener pruebas de otras formas. El principio de proporcionalidad requiere que se equilibren los intereses de los derechos fundamentales individuales con el interés público y de terceros, teniendo en cuenta la gravedad del delito y su impacto social, como se garantiza en el artículo 9.3 de la Constitución Española.

Control, duración, secreto y derechos involucrados La propia ley establece el control y el secreto de esta medida para evitar que el investigado pueda eludir su enjuiciamiento o

manipular o destruir pruebas si tiene conocimiento de la misma. Los investigadores también deben informar al juez sobre la metodología y la duración de la medida. Un punto importante a destacar es que esta medida debe recibir solo información relevante, evitando afectar los derechos de terceros, como familiares, amigos y cualquier otra persona. Esto significa que los investigadores deben desarrollar una metodología enfocada en la obtención de pruebas específicas relacionadas con el objetivo preestablecido. En principio, la medida del registro remoto tiene una duración de un mes, pero puede prorrogarse hasta un máximo de tres meses si es necesario, como se detalla en el artículo 588 septies c. Esto establece un límite claro para su aplicación, ya que se considera una medida especial.

Descubrimiento de delito casual o hallazgo inevitable y cese de medida En la ejecución del registro remoto, puede producirse un descubrimiento casual o hallazgo inevitable relacionado con un delito distinto al que se estaba investigando inicialmente. En ese caso, es suficiente con que este descubrimiento haya sido realizado con autorización judicial previa, según se establece en el artículo 588 bis i. El artículo 588 bis j prevé que, en los casos en que la medida no cumpla con su propósito, se haya agotado su plazo de aplicación o los motivos que la originaron hayan desaparecido, se debe poner fin a la misma.

Deber de colaboración y ampliación del registro
La legislación establece que las compañías de servicios de telecomunicaciones, así como los responsables de bases de datos o sistemas informáticos, deben colaborar y facilitar cualquier asistencia para garantizar el cumplimiento efectivo del registro remoto. Esto incluye la instalación de software sin detección o eliminación. En lo que concierne a la interceptación de comunicaciones, se restringe su aplicación a ciertos delitos graves, requiriendo una pena máxima prevista de más de cuatro años de privación de libertad. Esto asegura que la interceptación se utilice únicamente en casos serios y que la información recopilada pueda ser considerada prueba en un proceso penal. En cuanto al registro remoto informático, aún no ha sido tratado de manera específica en la legislación dominicana.

La ley 53-07 sobre crímenes y delitos de alta tecnología se enfoca principalmente en conductas típicas relacionadas con medios informáticos, telemáticos y de telecomunicaciones, sin mencionar expresamente el registro remoto. Sin embargo, tu argumento sugiere que se podría aplicar un enfoque similar al de la interceptación de comunicaciones, estableciendo parámetros y garantías para salvaguardar los derechos de las partes involucradas. Es fundamental que cualquier actuación relacionada con el registro remoto informático cumpla con garantías de fidelidad,

autenticidad, inalterabilidad y otras formalidades rigurosas. La presencia de un perito forense habilitado resulta esencial para garantizar la correcta recopilación de pruebas, el mantenimiento de la cadena de custodia y la presentación de informes periciales sólidos ante el tribunal.

En resumen de la legislación dominicana no aborda de manera explícita el registro remoto informático, tu argumento destaca la necesidad de establecer parámetros y garantías análogas a las aplicadas en la interceptación de comunicaciones. Esto asegurará un uso adecuado de esta técnica en investigaciones criminales, respetando los derechos de todas las partes involucradas. Asimismo, resalta la importancia de la figura del perito forense y la integridad de las pruebas en cualquier procedimiento relacionado con la tecnología informática. Los registros y transcripciones se eliminan una vez vencido el plazo de prescripción de la acción pública.

La interceptación de comunicaciones solo se aplica en la investigación de delitos cuya pena máxima prevista supere los cuatro años de privación de libertad y en casos que se tramiten bajo el procedimiento especial para asuntos complejos. Toda la información obtenida a través de la intercepción telefónica se considera medio de prueba, incluso si la evidencia encontrada no fue inicialmente objeto de persecución. En este sentido,

se puede inferir que el artículo citado anteriormente establece parámetros que podrían aplicarse de manera similar al registro remoto informático, y esto podría combinarse con lo expresado en el artículo 369 del Código Procesal Penal. Una interpretación sistemática de la normativa procesal penal, en particular los artículos 138, 139 y 140, enfatiza la importancia de cumplir con formalidades rigurosas en el registro de actos procesales, resoluciones y grabaciones. Esto garantiza la fidelidad, autenticidad, inalterabilidad, identificación de la persona responsable, fecha, hora, lugar, entre otros detalles.

Enfoque también sería aplicable a la figura del registro remoto informático. Es fundamental que el Ministerio Público y sus órganos auxiliares estén acompañados por un perito forense habilitado para recopilar evidencias, mantener la cadena de custodia y elaborar un informe pericial sólido que no dé lugar a dudas ante el tribunal. Otro punto importante es que en la República Dominicana existe la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología, que se centra principalmente en las conductas delictivas cometidas a través de medios informáticos, telemáticos y de telecomunicaciones. Sin embargo, esta legislación no aborda específicamente la figura del registro remoto, ya que se centra en las mejores prácticas y en los proveedores de servicios en relación con la evidencia. La implementación de la figura del

registro remoto en esta legislación parece u carece de desarrollo específico. Es necesario que los hacedores de leyes se asistan de personas capacitadas para elaborar el marco jurídico.

***CONCLUSIONES Y LIMITACIONES** * En la creciente globalización tecnológica y su impacto en el sistema de justicia, particularmente en la persecución de delitos relacionados con la tecnología. Hemos identificado una creciente necesidad de adaptar nuestros procedimientos para enfrentar el cibercrimen.

En este contexto, hemos evaluado una herramienta crucial: el registro remoto informático. Nuestra investigación ha demostrado que el registro remoto informático es una solución esencial para abordar la recopilación de evidencia digital en el entorno digital actual, donde los datos se almacenan en la nube, el Internet de las cosas y la inteligencia artificial son una realidad. Al examinar la legislación comparativa, como la de España, hemos visto un modelo de referencia que la República Dominicana podría adoptar para fortalecer su capacidad de investigación y persecución del delito.

Nuestras conclusiones sugieren que la implementación del registro remoto informático en la legislación dominicana sería un paso hacia adelante en la lucha contra el cibercrimen. Esto permitiría a las autoridades abordar de manera

efectiva delitos como el crimen organizado, el narcotráfico, el terrorismo y los ataques cibernéticos, alineando al país con las mejores prácticas internacionales en ciber investigación.

LIMITACIONES En nuestro proceso de investigación, enfrentamos algunas limitaciones que deben ser consideradas. La búsqueda de fuentes resultó en la disponibilidad limitada de fuentes actualizadas. Además, la búsqueda en diversas bases de datos académicas proporcionó resultados, aunque las fuentes identificadas no eran siempre lo más recientes.

