REPÚBLICA DE CUBA
MINISTERIO DE COMUNICACIONES

Boletín *Novedades TIC*

Junio 2019

Contenido

Sistema de Vigilancia Tecnológica

Ministerio de Comunicaciones

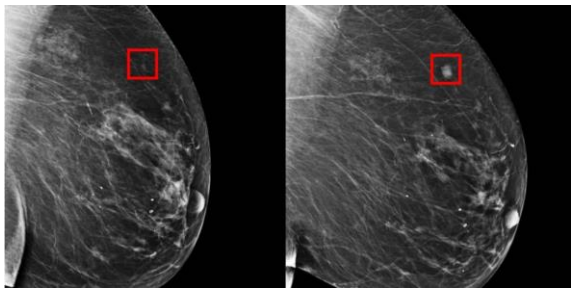
Junio, 2019

INTELIGENCIA ARTIFICIAL

1. MIT CREA IA QUE PREDICE HASTA CON CINCO AÑOS EL CÁNCER DE MAMAS

Fecha: 26/06/2019

El Laboratorio de Inteligencia Artificial y Computación del MIT creó un modelo de predicción que detecta tempranamente el cáncer de mamas.



El MIT a través de su Laboratorio de Inteligencia Artificial y Computación, creó una IA impresionante que logra detectar hasta con cinco años de anticipación el cáncer de mamas.

Además una de las mayores innovaciones es que esta tecnología funciona igual de bien tanto para mujeres blancas como para las de raza negra, ya que se ha demostrado que estos algoritmos en IA también tienen sesgos importantes.

Entrenado en mamografías y resultados conocidos de más de 60,000 pacientes con MGH, el modelo aprendió los patrones sutiles en el tejido mamario que son precursores de tumores malignos, sostiene el MIT.

Cómo el MIT detecta el cáncer de mamas

La profesora de Harvard, Constance Lehman, explica cómo funciona el sistema.

"Desde la década de 1960, los radiólogos han notado que las mujeres tienen patrones únicos y ampliamente variables de tejido mamario visibles en la mamografía. Estos patrones pueden representar la influencia de la genética, las hormonas, el embarazo, la lactancia, la dieta, la pérdida de peso y el aumento de peso. Ahora podemos aprovechar esta información detallada para ser más precisos en nuestra evaluación de riesgos a nivel individual ".

Pero quizás lo que más se destaca es que esta IA es útil para la detección del cáncer de mamas tanto para mujeres de raza blanca como de raza negra, que ya tienen una prevalencia de 42%.

Es particularmente sorprendente que el modelo funcione igual de bien para las personas blancas y negras, lo que no ha sido el caso con herramientas anteriores", dice Allison Kurian, profesora asociada de medicina / investigación / política de salud de la Escuela de Medicina de la Universidad de Stanford. "Si se valida y se pone a disposición para un uso generalizado, esto podría mejorar realmente en nuestras estrategias actuales para estimar el riesgo".

Disponible en:
https://www.fayerwayer.com/2019/06/mit-ia-cancer-mamas/?fbclid=IwAR0ZhrTuIWr0OzVG5NPDfuwbgcHh7oeqx5lGh9TfDnOWHPgxAVclN6MPcSw

2. LA INTELIGENCIA DE BAJO NIVEL LLEGA A LOS ROBOTS, UN CHIP PARA QUE TENGAN IMAGINACIÓN

Fecha: 24/06/2019

Ingenieros han logrado dar con la clave para que los robots sean más inteligentes, al menos con una pequeña porción de imaginación para que puedan calcular mejor sus movimientos.

En un entorno donde los seres humanos y los robots viven casi juntos realizando algún tipo de trabajo como puede ser en una cadena de montaje, tanto las máquinas

como los trabajadores no pueden estar trabajando muy cerca unos de otros para evitar accidentes.

Los avances en inteligencia artificial están haciendo que cada vez se difumine más esa barrera que existe entre los trabajadores y los robots para que puedan trabajar en mejor armonía, colaborando unos con otros y haciendo que la tasa de accidentes sea prácticamente inexistente.

Ahora un nuevo procesador fabricado por Realtime Robotics permite que los robots puedan planear rápidamente sus próximos movimientos para mantener así a los humanos totalmente seguros. Esta Startup, ubicada en Boston, parece que ha dado con la tecla de algo que ya estaban buscando otras tantas compañías de ingeniería desde hace tiempo. Desde Realtime Robotics están tratando de darle a los robots el tipo de inteligencia de bajo nivel necesaria para moverse en un entorno de trabajo junto a humanos.

Gracias a este chip, al conectarse a los sensores 3D de los robots, permite a las máquinas considerar distintos efectos diferentes en todo su rango de movimientos, imaginando previamente el resultado antes de elegir la acción que mejor se adapte a la tarea en cuestión.

De esta manera, con este procesador en un brazo robot en una cadena de montaje, el brazo antes de moverse hacia el lado derecho para dejar una pieza, podrá optar por frenarse o bien realizar un movimiento distinto si los sensores localizan la presencia de un ser humano en mitad del camino.

El chip es capaz de sobrecargar los cálculos matemáticos con un algoritmo de planificación de movimiento desarrollado por Konidaris y otros investigadores mientras estaba en la Universidad de Duke en Estados Unidos. Al ir ejecutando los cálculos en paralelo, el procesador puede realizar los movimientos más de 10.000 veces más rápido que un chip de un ordenador normal.

Este avance no ha pasado desapercibido para multitud de fabricantes de brazo robóticos, que ya está utilizando la tecnología de Realtime Robotics.

Disponible en:
https://computerhoy.com/noticias/tecnologia/inteligencia-nivel-llega-robots-chip-tengan-imaginacion-444037

3. 3 USOS MÁS COMUNES DE LA INTELIGENCIA ARTIFICIAL EN RECURSOS HUMANOS

Fecha: 24/06/2019

Desde la consultora Gartner han identificado los tres casos de uso más comunes de la Inteligencia Artificial en el terreno de los Recursos Humanos y los procesos de selección personal en las empresas.

Al igual que en otros terrenos tan múltiples y dispares como la salud, el comercio o las finanzas, la Inteligencia Artificial implica jugosas oportunidades para que las empresas mejoren la experiencia de los empleados y logren que los departamentos de Recursos Humanos sean más eficaces, valiéndose para ello de algoritmos cada vez más sofisticados, machine learning, o el poder del Big Data.

Desde la consultora Gartner recalcan que el 23% de las organizaciones que ya estaban probando de forma piloto o utilizando Inteligencia Artificial, lo estaban haciendo en el área de Recursos Humanos y reclutamiento de personal “en áreas como la gestión del talento, la prestación de servicios de recursos humanos y la gestión de la fuerza laboral”, tal y como reveló Helen Poitevin, vicepresidenta de investigación de la compañía.

Lo habitual es que la IA se demuestre en el dominio de Recursos Humanos tras demostrar valor en otras áreas de negocios. Gartner destaca en un informe reciente los tres casos más comunes de uso de la IA en RRHH y reclutamiento.

Captación de talento

En los medios suelen aparecer noticias relativas al sesgo discriminatorio de los algoritmos o al temor de que estos asuman todo el proceso de contratación. “Reconocemos que ninguno de los proveedores de tecnología u organizaciones que buscan aplicar la inteligencia artificial en el dominio de reclutamiento persiguen tal objetivo”, afirmó. Poitevin.

Desde Gartner explican que los reclutadores que usan IA comienzan analizando el mercado laboral, identificando competencias, detectando habilidades y captando sesgos en las descripciones de puestos y la clasificación de candidatos. Los reclutadores de recursos humanos emplean los chatbots para programar citas o responder preguntas comunes.

Las organizaciones con un gran volumen de candidatos, o aquellas que luchan por encontrar especialistas u otros perfiles raros, probablemente inviertan en tecnologías de IA, que podrán analizar e interpretar las respuestas de los candidatos, así como predecir el grado de ajuste y el rendimiento de los candidatos para las vacantes actuales. También desempeñarán tareas administrativas repetitivas.

Monitorización del compromiso a través del análisis de voz

El análisis de Voice of the employee (VoE) es la segunda área de dominio más popular que atrae a los departamentos para analizar el compromiso de los empleados. Desde Gartner ponen el ejemplo de una organización que pudo descubrir que una caída en el compromiso de un grupo de empleados en realidad se debía a problemas con el uniforme de trabajo, algo que podía solucionarse de forma directa y sencilla. “Esto ayudó a la organización a evitar el desgaste innecesario, costoso e indeseado”, subrayan.

En lugar de confiar únicamente en las encuestas, los líderes de recursos humanos también están interesados en detectar, analizar e informar sobre el sentimiento y las actitudes expresadas a través de más canales de comunicación de los empleados. Por ejemplo, pueden ver los feeds de redes sociales de los empleados, o las conversaciones y comentarios en las herramientas de colaboración internas.

El objetivo es identificar de qué hablan los empleados de manera positiva o negativa, así como los temas que se mencionan con mayor frecuencia. Otro punto clave destacado por Gartner del uso de la IA en

este ámbito es seguimiento de la salud de su cultura corporativa.

Las herramientas modernas de VoE que aprovechan las tecnologías de inteligencia artificial utilizan una variedad de técnicas de procesamiento de lenguaje natural y análisis textual para analizar actitudes y obtener información de las respuestas basadas en texto. Esto puede ser especialmente útil en tiempos de cambios significativos, como una reestructuración importante, un nuevo liderazgo o una nueva estrategia corporativa.

Asistentes virtuales de Recursos Humanos

Los asistentes virtuales de recursos humanos todavía se encuentran en una etapa de adopción temprana. Sin embargo, la expectativa es que podrá existir una interfaz única para cada proceso de RRHH imaginable -como responder a las consultas de los empleados, brindar información sobre las métricas de talento o realizar los pasos del flujo de trabajo del proceso-.

Por el momento uno de los usos más significativos es el de los chatbots para centros de contacto de atención al cliente. Las compañías que los han implementado se han caracterizado por una fuerte adopción por parte de los empleados.

Disponible en:
https://www.ticbeat.com/innovacion/3-usos-mas-comunes-de-la-inteligencia-artificial-en-recursos-humanos/

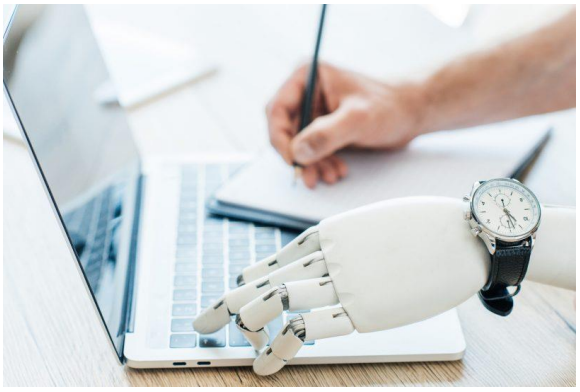
4. GHOSTWITER, LA IA QUE PILLARÁ A LOS ALUMNOS QUE COPIEN EN LOS EXÁMENES

Fecha:19/06/2019

La tradición de hacer trampa en los exámenes podría estar a punto de llegar a su fin.

La Universidad de Copenhague, en Dinamarca, ha desarrollado un software de inteligencia artificial que detecta quién ha copiado en los examenes, con una probabilidad de acierto del 90%.