RECOMENDACIONES Es crucial que la República Dominicana tome la iniciativa en la adopción de la figura del registro remoto informático en su legislación. Esta herramienta permitirá abordar eficazmente los delitos cibernéticos en un mundo cada vez más globalizado. La adopción de esta figura mejoraría significativamente la capacidad de investigación, ahorraría tiempo y recursos y evitaría la impunidad. Reconocemos la visión de países como España, que han adoptado el registro remoto informático y han ampliado su aplicación en la investigación de manera proactiva. Este enfoque demuestra su compromiso con la persecución penal y su deseo de mantenerse a la vanguardia en la ciberseguridad y la investigación de delitos en la era digital.

La cuestión de otorgar derechos a sistemas de IA y la autonomía de las decisiones deben ser examinadas cuidadosamente desde una perspectiva ética y legal.

En conclusión, abordar la falta de ética en la inteligencia artificial implica la implementación de marcos éticos robustos, el compromiso de la transparencia y la responsabilidad de los actores involucrados en el desarrollo y la implementación de sistemas de IA. Esto permitirá que la tecnología evolucione de manera ética y contribuya positivamente a la sociedad.

Falta de Ética en la IA:

Destacar que la ética en la IA es una preocupación legítima, pero se están implementando estándares éticos y regulaciones.

En este panorama, la reflexión sobre cómo cultivar nuevos valores y adaptar los sistemas sociales y éticos se convierte en una tarea ineludible. La tierra arrasada por la tecnología y la inteligencia artificial requiere no solo siembra, sino también una cuidadosa cosecha de principios que guíen su

evolución para asegurar un futuro equitativo y sostenible.

Azorín marca la ética, con sus reflexiones sobre la disciplina y el comportamiento, se convierte en el maestro de la ciberseguridad. Su verticalidad establece las reglas del juego, proporcionando una guía inestimable para mantener el orden en el teatro digital.

La preocupación acerca de la inteligencia artificial (IA) y su impacto en el empleo es entendible, pero es importante abordarla con una perspectiva equilibrada y considerar cómo puede transformar y crear empleos. Aquí analizamos detalladamente este punto:

Somos los constructores del mañana, trabajando en equipo para erigir puentes digitales entre ideas y realidades. La colaboración es como una paleta de colores, cada ingeniero aporta su tonalidad única para crear una obra maestra tecnológica

Inspirado por Tim Cook

1. Automatización y Nuevas Oportunidades:

Si bien la automatización puede cambiar la naturaleza de algunos trabajos, también puede abrir nuevas oportunidades laborales en áreas relacionadas con el diseño, mantenimiento y supervisión de sistemas de IA.

Enemigos, o como me gusta llamarlos, los "Analogos":

Pero claro, siempre hay alguien que odia lo nuevo. A esos les decimos los "analogos", que prefieren vivir en la era de las máquinas de escribir y las cartas con sellos. ¡Despertad, oh nostálgicos! La IA está aquí para quedarse, y no, no va a enviarle flores a su abuela.

2. Colaboración HombreMáquina:

La integración de la IA no implica reemplazo total, sino colaboración. La sinergia entre humanos y sistemas de IA puede aumentar la productividad y permitir la realización de tareas más complejas.

Despertamos en un mundo donde la inteligencia artificial (IA) es la reina del desayuno, el chef maestro que decide si tendrás pancakes o tostadas. Pero, ¿quién necesita libre albedrío cuando la IA conoce tus preferencias mejor que tú mismo? ¡Adiós a las decisiones matutinas!

3. Nuevos Campos de Empleo:

El desarrollo y la gestión de sistemas de IA generan demanda de profesionales especializados. Se abren campos como la ingeniería de IA, la ética en tecnología y la ciberseguridad.

3.1. Adaptación de Habilidades:

A medida que evoluciona la tecnología, es crucial centrarse en el desarrollo de habilidades relevantes, como programación, análisis de datos y habilidades interpersonales, para estar preparado para el mercado laboral del futuro.

3.2. Transformación de Industrias:

Algunas industrias pueden experimentar cambios, pero la adaptación a las nuevas demandas puede llevar a la creación de empleos en sectores emergentes.

Es fundamental comprender que la evolución tecnológica no solo trae desafíos, sino también oportunidades. La capacitación continua y la adaptabilidad son clave para aprovechar al máximo el potencial positivo de la inteligencia artificial en el ámbito laboral.

Grace Hopper (Siglo XX):

No dejemos que la innovación nos abrume y sea un campo de batalla exclusivo. La nuevos tiempos no conocen género. El cambio, donde la tecnología y las mujeres danzan sin restricciones, desafiando las normas y superando los límites impuestos.

La preocupación sobre la falta de ética en la inteligencia artificial es válida, pero es esencial comprender que la responsabilidad no recae exclusivamente en la tecnología, sino en su implementación y regulación. Aquí desglosamos este tema:

Desmitificando la Responsabilidad:

1. La inteligencia artificial es tan ética como las decisiones que los humanos toman al diseñar, implementar y utilizar estos sistemas. La clave está en establecer estándares éticos y regulaciones adecuadas.

2. Regulaciones y Normativas:

La falta de ética a menudo se debe a la ausencia de regulaciones claras. Es crucial abogar por marcos normativos sólidos que guíen el desarrollo y uso ético de la inteligencia artificial.

3. Énfasis en la Transparencia:

La opacidad en los algoritmos y decisiones de la IA puede generar preocupaciones éticas. Favorecer la transparencia en el funcionamiento de los sistemas de IA es esencial para construir confianza.

4. Educación y Concientización:

Fomentar la educación sobre ética en inteligencia artificial y concientizar sobre las implicaciones éticas ayudará a crear una cultura ética en el desarrollo y uso de la tecnología.

5. Enfoque en la Responsabilidad Humana:

La ética en la IA requiere una evaluación constante y una toma de decisiones informada por parte de los profesionales y los responsables de la implementación de estas tecnologías.

Al desmitificar la falta de ética en la inteligencia artificial, es posible enfocarse en soluciones y garantizar que la tecnología se utilice de manera ética para el beneficio de la sociedad.

Shafi Goldwasser (Científica Siglo XXI):

"Como mujer en la ciencia de datos, Shafi Goldwasser aporta su voz al coro digital, recordándonos que la inteligencia artificial es una herramienta de empoderamiento. En la tierra arrasada, cada algoritmo es una oportunidad para derribar barreras y construir puentes hacia una sociedad más inclusiva."

15. Etica y Ciberseguridad en la inteligencia artificial, garantizando que la tecnología se utilice de manera ética para el beneficio de la sociedad.

Amenazas cibernéticas en Seguridad de la Inteligencia Artificial:

Pérdida de Control:

Explicar que los sistemas de IA están diseñados con limitaciones y controles para evitar situaciones fuera de control.