Según una encuesta llevada a cabo entre 70.000 alumnos de instituto en Estados Unidos el año pasado, el 95% de los alumnos reconocía haber hecho trampas en los exámenes de una forma u otra. El 58% confesaba haber copiado alguna vez.



Cuando un alumno copia a otro durante el examen, o incluso envía a otra persona en su lugar para hacer la prueba, a veces el profesor detecta algo raro (dos textos que se parecen mucho, un estilo de escritura muy diferente), y acaba pillando al tramposo.

Pero en clases con docenas de alumnos o si un profesor lleva a varias clases, este trabajo de detective es muy complicado. Por eso la Universidad de Copenhague ha diseñado Ghostwriter, una inteligencia artificial que descubre a los alumnos que copian en los exámenes. Ghostwriter ha sido entrenada durante años analizando los textos de 130.000 exámenes de alumnos daneses.

Es capaz de detectar cuándo un alumno copia a otro durante el propio examen, o cuándo otra persona ha escrito el examen, ya sea porque ha suplantado al alumno que debería hacer la prueba, o porque el alumno

ha conseguido las respuestas antes del propio examen.

Ghostwriter utiliza un red neural que analiza patrones de un texto: errores ortográficos y gramaticales, longitud y estructuras de las frases, uso de coletillas, palabras favoritas, o frases hechas, y las compara con los exámenes, trabajos o textos remitidos por los alumnos. Así puede saber si un alumno ha copiado a otro, o si un texto que ha presentado es suyo o no, porque tiene un estilo diferente.

La Universidad de Copenhague asegura que Ghostwriter, la inteligencia artificial que detecta las trampas en los exámenes, detecta a los tramposos con un porcentaje de acierto del 90%. Aún así reconoce que este software no debe usarse para acusar, sino como indicio de trampa para que los profesores investiguen si es cierto o no.

Además de convertirse en la pesadilla de los estudiantes, Ghostwriter ya se está probando en otras actividades similares, como detectar documentos falsos, o descubrir si los tuit o mensajes de las redes sociales han sido escritos por un bot, o una persona real.

Disponible en:
https://www.ticbeat.com/tecnologias/ghostwriter-la-ia-que-pillara-a-los-alumnos-que-copien-en-los-examenes/

5. LA HERRAMIENTA DE INTELIGENCIA ARTIFICIAL QUE REVOLUCIONA LA ATENCIÓN AL CLIENTE

Fecha: 05/06/2019

Es el caso de las compañías de servicios públicos y de telecomunicaciones quienes enfrentan una serie de retos relacionados con sus procesos de transformación digital, en gran medida impulsados por una nueva generación de clientes quienes han crecido usando tecnologías digitales.

Algunos de estos retos se desprenden de las exigencias de los nuevos usuarios quienes son mucho más exigentes en lo que se refiere a calidad de servicio, pero sobre todo a los tiempos de atención a sus quejas y solicitudes.

Con el objetivo de sortear con éxito estos desafíos, cada vez más organizaciones recurren al uso de soluciones digitales basadas en tecnologías como la inteligencia artificial.

Una de ellas son los chatbots, un programa que incorpora elementos de inteligencia artificial, adoptando funciones cognitivas humanas para establecer conversaciones con una persona y brindar respuestas automáticas a los mensajes y solicitudes hechos por el usuario.

Este tipo de herramientas emplean un lenguaje natural, lo que da como resultado una comunicación fluida e inmediata, y contribuye a crear métodos de atención más interactivos, especializados y ágiles, que a su vez estimulan el aumento en la satisfacción del cliente y, por ende, el uso recurrente de este tipo de herramientas.

Cuatro ventajas que ofrecen los chatbots en los procesos de atención al cliente

Brindan experiencias personalizadas y responden ágilmente a las solicitudes, necesidades e inquietudes de los usuarios.

Contribuyen a la optimización de las labores relacionadas con la atención a los usuarios

y permiten focalizar los esfuerzos del personal de la compañía en la gestión de requerimientos o situaciones más complejas.

Impulsan la relación con el cliente gracias a la inmediatez con la que se gestiona su requerimiento y al amplio conocimiento que tiene la empresa sobre sus necesidades, preferencias y hábitos.

Simplifican la programación de citas y la resolución de dudas de los clientes relacionadas con los productos, iniciativas o servicios que ofrecen las compañías.

El uso de herramientas como los chatbots, viene marcando un hito importante en la implementación de estrategias de atención al cliente que múltiples organizaciones desarrollan con el fin de diversificar sus canales de atención y darle un manejo más efectivo a los altos flujos de Peticiones, Quejas y Reclamos (PQRs).

Debido a la efectividad y alta demanda que están teniendo herramientas como los chatbots, el IDC (International Data Corporation), estima que para 2020 la inteligencia artificial alcanzará un mercado de 47 mil millones de dólares, lo cual representa una tasa de crecimiento anual del 55%.

Al respecto, Jesús Sánchez, Vicepresidente de Mercadeo de Open, aseguró que "la adopción de esta tecnología resulta fundamental para la industria de las utilities y de las telecomunicaciones, ya que representa una gran estrategia de fidelización de clientes y optimización del recurso humano. Los chatbots brindan un conocimiento más profundo del cliente y sus necesidades a través de un diálogo rápido, concreto y hábil"

Disponible en:
https://www.tynmagazine.com/la-herramienta-de-inteligencia-artificial-que-revoluciona-la-atencion-al-cliente/

SEGURIDAD INFORMÁTICA

1. SEGURIDAD Y PRIVACIDAD EN LA INTERNET DE LAS COSAS: ¿A DÓNDE VAN NUESTROS DATOS?

Fecha: 26/06/2019

Así es la seguridad y la privacidad en la era del Internet de las Cosas. Este artículo analiza los factores de los que dependen y cómo nos comunicamos con dispositivos conectados.