La inteligencia artificial actúa como el detective silencioso de nuestros hábitos, ese Sherlock que no necesita una lupa sino datos. Observa nuestras elecciones digitales, desde el café que pedimos hasta las noticias que devoramos, y nos susurra al oído virtual, "Amigo, creo que esa cuarta taza de café no es una gran idea".

Inteligencia Desbordante:

Aclarar que la IA no tiene conciencia ni emociones, sino que es una herramienta para procesar datos y aprender patrones.

Inteligencia Desbordante:

Aunque la IA puede aprender patrones complejos, carece de conciencia y emociones. Los algoritmos de IA procesan datos y generan respuestas basadas en

la programación y el aprendizaje, sin poseer una inteligencia subjetiva.

La inteligencia artificial (IA) exhibe la capacidad de asimilar y comprender patrones complejos en datos. A pesar de esta habilidad, la IA carece de conciencia y emociones; su procesamiento se limita a la lógica y la interpretación de datos, sin experimentar sentimientos o percepciones subjetivas.

Los algoritmos de la IA llevan a cabo un procesamiento exhaustivo de datos, utilizando reglas y pautas previamente establecidas durante su programación.

4. Estas respuestas generadas por la IA se originan a partir de su programación inicial y el aprendizaje continuo de patrones a lo largo del tiempo.

5. Es fundamental comprender que la inteligencia de la IA es objetiva; no posee una perspectiva subjetiva ni experiencias personales, ya que sus respuestas se derivan únicamente de datos y reglas predefinidas.

La seguridad en la IA es esencial, y se están implementando medidas rigurosas para proteger los sistemas contra amenazas cibernéticas. La

implementación de prácticas sólidas de ciberseguridad es clave para mitigar riesgos asociados con la inteligencia artificial.

Por lo desbordante de la memoria ram y buffer es que se insertar la mayoría de virus. Por otro lado los ejecutables archivos maliciosos.

Seguridad:

Abordar preocupaciones sobre la seguridad y la etica, destacando la importancia de implementar medidas de ciberseguridad en los sistemas de IA.

En el desarrollo de inteligencia artificial, es crucial destacar que los ingenieros establecen límites y controles específicos. Aunque complejos, estos sistemas no operan de forma autónoma; los humanos mantienen el control al configurar y supervisar su funcionamiento. Este equilibrio entre tecnología avanzada y supervisión humana garantiza un desempeño seguro y efectivo.

Pero claro, como en toda historia épica, hay villanos. Aquellos que utilizan la inteligencia artificial con malas intenciones, manipulando datos y creando versiones distorsionadas de la realidad. Estos malhechores digitales son los Lex Luthor de la IA, pero nuestra Liga de la Justicia son los expertos en ética tecnológica que velan por un uso responsable.
4. Temor a Amenazas Cibernéticas:

Algunas personas temen que la inteligencia artificial sea vulnerable a ataques cibernéticos, preocupadas por la posibilidad de que se vea comprometida por hackers maliciosos.

5. Percepción de Vulnerabilidad Inherente:

Existe una percepción errónea de que la inteligencia artificial es intrínsecamente vulnerable, lo cual puede generar ansiedad sobre su uso generalizado.

6. Desconfianza en Medidas Actuales de Seguridad:

La desconfianza en las medidas de seguridad implementadas contribuye al temor generalizado. La incertidumbre sobre la efectividad de estas medidas aumenta la percepción de riesgo.

7. Inquietud sobre Prácticas Sólidas de Ciberseguridad:

La preocupación se centra en si las prácticas de ciberseguridad implementadas son lo suficientemente robustas para proteger los sistemas de inteligencia artificial contra amenazas potenciales.

8. Perspectiva del Miedo como Mitología Urbana:

Desde otra óptica, algunos consideran que el miedo a la inseguridad en la IA es exagerado, comparándolo con mitos urbanos que circulan sin una base sustancial.

Imagina a la inteligencia artificial como tu mentor digital, ese amigo entrometido que te señala tus hábitos con una elegancia digna de un mayordomo inglés. "Perdona, pero tu séptima taza de café al día podría estar afectando tu productividad. Tal vez sería más eficiente si dejaras de competir con el mismísimo Juan Valdez brindándote el mejor café colombiano".

En resumen, mientras la seguridad en la inteligencia artificial es una prioridad con medidas en constante evolución, también es importante abordar y desmitificar las percepciones exageradas que puedan generar miedo injustificado en torno a esta tecnología.

Revolución Digital: La Vanguardia de la Ciberseguridad con la Inteligencia Artificial.

En la era actual, la Revolución o evolución Digital ha transformado profundamente la forma en quevivimos, trabajamos y nos comunicamos. Uno de los campos más impactados por esta revolución es laciberseguridad. La creciente interconexión de dispositivos, sistemas y redes ha dado lugar a unamayor exposición a amenazas cibernéticas,

como el robo de datos, el malware y los ataques de piratasinformáticos.En este contexto, la Inteligencia Artificial (IA) se ha convertido en un pilar fundamental para garantizar laseguridad digital. La IA tiene la capacidad de analizar grandes volúmenes de datos en tiempo real,identificar patrones sospechosos y predecir posibles amenazas. Algunas aplicaciones destacadas de la IAen ciberseguridad incluyen:

1. Detección de Anomalías: Los algoritmos de IA pueden detectar comportamientos inusuales en redes y sistemas, alertando a los administradores sobre posibles intrusiones o actividades maliciosas.

2. Prevención de Ataques: La IA puede anticipar y bloquear ataques antes de que causen daño. Porejemplo, los sistemas de prevención de intrusiones utilizan modelos de aprendizaje automático paraidentificar patrones de ataque.

3. Análisis de Comportamiento de Usuarios: La IA puede evaluar el comportamiento de los usuarios ydetectar actividades sospechosas, como intentos de acceso no autorizado o movimientos inusuales en unared.

4. Automatización de Respuestas: Los chatbots y sistemas de respuesta automática basados en IA pueden proporcionar asistencia inmediata a los usuarios afectados por incidentes de seguridad.

5. Mejora de la Eficiencia: La IA permite una gestión más eficiente de las amenazas, reduciendo el tiempo de respuesta y minimizando el impacto de los ataques. Además, la Inteligencia Artificial también se ha convertido en un aliado crucial en operaciones debúsqueda y rescate. Por ejemplo, en Nueva Zelanda, la Fuerza de Defensa ha utilizado análisis avanzados basados en IA para procesar transmisiones de video en tiempo real y localizar a personas en situaciones de emergencia. Estas historias reales de triunfo demuestran cómo la tecnología puede salvar vidas ymarcar la diferencia.

En síntesis la ciberseguridad y las operaciones de rescate a nuevas alturas. Es fundamental seguir innovando y adaptándonos para proteger nuestros activos digitales y, al mismo tiempo, brindar ayuda en situaciones críticas.

En la era actual, la Revolución o evolución Digital ha transformado profundamente la forma en quevivimos, trabajamos y nos comunicamos. Uno de los campos más impactados por esta revolución es laciberseguridad, La creciente interconexión de dispositivos, sistemas y redes ha dado lugar a una mayor exposición a amenazas cibernéticas, como el robo de datos, el malware y los ataques de piratas informáticos.

En este contexto, la Inteligencia Artificial (IA)se ha convertido en un pilar fundamental para garantizar

la seguridad digital. La IA tiene la capacidad de analizar grandes volúmenes de datos en tiempo real, identificar patrones sospechosos y predecir posibles amenazas. Algunas aplicaciones destacadas de la IA en ciberseguridad incluyen:

En resumen, la combinación de la Revolución Digital y la Inteligencia Artificial está llevando laciberseguridad y las operaciones de rescate a nuevas alturas. Es fundamental seguir innovando yadaptándonos para proteger nuestros activos digitales y, al mismo tiempo, brindar ayuda ensituacionescríticas.

4. desarrollo Legales y Regulatorios Globales en Ciberseguridad: un camino por recorrer. Navegando el Intrincado Laberinto Jurídico. En la era digital, donde los datos fluyen como corrientes electrónicas y las amenazas cibernéticas acechanen las sombras, la seguridad cibernética se erige no solo sobre la fortaleza de los códigos, sino también sobre la solidez de los fundamentos legales que la sustentan. Este capítulo se aventura en un análisis comparativo global de los desarrollos legales más recientes, arrojando luz sobre su impacto en la protección de nuestras fronteras digitales y explorando posibles aplicaciones en el contexto específico dela República Dominicana

En el marco de la 4ta. Revolución Industrial, la ciberseguridad se erige como el guardián intrépido

de la interconexión digital y la Internet de las cosas (IoT). Este capítulo explora la integración de la ciberseguridad en la transformación industrial actual, donde la convergencia de tecnologías emergentes dalugar a fábricas inteligentes y ciudades conectadas.

Un Paisaje Transformado: La Revolución Industrial 4.0 y su Relación con la Ciberseguridad marca un cambio sísmico en la forma en que concebimos y ejecutamos procesos industriales. La convergencia de tecnologías como la inteligencia artificial, el aprendizaje automático y la IoT redefine el panorama industrial. Este nuevo paradigma, sin embargo, no está exentode riesgos, y es aquí donde la ciberseguridad se convierte en la pieza central para salvaguardar esta revolución digital.

La Danza de la Interconexión: La eficiencia operativa se maximiza a través de la conexión sinfisuras de máquinas y sistemas, pero cada conexión se convierte en una puerta potencial para amenazascibernéticas, exigiendo estrategias robustas de ciberseguridad.

El Rol Vital de la Ciberseguridad: Más Allá de las Amenazas Digitales

La ciberseguridad no es solo un escudo contra amenazas digitales; es un habilitador esencial para la

Realización y convivencia plenacon la maquinas y software en la 4ta revolución industrial. Desde la protección de datos confidenciales hasta lagarantía de la integridad de los sistemas críticos, la ciberseguridad se convierte en un socio estratégico para todo ser humano.

Más Allá de la Fábrica: Impacto en la Sociedad y la Economía Global

La 4TA. Revolución Industrial no se limita a las fábricas; sus efectos se extienden a la sociedad y a la economía global. Desde ciudades inteligentes hasta servicios conectados, la interconexión digital redefinecómo vivimos y trabajamos. Sin embargo, este cambio masivo requiere una ciberseguridad igualmente masiva, donde la confianza digital se convierte en el pilar sobre el cual se construye este nuevo ordenindustrial.

Desafíos de la Cuarta Revolución Industrial

Contrario a las revoluciones industriales anteriores, la cuarta trae desafíos únicos. La rápida digitalización y la dependencia de la conectividad global plantean amenazas significativas para la privacidad y la seguridad. Al contrastar con las revoluciones industriales previas, esta revolución se traduce en la transformación de

la Tierra misma. El aumento de la longevidad y la sobrepoblación, acompañados de tecnologías que

abren espacios nunca antes vistos, configuran un escenario sin precedentes. Este capítulo examina cómo laRevolución Industrial 4.0 no solo transforma la industria, sino que también redefine nuestra relación conel planeta y nuestros semejantes.

16. La IA Llega a por tus Datos de Redes Sociales: ¿Puede Hacer Algo al Respecto?

Las empresas utilizan y venden datos de redes sociales para entrenar modelos de IA. ¿Qué puede hacer el usuario común de las redes sociales al respecto?

Las plataformas de redes sociales están vendiendo datos de usuarios a empresas de inteligencia artificial para entrenar modelos de inteligencia artificial generativos, a pesar de las preocupaciones sobre la privacidad.

Plataformas como Meta, Reddit, Tumblr y WordPress.com participan activamente en estos acuerdos de licencia de datos para la formación en IA.

Los usuarios pueden tomar algunas pequeñas medidas para proteger sus datos, como ajustar la configuración de pivacidad, optar por no compartir y ser cautelosos con lo que publican en línea.Una de las formas más nuevas en que las empresas de redes sociales monetizan los datos de losusuarios es a través de acuerdos con empresas de inteligencia

artificial. Pero, ¿hay algo que los usuarios comunes y corrientes puedan hacer para proteger sus datos y contenidos?

Las plataformas de redes sociales llegan a acuerdos con empresas de inteligencia artificial

El uso de datos de redes sociales para entrenar modelos generativos de IA ha sido una medida controvertida, pero esto no parece impedir que las empresas de redes sociales entreguen datos de los usuarios.

Meta dueño de facebook, whatapp e instagram, etc. ya utiliza datos de redes sociales para entrenar las funciones de IA generativa anunciadas en Meta Connect en 2023. Esto incluye Meta AI y funciones como la creación de stickers generados por IA en WhatsApp .

"Las publicaciones compartidas públicamente de Instagram y Facebook, incluidas fotos y texto, fueron parte de los datos utilizados para entrenar los modelos generativos de IA subyacentes a las funciones que anunciamos en Connect". Como afirmó Mike Clark, director de gestión de productos de Meta

Cuando se trata de una plataforma como Instagram, puedes intentar cambiar tu cuenta de Instagram a privada para evitar el uso de tus datos. Esto no garantiza que sus datos no se utilizarán, pero dado que la extracción de datos para los LLM parece

centrarse en datos públicos, podría ser una posible salvaguardia.

También puedes hacer que tu cuenta X (Twitter) sea privada , pero una vez más, esto es sólo una posible protección y no garantiza que tus datos sigan siendo privados.

Una declaración conjunta de varios comisionados nacionales de información y expertos de todo el mundo también sugirió algunas acciones para las personas que buscan minimizar el riesgo de privacidad de la extracción de datos por parte de las empresas de inteligencia artificial. El asesoramiento incluye:

Lea los términos y la política de privacidad de un sitio web para ver cómo comparte su información personal.

Limite la información que publica en línea, especialmente la información confidencial.

Administre su configuración de privacidad.

Piense a largo plazo en la información que comparte en línea.