El escándalo de Cambridge Analytica ha mostrado el peligro de la recopilación masiva y la agregación de información. La empresa utilizó datos obtenidos de diferentes fuentes, entre los que se incluían los de millones de usuarios de Facebook, para enviar publicidad dirigida e influir así en las elecciones de Estados Unidos. Los obtuvo de forma fraudulenta a través de esta plataforma social con la que los usuarios interactúan y con la que comparten conscientemente información personal.

Hasta cierto punto, nos preocupa de la información que tenemos en redes sociales. Elegimos contraseñas decentes y protegemos con antivirus nuestros móviles y ordenadores. Al menos, aquellos aparatos con apariencia de ordenadores.

En los últimos años, ha surgido un creciente número de dispositivos (termómetros, cámaras, alarmas, etc.) equipados con sensores y otros elementos tecnológicos que nos permiten monitorizar y controlar todo lo que ocurre en el hogar. Podemos obtener la información que recogen y actuar desde un smartphone sin necesidad de estar en casa, de manera remota. Esto

implica, por supuesto, que estos dispositivos pueden comunicarse a través de la Red, dando origen al término internet de las cosas o IoT (Internet of Things).

¿Cómo nos comunicamos con esos dispositivos?

El primer problema de seguridad en estos dispositivos es precisamente ese: que los vemos únicamente como cosas. Pero un dispositivo capaz de comunicarse a través de internet es un ordenador.

Aunque esté metido en una caja pequeña sin pantalla ni cables, tiene los mismos problemas de seguridad que un ordenador. A eso se añade que, al no interactuar directamente con el dispositivo, no nos damos cuenta de si le pasa algo raro. No vemos si da mensajes extraños de error o si "va lento".

Para comunicarnos con estos dispositivos IoT, podríamos usar varios mecanismos. Lo más natural sería pensar que, cuando estamos fuera, podríamos utilizar una aplicación móvil para comunicarnos con el dispositivo que está en casa: el smartphone obtendrá así la información que ofrece el dispositivo (por ejemplo, la temperatura) o bien le dará las órdenes correspondientes (por ejemplo, encender la calefacción).

Todo ello protegido por el correspondiente intercambio de información de autenticación (códigos de verificación, contraseñas, etc.) para impedir que pueda ser controlado por cualquiera.

Sin embargo, hoy en día, las redes residenciales no permiten usar este mecanismo. Se utilizan direcciones IP privadas (direcciones IP que identifican cada aparato dentro de la red doméstica) y dispositivos NAT en el router para conectarse a internet a través de una IP pública. Estos únicamente permiten que se establezcan comunicaciones desde la red de casa hacia el exterior: la información puede fluir en los dos sentidos, pero lo que llamamos conexión solo puede iniciarse desde el interior (red doméstica) hacia el exterior

Por eso, los fabricantes de la mayoría de dispositivos IoT en venta deciden utilizar un segundo mecanismo de comunicaciones. Los dispositivos de casa inician la comunicación con servidores en la nube (perteneciente al fabricante del dispositivo), que actúan como pasarela a internet. De esta forma, nuestros dispositivos le informan de las medidas que realizan y se mantienen en contacto por si deben recibir órdenes.

Esta comunicación funciona porque la inician los dispositivos desde nuestra red doméstica hacia el exterior. El usuario que está fuera de casa puede acceder al servidor a través de su móvil y consultar los datos de sus dispositivos o incluso darles órdenes. El servidor reenvía las órdenes a los aparatos dentro del hogar y permite consultar la información que ha recibido de ellos.

Este mecanismo es cómodo y permite vender dispositivos listos para usarse con poca configuración, pero a costa de que los datos de nuestros sensores y el acceso al control de nuestra casa estén en manos de un intermediario. Estos intermediarios serán el blanco de ataques y filtraciones.

Comunicaciones sin intermediarios

La alternativa será utilizar tecnologías que permitan comunicarnos con los dispositivos sin utilizar intermediarios. Esa es una de las ventajas de la siguiente versión del protocolo IP, la versión 6 (IPv6), que no acaba de despegar. Quizá la proliferación de dispositivos de IoT sea la que genere el impulso definitivo para que los operadores ofrezcan conectividad con IPv6, permitiendo utilizar direcciones IP públicas en las redes residenciales y facilitando la comunicación sin intermediarios.

En este escenario, será fundamental vigilar la actividad y los flujos de comunicación en las redes residenciales. La monitorización de este tipo de tráfico es una de las líneas de investigación del Grupo de Redes, Sistemas y Servicios Telemáticos del Instituto de Smart Cities (ISC) de la Universidad Pública de Navarra (UPNA).

Mientras no aparezcan estas soluciones, debemos ser conscientes de que la información de nuestro hogar es manejada por las empresas que proporcionan los dispositivos que usamos. No debemos pensar que estamos comprando una cámara conectada, sino que estamos contratando el servicio de que alguien vigile.

Incluso aunque no tengamos una cuota que pagar y, de hecho, nadie vigile las imágenes que sacamos, el almacenamiento es un servicio. Los datos de la cámara estarán en la nube (o sea, los servidores) de la empresa que vende el dispositivo y su protección depende en parte de esa empresa. Así que debemos elegir empresas de confianza y, al menos, informarnos de lo que nos prometen que harán o no harán con nuestros datos.

La seguridad depende de nosotros

Pero la protección del acceso a los datos depende también de nosotros. Deberemos seguir las buenas prácticas para cualquier sistema web que almacene información privada, como configurar una identidad eligiendo bien la contraseña y no reutilizar la contraseña de otra página para evitar que se pueda averiguar a partir de filtraciones de otros sitios menos seguros.