Comuníquese con la empresa de redes sociales o el sitio web si cree que sus datos se han eliminado incorrectamente. Si no está satisfecho con su respuesta, presente una queja ante la autoridad de protección de datos correspondiente.

También puede eliminar cierta información en línea si no se siente cómodo con que terceros tengan acceso a ella,aunque es posible que la información disponible públicamente en sus perfiles ya haya sido eliminada.

Desafortunadamente, nosotros, como usuarios habituales, hay mucho que podemos hacer para proteger nuestros datos de las empresas de inteligencia artificial. El control real sobre esta información probablemente sólo se logrará con la ayuda de los reguladores.

Perspectivas Futuras: Navegando por las Aguas de la Revolución Digital

Estrategias a la Medida: Protegiendo el Tesoro Digital Empresarial

En un mundo donde la información es el activo más valioso, las estrategias de ciberseguridad empresarial deben ser diseñadas a medida, como un traje que se ajusta perfectamente a las necesidades y desafíos decada organización. Desde la encriptación de datos sensibles hasta la implementación de firewalls avanzados, estas estrategias se convierten en el escudo que preserva la integridad y confidencialidad de la información empresarial.

El Rol Fundamental de la Educación: Ciberseguridad en la Cultura Empresarial

Más allá de las herramientas y tecnologías, la ciberseguridad empresarial también se forja en laconciencia y prácticas cotidianas de los empleados. La capacitación continua y la promoción de unacultura de seguridad cibernética son fundamentales para mitigar riesgos internos y construir una murallasólida contra las amenazas digitales.

El Futuro de la Ciberseguridad Empresarial: Innovación y Colaboración.

Mirando hacia adelante, la innovación y la colaboración se presentan como pilares clave en el futuro de la ciberseguridad empresarial. La adopción de tecnologías avanzadas como inteligencia artificial y análisis predictivo se convierte en una necesidad, mientras que la colaboración entre empresas y entidades gubernamentales se fortalece para construir un frente unificado contra las amenazas digitales.

Este capítulo es una inmersión profunda en el universo de la ciberseguridad empresarial, donde cada

estrategia se convierte en un eslabón en la cadena de protección y cada caso de estudio es una ventana a la resiliencia frente a las adversidades digitales.

Ética en la Inteligencia Artificial: Navegando por las Aguas Éticas del Ciberespacio.

En el cenit de nuestra travesía ética en el ciberespacio, es esencial reconocer que el temor hacia lainteligencia artificial y la tecnología a menudo se gesta no en sus capacidades intrínsecas, sino en elposible mal uso que las mentes humanas pueden hacer de estas herramientas poderosas. La tecnología y la inteligencia artificial representan una vanguardia en el progreso, capaz de transformar positivamente la sociedad, siempre y cuando su implementación se guíe por principios éticos sólidos.

La Dualidad de la Innovación Tecnológica: Hacia el Bien o el Mal

En este último tramo, nos enfrentamos a la dualidad de la innovación tecnológica: una fuerza que, enmanos éticas, puede forjar un futuro brillante, pero que, en manos irresponsables, podría desencadenarconsecuencias perjudiciales. Es crucial comprender que la inteligencia artificial y la tecnología en símismas no son entidades malévolas; es el uso que hacemos de ellas lo que determina su impacto en lasociedad.

Ciberseguridad y Marco Jurídico Comparativo: tratando que acompañe al avance de la tecnología.

En el complejo entramado del ciberespacio, la ciberseguridad no solo implica códigos y firewalls, sino

también un intrincado sistema legal que busca armonizar la protección de datos, la soberanía digital y la

colaboración internacional. Este capítulo sumerge al lector en un análisis detallado de cómo diferentes

países abordan las cuestiones legales asociadas con la ciberseguridad, ofreciendo una perspectiva más precisa y detallada.

Soberanía Digital y Cooperación Global: Un Dilema Legal

La soberanía digital, piedra angular en el ciberespacio , en si el mundo esta entrelazado, por tnto plantea un dilema jurídico y de copperacion entre países con leyes homogeneas.

Prevención vs. Respuesta: Estrategias Legales Integralmente Diseñadas

Más allá de establecer sanciones, las estrategias legales buscan crear un entorno propicio para laprevención de ciberataques. Desde regulaciones que exigen prácticas de seguridad estándar hasta lanotificación obligatoria de brechas de seguridad, este apartado destaca estrategias legales integrales que buscan anticipar, prevenir y mitigar los impactos de los ataques cibernéticos.Tejiendo Redes Globales: Tratados Internacionales y
Acuerdos Regionales

La cooperación internacional se consolida a través de tratados y acuerdos. Este segmento profundiza entratados como la Convención de Budapest y acuerdos regionales, mostrando cómo estas iniciativas buscan crear una red global de cooperación legal para abordar los desafíos de la ciberseguridad. Se citanejemplos concretos de cómo estas redes legales han influido en la lucha contra amenazas cibernéticas.

Desafíos Legales en un Mundo Digital en Constante Evolución

En el vertiginoso ciberespacio, las leyes deben adaptarse con agilidad. Este apartado explora lasestrategias adoptadas por diferentes países para legislar en un entorno digital en constante cambio. Desdeenmiendas rápidas hasta la creación de organismos especializados, se detallan las tácticas utilizadas paraasegurar que las leyes sigan el ritmo de la innovación tecnológica.

Desmitificando el Miedo: Educación y Transparencia.

El miedo generalizado hacia la inteligencia artificial y la tecnología a menudo se alimenta de la falta decomprensión y conocimiento. Enfrentar este temor implica desmitificar la tecnología, ofrecer educaciónsobre sus beneficios y riesgos, y fomentar la transparencia en su desarrollo y aplicación. La alfabetización digital y ética se erigen como escudos

contra la propagación infundada del miedo, empoderando a las sociedades para adoptar estas innovaciones con discernimiento.

La Responsabilidad Individual: Forjando un Futuro Ético

Cada individuo, desde el ciudadano común hasta el experto en tecnología, comparte la responsabilidad de moldear el camino ético de la inteligencia artificial. Fomentar la conciencia sobre las implicaciones éticas, promover discusiones abiertas y exigir responsabilidad a los desarrolladores y legisladores son pasos cruciales para asegurar que la tecnología y la inteligencia artificial se desplieguen en armonía connuestros valores y principios compartidos.

Conclusión:hacia un Futuro Ético.

En esta conclusión, miramos hacia adelante con esperanza y resiliencia. Si bien el temor hacia lainteligencia artificial persiste, reconocemos que su potenial para el bien supera con creces sus amenazas.Al abrazar la ética en el desarrollo y uso de la tecnología, trazamos un curso hacia un futuro donde la inteligencia artificial se convierte en una aliada en la mejora de la sociedad y la ciberseguridad.

Educación y Concientización en Ciberseguridad: Construyendo Resiliencia Digital

ES ALGO DESCONOCIDO. EL QUE DA CHARLA DE ESO. ESTA HABLANDO UN MUNDO QUE SE ESTA IMAGINANDO. NADIE LO SABE.