En caso de duda, los gestores de contraseñas de los sistemas operativos o independientes, como 1password, nos permiten generar contraseñas diferente para cada sitio y no perderlas. Elegir la misma contraseña para el acceso a los dispositivos que monitorizan nuestra casa que la que estamos usando en cualquier pagina web es igual de sensato que dejar la llave debajo del felpudo porque a nadie se le va a ocurrir mirar ahí…

Disponible en:
https://www.ticbeat.com/seguridad/seguridad-y-privacidad-en-la-internet-de-las-cosas-a-donde-van-nuestros-datos

2. INVESTIGAN A YOUTUBE POR NO PROTEGER LA PRIVACIDAD DE LOS NIÑOS

Fecha: 26/06/2019

YouTube bajo la lupa de nuevo por no hacer lo suficiente para proteger a los niños.

No es la primera vez que YouTube está en el centro de la polémica por algún caso relacionado con menores de edad. No en los últimos años. Y es que, todo lo que tenga que ver con niños hay que tratarlo con

pies de plomo, cosa que no parece estar haciendo la responsable de esta plataforma, que no es otra que Google.

Hace algún tiempo ya que el gobierno de los Estados Unidos, a través de la FTC (Comisión Federal de Comercio), está investigando la gestión que hace YouTube de su plataforma de vídeos. Así lo ha informado, al menos, a The Washington Post.

En los últimos tiempos han llegado quejas por el hecho de que YouTube no esté haciendo todo lo que está en sus manos para proteger a los pequeños que hacen uso del servicio. Creen, por otra parte, aunque no menos grave, que YouTube ha ido recopilando información sobre los usuarios, es decir, los niños, de una manera incorrecta. Y esto no viene de ahora: las investigaciones se remontan a 2015.

YouTube y YouTube Kids podrían estar incumpliendo las normas

La FTC parte de la hipótesis de que tanto YouTube como YouTube Kids están incumpliendo de manera sistemática las leyes federales en lo que respecta a la gestión de los contenidos que ofrecen a niños. Sabemos que la cuestión está directamente relacionada con la privacidad de los más pequeños y que esta ha sido previamente denunciada por varios usuarios – probablemente familias – desde hace tiempo.

De ahí que la FTC iniciara las investigaciones de las que hoy estamos hablando. Y aunque todavía se desconocen los detalles, es evidente que estaríamos ante un asunto de carácter grave, por el que YouTube pagará las consecuencias.

La fuente de toda esta historia ha confirmado que las investigaciones se encuentran ya en etapas muy avanzadas y que pronto podríamos conocer sus pormenores, así como el acuerdo o la multa que pueda determinar el organismo que investiga el caso.

Las medidas que ha tomado (y podría tomar) YouTube

Es evidente que una multa no solucionará las cosas. Y aunque es un correctivo muy interesante, la parte más interesante de la resolución a este problema llegará a través de las iniciativas que pueda poner en marcha YouTube para proteger a los más pequeños.

En los últimos tiempos ya hemos visto algunas. Por ejemplo, en estos momentos ya no se pueden hacer comentarios en los vídeos en los que aparecen niños. Tampoco se pueden realizar directos en los que salgan menores, a no ser que estén acompañados por adultos.

Además, es posible que dentro de poco, también puedan incluirse otras mejoras. Algunas podrían tener que ver directamente con el algoritmo de YouTube a la hora de recomendar nuevos vídeos para ver. Otra opción que los directivos de la plataforma están estudiando es la de pasar todos, absolutamente todos, los vídeos de niños y para niños a YouTube Kids, dejando la plataforma para “adultos” sin todos estos contenidos.

Sin embargo, este cambio tan importante podría dejar muy tocada a YouTube. La plataforma perdería de este modo una

oportunidad muy suculenta de obtener ingresos. He aquí una de las principales razones por las que no lo hace (por lo menos de momento). Pero es que además, la cantidad de vídeos a mover de un lado a otro sería verdaderamente ingente y difícil de clasificar. No en vano, hay muchos contenidos que pueden ser aptos para niños, pero que también lo son para adultos. Ahora mismo estamos pensando, por ejemplo, en lo dibujos de La Pantera Rosa clásicos, a los que pequeños y mayores pueden quedarse pegados del mismo modo.

Sea como sea, YouTube no ha querido dar ninguna explicación al respecto, por el momento, indicando que, como siempre, están pensando en iniciativas nuevas para mejorar la plataforma.

Disponible en:
https://www.tuexperto.com/2019/06/20/investigan-a-youtube-por-no-proteger-la-privacidad-de-los-ninos/

3. SI USAS FIREFOX, QUIZÁS ESTÉS EN PELIGRO: DESCUBREN UN FALLO QUE AFECTA A MILES DE PCS

Fecha: 19/06/2019

Las actualizaciones pueden ser muy molestas a la hora de descargarlas pero suelen ser un recurso imprescindible para bloquear la entrada a nuestros dispositivos a los ciberdelincuentes. Por eso, Mozilla ha pedido a todos sus usuarios que actualicen lo antes posible su navegador Firefox a la última versión disponible.

Firefox se enfrenta a un fallo de seguridad importante que está poniendo en riesgo los ordenadores de algunos usuarios. Esta vulnerabilidad se instaló en los PCs de cientos de clientes de Mozilla con el lanzamiento de Firefox 67.0.

La nueva actualización contenía un error en el código que ha estado permitiendo que los piratas informáticos accedieran a aquellos ordenadores que ejecutaban la nueva versión 67.0 sin el parche de seguridad que inmediatamente después lanzó Mozilla.

Nada más descubrir el bug, la compañía lanzó Firefox 67.0.3 para corregir el error de seguridad y publicó un aviso pidiendo a sus usuarios que actualicen sus navegadores cuanto antes. El problema ha sido tan grave que hasta la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos emitió una alerta pidiendo la actualización de todos los sistemas.

Gracias a este error de seguridad que se conoce como CVE-2019-11707, los atacantes pueden inyectar su propio código y controlar el ordenador a través de webs maliciosas si el usuario las visita con Firefox cuando aún no ha instalado el parche de seguridad de la última versión disponible.

Mozilla ha puesto ha disposición de todos sus usuarios una serie de actualizaciones para dispositivos Windows de 32 y 64 bits, así como macOS o Linux. El proceso es muy sencillo, una vez descargada esta última versión, en la esquina superior derecha, se encuentra dentro de la sección de Ajustes el apartado de Ayuda y Acerca de Firefox donde está toda la información necesaria, aunque también se puede consultar el comunicado emitido por la compañía.

No es la primera vez que Mozilla se enfrenta a este problema conocido como ataque de día cero, por aprovechar una vulnerabilidad de un sistema que aún no ha sido descubierta por los responsables del

sistema. En 2016, se vieron obligados a lanzar un parche de seguridad urgente para bloquear un fallo que permitía a los ciberdelincuentes eliminar el anonimato que crea el navegador Tor y recopilar los datos personales, por este motivo siempre es importante estar pendiente de todas las actualizaciones disponibles.

Disponible en:
https://computerhoy.com/noticias/tecnologia/usas-firefox-quizas-estes-peligro-descubren-fallo-afecta-miles-pcs-441159

4. 6 LUGARES DONDE LOS HACKERS PUEDEN AVERIGUAR INFORMACIÓN SOBRE TI

Fecha: 18/06/2019

Los hackers cuentan en la actualidad con un jugoso abanico de lugares en los que recabar datos de empresas y usuarios para realizar toda clase de chantajes, infectar sus dispositivos, secuestrar móviles o robar datos sensibles. Repasamos algunos de ellos.

No solo en la Deep Web viven los hackers traficando con ingentes cantidades de contraseñas o buscándoles las cosquillas a grandes empresas tras fugas masivas de datos, sino que los lugares más comunes y usados de la red son también un suculento nido de información para ellos.

Así, cuando compras online, utilizas tus redes sociales o rellenas una encuesta en Internet, atraviesas puntos o empleas herramientas que los ciberdelincuentes intentan emplear para hacerse con información sensible. Destacamos varios lugares donde los hackers pueden averiguar información sobre ti.

6 sitios donde los hackers pueden robar tus datos

Medios sociales: Ingresar la mayor cantidad de información personal posible en sus páginas de redes sociales facilita mucho el trabajo de los piratas informáticos.

En ellos viertes muchos datos clave sobre ti, como tu lugar de residencia, donde trabajas, tu cumpleaños, tu pareja, tus opiniones políticas o creencias religiosas, los miembros de tu familia o el lugar a donde te vas de vacaciones.

Esto puede producir suplantaciones de identidad, atracos, chantajes y robo físico, además de hurto de datos y credenciales.

Portales de comercio electrónico: Es fundamental tener mucho cuidado con las tiendas online en las que introduces los números de tu tarjeta de crédito, emplear gestores de contraseñas, valerte de herramientas como Paypal o vigilar a fondo el certificado de seguridad.

Cuestionarios y encuestas online: En algunas puedes encontrar preguntas personales como dónde creciste o cómo fue tu infancia, similares a las preguntas de seguridad.

En lugar de eliminar la información ingresada, muchos cuestionarios guardan sus respuestas, lo que significa que pueden ser utilizados por piratas informáticos para el robo de identidad. Por ello, resulta clave pensar en lo que tus respuestas pueden revelar sobre ti.

Motores de búsqueda: La forma más sencilla de minimizar tu presencia en los resultados de los motores de búsqueda es encontrar sus páginas web que aportan tus

datos y eliminarlas (o solicitar que se eliminen) cuando sea posible.

Fitness trackers: Incluso la pulsera se puede utilizar para realizar un seguimiento de tu actividad física. La información sobre su ritmo cardíaco y los pasos diarios puede no ser de mucha utilidad para los piratas informáticos, pero el movimiento de tus manos es una historia diferente.

De acuerdo con un estudio, si usas un rastreador de ejercicios mientras ingresas el código de acceso de su teléfono inteligente o el número PIN, los hackers pueden hacerse con información valiosa.

Contenedores de basura digital: El hecho de que se haya movido al icono de la papelera en su escritorio no significa que estés a salvo de piratas informáticos.

Cuando "borras" la información, como documentos fiscales o fotografías personales, en realidad solo estás eliminando el sistema de archivos sin eliminar los datos reales. Con el software adecuado, los hackers pueden recuperar cualquier cosa en su contenedor de basura y usarlo para su propio beneficio. Si realmente deseas eliminar tu basura digital, debe limpiar el disco duro.

Disponible en:
https://www.ticbeat.com/seguridad/6-lugares-hackers-informacion-sobre-ti/

USO SOCIAL DE LAS TIC

1. POR QUÉ EL 5G REDUCIRÁ UN 30% LA EFICACIA DE LA PREVISIÓN METEOROLÓGICA

Fecha: 11/06/2019

Te explicamos los motivos por los que la esperada conexión 5G propiciaría que los pronósticos del tiempo viesen reducida su eficacia en hasta un 30%, según los expertos.
Durante la última semana hemos oído hablar del 5G prácticamente cada día por la polémica con Huawei. Todo apunta a que será una de las grandes vías de conexión en el futuro cercano. Sin embargo, se da la curiosa circunstancia de que puede afectar negativamente a una de las ventajas que nos ofrece la tecnología desde hace décadas: la previsión del tiempo.