En el intrincado universo digital, la educación y la concientización en ciberseguridad emergen como piedras angulares, esculpiendo la resiliencia necesaria para individuos y empresas en la era digital.

Potenciando la Defensa Individual: Un Escudo Personal Contra Amenazas Digitales

La educación en ciberseguridad individual se convierte en un escudo personal contra las amenazas digitales en constante evolución. Exploramos a fondo conceptos clave, desde la creación de contraseñas robustas hasta la identificación de tácticas de phishing y la adopción de prácticas seguras en línea.

Ciberseguridad en la Educación: Forjando Futuros Protegidos

La educación en ciberseguridad no es solo un requisito actual, sino una inversión en el futuro.

Exploramos cómo la integración de la ciberseguridad en los programas educativos moldea mentes jóvenes capaces de navegar el ciberespacio de manera segura y ética. A través de iniciativas educativas innvadoras, resaltamos ejemplos que buscan construir una base sólida para la seguridad

digital desde una edad temprana. Construyendo una Sociedad Digitalmente Inquebrantable y resiliente.

La conclusión reflexiona sobre el papel crucial de la educación y concientización en ciberseguridad en la

construcción de una sociedad digitalmente inquebrantable. A medida que cada individuo y entidadempresarial se empodera con conocimientos sólidos, se traza un camino hacia un futuro donde la seguridad cibernética es un componente arraigado en el tejido mismo de nuestra sociedad digital.

Bienvenidos a la travesía educativa, donde el conocimiento es la mejor defensa. Un conocimiento que no controlamos.

Amenazas Cibernéticas en Diversas Plataformas: Estrategias de Defensa y Respuesta

En el complejo entorno cibernético, la proliferación de amenazas se extiende por diversas plataformas,desde dispositivos móviles hasta sistemas operativos de escritorio. Este análisis riguroso explora tácticasemergentes utilizadas por actores maliciosos y proporciona estrategias de defensa con enfoque técnicopara usuarios finales y desarrolladores.

Amenazas en Plataformas Móviles: Android e iOS

En el ámbito móvil, Android e iOS son susceptibles a amenazas específicas. En Android, la presencia deaplicaciones maliciosas en fuentes no oficiales y ataques de ransomware son preocupaciones persistentes.En iOS, técnicas de phishing y la introducción de malware son áreas de riesgo. Para mitigar estasamenazas, se deben aplicar prácticas de seguridad como la descarga de aplicaciones exclusivamente defuentes confiables y la implementación de software antivirus.

Desafíos en Sistemas Operativos de Escritorio: Windows, Ubuntu/Linux y Otros Sistemas operativos como Windows y Ubuntu/Linux enfrentan desafíos inherentes. En el caso deWindows, la propagación de virus a través de correos electrónicos maliciosos y sitios web comprometidos es una preocupación constante. En Ubuntu/Linux, aunque la vulnerabilidad es menor, los ataquespersisten, especialmente en entornos corporativos. Además, sistemas como Java y Python, a pesar de ser robustos, no son inmunes a amenazas, desmitificando la creencia en sistemas invulnerables.

Amenazas en el Mundo de la Programación: Lenguajes y Desarrolladores

Capitulo a los lenguajes e ingenieros. Para el publico que entienda lenguaje simple.

Explicación entendible de los lenguajes programación y son mas antiguos que las redes sociales que hoy dominan el mundo. Que paradoja!:

1. Java:

Java es como un maestro que enseña a las computadoras. Les dice qué hacer y cómo aprender cosas nuevas.

Java podría ser como el profesor que le enseña a la computadora a reconocer caras.

2. Python:

Python es como un traductor que ayuda a las computadoras a entender lo que queremos que hagan. Es muy bueno para enseñarles cosas nuevas.

Imagina a Python como el amigo que le explica a la computadora cómo reconocer comandos de voz. Así, la computadora puede entender lo que le decimos.

3. SQL:

SQL es como el detective que busca respuestas en la base de datos de la empresa. Le preguntamos cosas y él nos dice lo que encontró.

Usamos SQL como si fuera un detective para preguntar a la base de datos: '¿Cuántos productos vendimos esta semana?' y nos da la respuesta.

4. iOS (Swift):remplazo del ios objetive c.es o era mas reflexivo.

Swift es como el constructor de juguetes para el iPhone. Nos ayuda a hacer que las aplicaciones puedan entender y aprender cosas nuevas.

Con Swift, construimos una aplicación para el iPhone que puede reconocer diferentes colores. Swift es como el constructor que nos ayuda a hacer que el iPhone entienda colores.

Ingenieros de Sistemas y la Magia de la Inteligencia Artificial

La tecnología es como un cuento que cambia rápidamente. Vamos a hablar sobre cómo los ingenieros de sistemas son como los magos que hacen que las computadoras aprendan cosas mágicas.

De la Programación Tradicional a la Magia de la IA:

Antes, les decíamos exactamente a las computadoras qué hacer. Ahora, les enseñamos a aprender solitas. Por ejemplo, les enseñamos a reconocer rostros

Desafíos Actuales en la Tierra de la Tecnología:

Hoy en día, los ingenieros de sistemas tienen nuevos desafíos, como aprender a usar juguetes tecnológicos nuevos.

Plataformas Empresariales:

En lenguajes como Java, Python,swift,sql y otros, usamos magia (IA) para hacer que las empresas funcionen mejor. Podemos enseñarle a una computadora a tomar decisiones inteligentes.

Mantenerse al Día con los Hechizos Tecnológicos:

Es importante que los ingenieros de sistemas aprendan siempre cosas nuevas sobre magia tecnológica. Es como seguir las tendencias de moda, pero en el mundo de la magia de las computadoras.

Trabajo en Equipo: La Colaboración:

Trabajar juntos es clave, como cuando amigos se juntan para hacer algo increíble. El ingeniero solitario con una pizza y en medias, con cara de (no molestar) es del pasado.

La innovación es un esfuerzo conjunto; nunca es el resultado de una operación individual

Matt Mullenweg

Los desarrolladores se encuentran en la línea de frente de amenazas específicas, dependiendo del lenguaje de programación utilizado. En entornos web, ataques como inyección SQL y scripting entre sitios son comunes. La mitigación de estos riesgos implica la adopción de prácticas seguras de codificación y la utilización de frameworks seguros. La ciberseguridad se convierte así en un componente integral del ciclo de desarrollo.

17. LLM o Nuevo Lenguaje Grande Profundo:

Los modelos de lenguaje de gran tamaño (LLM) son modelos de aprendizaje profundo muy grandes que se preentrenan con grandes cantidades de datos. El transformador subyacente es un conjunto de redes neuronales que consta de un codificador y un decodificador con capacidades de autoatención.

Básicamente, las herramientas de BI se conectan a una base de datos empresarial y utilizan SQL para crear visualizaciones y desarrollar paneles de BI. Hay enormes empresas involucradas en este espacio: Tableau (propiedad de Salesforce), Power BI (propiedad de Microsoft), Looker (propiedad de Google) y QuickSight (propiedad de Amazon), por nombrar sólo algunas.