Con el despliegue del 5G puede que los pronósticos meteorológicos reduzcan su eficacia en un 30% y volvamos a la situación que había a principios de los 80 con los sistemas que se usan hoy día de forma mayoritaria.

El motivo es que una de las frecuencias usadas en el 5G y la de la previsión de tiempo son muy similares. El 5G emite por múltiples frecuencias, entre ellas los 24GHz, mientras que los satélites meteorológicos se basan en la frecuencia 23.8GHz por ser la adecuada para detectar el vapor de agua en la atmósfera con gran precisión.

El problema ha dejado de ser anecdótico y la Organización Mundial de Meteorología y la NASA han solicitado que se reduzca la potencia con la que se emite en esas frecuencias o una redistribución de frecuencias. Aunque en el estado en el que se encuentra el despliegue es complicado

recular, ya que obligaría a aumentar el número de antenas o a cambiar innumerables aparatos.

A pesar de que la alarma ha saltado en Estados Unidos, es un problema que puede afectar a nivel mundial y perjudicar a las previsiones de todo el planeta. Aunque existen otras frecuencias útiles para la medición y previsión de temporales, la situada en 23.8GHz es de las más utilizadas y se están analizando otras usadas habitualmente para saber si también se pueden ver afectadas por el 5G.

¿Preferirías tener 5G o saber el tiempo que va a hacer? Esperemos que en ningún momento nos encontremos en una situación similar. Lo que está claro es que tras las graves polémicas que se están viendo en la guerra comercial donde el 5G tiene tanta importancia, pocos esperábamos encontrar una problemática tan particular.

Disponible en:
https://www.ticbeat.com/tecnologias/por-que-el-5g-reducira-un-30-la-eficacia-de-la-prevision-meteorologica/

2. LA TECNOLOGÍA TAMBIÉN LLEGA A LA MEDICINA: ASÍ SERÁ IR AL MÉDICO EN EL FUTURO

Fecha: 18/06/2019

El futuro de la medicina ya se beneficia en la actualidad del poder masivo de los datos y su interpretación para ofrecer un elevado grado de personalización a los usuarios, los gigantescos avances en el terreno de la IA para predecir enfermedades con antelación, monitorizar a los pacientes o descubrir nuevos fármacos, o de la capacidad casi infinita de la impresión 3D para abaratar costes y encontrar nuevas soluciones médicas desde biotintas para imprimir córneas humanas a medicamentos, implantes de tráquea, órganos, reconstrucción de nervios dañados o fabricación de tejidos.

Una pregunta que planea sobre muchas cabezas es ¿cómo será ir al médico en el futuro? ¿Qué cosas cambiarán? ¿Cómo la tecnología simplificará procesos, ayudará a mejorar la atención médica o salvará millones de vidas con la ayuda inestimable del Big Data, la robótica, el Internet de las Cosas o los wearables para monitorizar la salud de los pacientes?

En primer lugar, la relación médico-paciente tendrá un carácter más cooperativo, simultáneo y virtual gracias a toda clase de dispositivos que permitirán hacer un seguimiento en tiempo real del estado del paciente, contar con un historial médico online avanzado e incluso, administrar la medicación a través de dispositivos dentro del cuerpo humano y monitorizar enfermedades gracias a innovadores gadgets como píldoras inteligentes inalámbricas o biosensores portátiles, desde lentes de contacto que rastrean los niveles de glucosa hasta zapatos que miden el peso, el equilibrio y la temperatura.

Así, una de las labores de la innovación tecnológica será alertar a los médicos si algo está mal y proporcionar un diario de salud digital.

Las aplicaciones médicas pondrán más control en las manos de los pacientes, incrementando drásticamente su seguridad y otorgándoles más conocimiento -en un mismo lugar y de forma simplificada e

interactiva desde el smartphone, en lugar de diversos documentos y recetas-.

Las apps aliviarán la confusión y se convertirán en un centro de todos los datos que los pacientes precisan para su recuperación, desde alertas para tomar los medicamentos, controlar efectos secundarios, o remitir información relevante a los especialistas.

Las aplicaciones democratizarán el acceso básico a la atención médica, programarán las citas, guiarán a los pacientes para los tratamientos y brindarán un seguimiento útil al médico, además de realizar exámenes y diagnósticos virtuales, videollamadas para consultar dudas –mejorando los problemas de costes, desplazamientos y rapidez de la asistencia a domicilio, algo especialmente significativo dentro de las economías en desarrollo, áreas rurales y alejadas o zonas devastadas por desastres naturales o o conflictos armados-.

Las citas virtuales conllevarán un importante ahorro económico, mejorarán la eficacia gracias a la combinación del IoT con el análisis de datos avanzados y aliviarán carga de trabajo y sobresaturación de la atención primaria.

Cabe destacar en la propia actualidad existen más de 97.000 aplicaciones móviles relacionadas con la salud y la forma física: las diez mejores aplicaciones de salud propician cada día 4 millones de descargas gratuitas y otras 300.000 de pago, mientras que este año, el mercado de la salud móvil moverá 26.000 millones de dólares.

Los ámbitos más destacados son pérdida de peso, ejercicio, salud femenina, sueño y meditación o embarazo. Según el Grupo Research Now, casi el 50% de los médicos introducirán aplicaciones médicas a su práctica en los próximos cinco años, mientras que una encuesta de MedPanel revela que el 42% de los médicos encuestados admitieron que sus pacientes podrían beneficiarse del uso de aplicaciones.