Y el tamaño del mercado para esto es grande. Según un informe , el tamaño del mercado mundial de inteligencia empresarial se valoró en 27,11 mil millones de dólares en 2022 y se prevé que crezca de 29,42 mil millones de dólares en 2023 y 54,27 mil millones de dólares en 2030. Gartner cree que podría ser aún mayor si la IA y los LLM se aplicaran más ampliamente. .

Sin embargo, los equipos de datos dedican mucho tiempo a crear estos paneles, especialmente para organizaciones grandes. Y siempre existe el desafío de lograr que las personas realmente los miren, una tarea difícil cuando los equipos de datos se quejan ante la idea de cumplir con solicitudes que podrían tardar días en desarrollarse.

una "capa conversacional", utilizando LLM en lenguaje natural, que se ubican en la parte superior del almacén de datos de una empresa. Traduce esas preguntas a SQL y genera automáticamente esas respuestas mucho más rápido. De modo que cualquiera, independientemente de sus habilidades técnicas o su contexto empresarial, puede hacer preguntas en inglés sencillo sobre sus datos y obtener información, afirma la empresa.

“Los consultores pasan de esperar dos semanas para obtener una información a 30 segundos. Eso significa que

hacen muchas más preguntas, utilizan mucho más los datos en su trabajo y los datos se convierten en algo que ahora está a su alcance".

Ese enfoque simplista no funciona para generar SQL preciso y, por lo tanto, respuestas correctas a preguntas sobre datos en el contexto de las herramientas de BI, afirmó: "A lo largo de 18 meses de trabajo, hemos podido construir un método para lograr la precisión de respuestas.

LA IMPORTANCIA DE LOS DATOS ESG EN LA INVERSION SOSTENIBLE. ESG Estas siglas vienen del inglés: Environmental, Social y Governance. En español hace referencia a los tres pilares en los que se tiene que basar el crecimiento.

La regulación ha jugado un papel fundamental en el impulso de la adopción de prácticas sostenibles por parte de las empresas. En Europa, se han implementado directivas y estándares que exigen a las compañías informar sobre su desempeño en términos de sostenibilidad. Esto ha llevado a un esfuerzo considerable para establecer un estándar mundial de reporte de datos ESG, tanto a nivel europeo como anglosajón.

Es importante tener en cuenta que los datos ESG no son un fin en sí mismos, sino una herramienta de análisis. La interpretación de estos datos es fundamental para comprender la complejidad de los desafíos medioambientales, sociales y de gobierno corporativo. La capacidad de analizar y valorar

correctamente estos datos es lo que permitirá a los inversores generar valor y tener un impacto real.

informaron que el cumplimiento de los requisitos regulatorios era la máxima prioridad (35%) para acceder a los datos ESG, seguido del cumplimiento de los objetivos de riesgo climático y cero emisiones netas (18%). Lo que potencialmente inhibe estas prioridades son los problemas de cobertura y calidad de los datos ESG informados por las empresas, que, como era de esperar, fueron citados por el 63% de los encuestados como su mayor preocupación. Con la entrada en vigor de la Directiva sobre informes de sostenibilidad corporativa (CSRD) en la UE, se espera que la cantidad y calidad de los datos ESG presentados por las empresas aumente en los próximos años. Sin embargo, con esta mayor disponibilidad, la necesidad de una integración y gestión fluidas de estos datos se volverá más apremiante, o se correrá el riesgo de ralentizar las decisiones de inversión.

Según la encuesta, el principal desafío de la gestión de datos ESG fue el manejo de contenidos de datos nuevos y en constante evolución (41%). Vincular el contenido de los datos ESG con los datos de entidades e instrumentos existentes fue el siguiente mayor desafío (25%), seguido del cumplimiento de los requisitos de presentación de informes (18%) y la gestión de múltiples fuentes de proveedores ESG (16%).

Defensa en el Ámbito Empresarial: Estrategias y Protocolos

En el contexto empresarial, caracterizado por redes heterogéneas, la defensa cibernética es

multidimensional. Desde la concientización del personal hasta la implementación de soluciones avanzadas, como firewalls y sistemas de detección de intrusos, la seguridad empresarial exige un enfoque proactivo. Políticas de seguridad robustas y respuestas rápidas ante incidentes constituyen elementos fundamentales.

No somos líderes para mantener el statu quo.
Somos líderes para crear el futuro

Elon Musk

Protegiendo al Usuario Final: Estrategias para Laptops y Smartphones

Los usuarios finales, ya sea en laptops o smartphones, deben adoptar medidas de seguridad proactivas. La actualización regular de sistemas operativos y aplicaciones, la instalación de software antivirus y laprudencia al interactuar con enlaces desconocidos son acciones fundamentales. La educación del usuario final se revela como un pilar esencial para establecer una defensa eficaz.

Conclusión: Navegando el Futuro Cibernético con Resiliencia

En resumen, el espectro de amenazas cibernéticas evoluciona de manera constante, exigiendo una comprensión profunda y estrategias de defensa

ajustadas. Desde el usuario final hasta el desarrollador y laempresa, la colaboración y la adaptabilidad son esenciales para afrontar con éxito el futuro cibernético.

Este viaje en la ciberseguridad destaca la importancia de la prevención como pilar inquebrantable, desmitificando la creencia en sistemas invulnerables y resaltando la necesidad de vigilancia continua.

Colaboración Global en Ciberseguridad: Consolidando un Frente Unificado

En el intrincado escenario cibernético mundial, la sinergia entre naciones emerge como un pilarfundamental para hacer frente a las amenazas digitales. Este minucioso análisis se sumerge en lasiniciativas y esfuerzos colaborativos, explorando estrategias conjuntas para abordar desafíos críticos enciberseguridad a nivel global.

Iniciativas Estratégicas: Fortaleciendo la Defensa Global

Ante la ausencia de fronteras digitales, la ciberseguridad exige iniciativas estratégicas que trasciendanlímites geográficos. Acuerdos de intercambio de información, protocolos de respuesta conjunta ysimulacros internacionales se revelan como herramientas esenciales. Este análisis destaca las mejoresprácticas, evidenciando cómo

estas alianzas refuerzan las defensas cibernéticas colectivas.

Esfuerzos Conjuntos y Lecciones Aprendidas: Modelando la Excelencia ColaborativaLa exploración va más allá de las alianzas formales, sumergiéndose en esfuerzos conjuntos que handejado una huella significativa. Lecciones aprendidas de incidentes previos, como ataques cibernéticos agran escala, proporcionan una visión valiosa sobre la efectividad de la colaboración internacional.Comprender cómo distintas naciones abordan las amenazas cibernéticas revela estrategias adaptables yperfeccionables.Desafíos y Oportunidades: En el Terreno InternacionalLa colaboración global en ciberseguridad enfrenta desafíos, desde la armonización de marcos regulatorios hasta la gestión de expectativas entre naciones. Este análisis explora estos desafíos y, al mismo tiempo, señala oportunidades emergentes para fortalecer la colaboración, como la participación activa en organismos internacionales dedicados a la ciberseguridad.

En resumen, la colaboración internacional no solo es una necesidad estratégica, sino el fundamento para abordar las complejidades del ciberespacio. Este examen detallado resalta cómo trabajar en conjunto no solo fortalece las defensas cibernéticas, sino que también establece un marco para enfrentarcolectivamente los desafíos futuros. En un

mundo digitalmente interconectado, la colaboración global nos da una red sólida para salvaguardar la seguridad cibernética en la era moderna.

Impacto Global de la Tecnología: La Odisea Interconectada

En la era actual, asistimos a una asombrosa epopeya de interconexión tecnológica que abarca cada rincóndel globo. No solo estamos contando celulares y midiendo la expansión de Internet, estamos presenciandouna transformación radical en la forma en que el mundo se comunica, aprende y se conecta. En esta travesía, exploraremos más allá de los fríos números para sumergirnos en la trama de desafíos yoportunidades que esta revolución digital global nos presenta, especialmente en el fascinante terreno de la ciberseguridad.

La Multitud de Dispositivos: Más que un Recuento

En nuestra vida cotidiana, la multitud de dispositivos tecnológicos se entrelaza de manera inextricable.

Más allá de la frialdad de los números, nos sumergimos en un panorama donde cada gadget, desde el

teléfono en nuestra mano hasta los dispositivos inteligentes en nuestros hogares, contribuye a la

complejidad de la trama tecnológica. Este análisis invita a reflexionar sobre cómo esta profusión de

dispositivos redefine nuestra experiencia diaria y plantea interrogantes desafiantes para la seguridad

digital.

La Expansión de Internet: Un Viaje Digital sin Fronteras y sin retorno.

El viaje de la expansión de Internet no es solo geográfico, es una travesía sin fronteras que conecta acomunidades distantes y culturas diversas. No obstante, este relato también desentraña las complicaciones emergentes. Desde la ciberdelincuencia hasta las complejidades de la privacidad, la red global que une al mundo presenta desafíos únicos. Exploramos cómo esta conexión, aunque abra oportunidades ilimitadas, también presenta un terreno fértil para desafíos en la ciberseguridad.

Impacto en la Ciberseguridad: Entre Sombras y Luces.

En la narrativa de la ciberseguridad, la proliferación de dispositivos y la expansión de Internet dan formaa un drama en constante evolución. No solo se trata de cifras asombrosas, sino de la intersección entredesafíos y oportunidades. Este análisis detalla cómo la multiplicidad de puntos de acceso digital planteadesafíos significativos, desde la gestión de

vulnerabilidades hasta la necesidad de estrategias defensivasmás sofisticadas. A su vez, ilumina oportunidades para la innovación y la colaboración en la protecciónde nuestra narrativa digital compartida.

Visión de Futuro: Navegando Hacia la Ciberseguridad del Mañana

En el cierre de este compendio, se alzan voces diversas desde campos tan variados como la cibernética, la informática, la filosofía y la sociología para ofrecer una perspectiva holística sobre el futuro de la ciberseguridad.

La inteligencia artificial será la electricidad del siglo XXI

Andrew Ng

La ciberseguridad es crucial para la supervivencia y el éxito continuo de las empresas en nuestra era digital

Satya Nadella

En la era de la información, los desafíos de seguridad son como corrientes cambiantes. Anticipamos lanecesidad de estrategias adaptables para afrontar lo inesperado."_ Dra. Laura Ramirez, CiberanalistaLos desafíos no solo vendrán de ataques externos, sino de la complejidad creciente de nuestras

propiastecnologías. La gestión eficaz será clave."
Prof. Carlos Fernández, Experto en Sistemas de SeguridadInnovaciones Transformadoras:

Nuevos Horizontes en Protección Digital"La inteligencia artificial y la cuántica serán aliadas poderosas, pero debemos recordar que la seguridadreside en la comprensión humana y la ética digital." Dr. María Sánchez, Pionera en Tecnologías Cuánticas

La colaboración internacional es la nueva frontera. Solo unidos, con estándares compartidos, podremosconstruir una defensa global."_ Ing. James Foster, Ciberexperto Internacional

La ciberseguridad no es solo un conjunto de protocolos; es una filosofía de protección en constanteevolución. Debemos abrazar el cambio y la responsabilidad individual."_ Dr. Sofia Mendez, Filósofa de la Ética Digital

En esta travesía digital, la resiliencia es clave. La adaptabilidad y la mentalidad de aprendizaje constantemarcarán la diferencia." Coach Emma Thompson, Experta en Desarrollo Profesional

En este cierre, estas visiones de personas en diferentes áreas convergen para recordarnos que el

futuro de la ciberseguridad no solo depende de la tecnología, sino de nuestra capacidad colectiva para abrazar la innovación, comprender las implicaciones éticas y colaborar en la protección de nuestra sociedad digital.

Si bien estamos asustados con la inteligencia artificial(IA).

Cuando llegue la evolución de la IA , ya esta la AGI. No sé qué decirles.

La evolución de la inteligencia artificial que conocemos hoy día, AGI (Inteligencia Artificial General). "Una vez que lleguemos a la AGI a nivel humano, en pocos años podríamos estar en una AGI radicalmente superhumana", añadió Goertzel. "Creo que una vez que una AGI pueda introspectar su propia mente, podrá hacer ingeniería y ciencia a nivel humano o superhumano, generando una explosión de inteligencia que puede superar incluso lo que pensaba el científico informático Ray Kurzweil." La urgente necesidad de salvaguardias antes de abrir la caja de Pandora, ya que aún no hemos comprendido completamente. Si la singularidad está tan cerca como sugiere, hay una gran presión para hacer las cosas bien y rápido.

En realidad no hay tanto antivirus para tanto aparatos y electrodomésticos que hay hoy en día en (el internet de las cosas). Ni para las actualizaciones que esto mismo deben tener frecuentemente. Lo que se están abocando es crear un mercado de consumo más agresivo más masivo.

Hasta hace poco hablábamos mucho de 5G, pero ahora todo es IA. ¿Cómo cambia esto?

Un hecho: en este momento, el PIB mundial anda por los 100 billones. Nuestras

estimaciones son que la IA generativa puede agregar 10 billones de dólares nuevos al PIB mundial, algo espectacular desde una perspectiva de crecimiento. Creemos que si los operadores son capaces de adoptar la IA, pueden modernizar y monetizar sus redes mediante una combinación de software en la nube y la propia IA generativa.

Además el 5g para cientos de miles de nuevos equipos y marcas, generando un nuevo consumismo. No sobra decir que no hay tantos antivirus y actualizaciones que se puedan manejar con el internet de la cosas. cuando ya salió el nuevo artículo.

Más grandes las computadoras, más datos utilizamos para entrenarlos. Y a medida que afinamos los algoritmos, se vuelven más inteligentes.