En cuanto a la atención médica, los profesionales contarán cada vez más con el apoyo de la Inteligencia Artificial, el machine learning o el deep learning, que sirven, entre otras cosas, para acelerar la toma clínica de decisiones, conectar datos valiosos y ser herramientas de apoyo para el diagnóstico y evaluación médicos. Muchas compañías ya desarrollan soluciones punteras en este ámbito, como el notable caso de IBM Watson.

Destacan ya en la actualidad numerosos sistemas inteligentes y algoritmos capaces de proezas como reconocer un infarto por teléfono -algo que ya pone en práctica una startup de Copenhague-, los test exprés para realizar diagnósticos precoces de varios tipos de cáncer, sensores inteligentes para monitorizar apacientes intubados, reduciendo los riesgos dentro de las unidades de cuidados intensivos o algoritmos que pueden predecir psicosis, neumonía, cáncer, problemas de corazón o demencia.

Los dispositivos de detección se servirán de indicadores como la piel, los ojos o el aliento para desarrollar diagnósticos con la ayuda de la IA.

En el futuro médico no podemos olvidarnos del inmenso potencial de la tecnología blockchain, con una gran capacidad a sus espaldas para revolucionar el sistema sanitario.

La ventaja de la cadena de bloques reside en que permitirá crear bases de datos comunes con información médica blindada y segura, mejorando con creces la privacidad debido a su sistema de encriptado. Según el estudio de IBM, Healthcare Rallies for Blockchain, el 56% de las compañías de salud tiene pensado

implementar una solución de blockchain comercial para 2020.

Las aplicaciones son muy diversas: transmitir registros de pacientes, optimizar la cadena de suministro farmacéutica, mejorar la facturación o realizar ensayos clínicos.

Si ir al médico en el futuro tiene estrecho contacto con wearables, aplicaciones móviles y consultas virtuales con tu profesional sanitario, la robótica mejorará especialmente la atención quirúrgica y los tratamientos deslocalizados: la telecirugía experimentará un notable ascenso, la nanocirugía también vivirá un importante desarrollo en la reparació celular o los tratamientos no invasivos y los cirujanos recibirán un importante apoyo por parte de pequeños y precisos autómatas.

La impresión 3D permitirá dar vida a toda clase de productos: desde fármacos a gadgets como audífonos, prótesis o materiales inorgánico, órganos y tejidos como la piel o los vasos sanguíneos, e incluso reproducción de células madre.

En el futuro, irás menos y mejor a la consulta del médico: las aplicaciones de tu smartphone podrán avisar a los profesionales de cualquier alteración en tu organismo, sensores inteligentes podrían evitar que tengas que desplazarte de casa para ser monitorizado y tu propio médico podría administrarte la medicación a distancia con ayuda tecnológica, realizar una consulta virtual al otro lado de la pantalla o controlar tu estado de salud mediante tecnología wearable, pues los biosensores desempeñarán un papel clave para detectar alteraciones y desviaciones en el organismo, algo fundamental para vigilar de cerca a pacientes con enfermedades crónicas peligrosas.

Disponible en:
https://computerhoy.com/noticias/life/tecnologia-tambien-llega-medicina-sera-ir-medico-futuro-439751

3. CHINA PRESENTA EL PRIMER PROCESADOR CEREBRO-ORDENADOR

Fecha: 11/06/2019

Hace unos años sonaría a episodio de Black Mirror, pero lo cierto es que la conexión entre tecnología y cerebro está cada vez más próxima debido a los estratosféricos avances en materia de computación

Encontramos ejemplos como el Bryan Johnson, que ha diseñado un microchip que puede instalarse en el cerebro para corregir daños neuronales provocados por enfermedades como el Alzheimer, el proyecto de comunicación cerebro-cerebro llamado Silent Talk y financiado por DARPA, las interfaces cerebro-ordenador, el biohacking o las iniciativas de implantes para controlar cosas con la mente o incluso, conectarla con la nube.

Ahora, China ha dado un gran paso adelante presentando Brain Talker, un chip que sugiere que las interfaces cerebro-computadora (BCI) son dispositivos que proporcionarán pronto una línea directa de comunicación entre el cerebro y una computadora.

El diseño nace de una colaboración entre la Universidad de Tianjin y la estatal China Electronics Corporation. Gracias a ambos ha podido ver la luz este “Brain Talker”, un chip de ordenador diseñado

específicamente para su uso en BCI (Brain–computer interface).

“Las señales transmitidas y procesadas por el cerebro son abrumadoras”, dijo el investigador de la Universidad de Tianjin, Ming Dong. “Este BC3 [chip de códec cerebro-computadora] tiene la capacidad de discriminar las señales eléctricas neuronales y decodificar su información de manera eficiente, lo que puede aumentar la velocidad y la precisión de las interfaces cerebro-computadora”. Ming cree que el chip podría ayudar a sacar a los BCI de los laboratorios y masificar su uso en otras aplicaciones.

“Las interfaces cerebro-computadora tienen un futuro prometedor. La tecnología BCI de The Brain Talker Chips Advances permite que sea más portátil, portátil y accesible para el público en general”, señala el comunicado oficial.

Disponible en:
https://computerhoy.com/noticias/tecnologia/china-presenta-primer-procesador-cerebro-ordenador-433755

4. EL PENSAMIENTO SERÁ LA NUEVA ARMA DEL PENTÁGONO

Fecha: 03/06/2019

Desarrollará tecnologías capaces de leer y dirigir la mente de los soldados

El Pentágono se propone desarrollar tecnologías capaces de leer la mente de los soldados para que puedan dirigir centros de control, detectar intrusiones en una red segura y controlar drones, solo con el pensamiento.

Estados Unidos ha contratado a científicos para desarrollar tecnologías capaces de leer instantáneamente las mentes de los soldados, sin necesidad de cirugía ni de implantes en el cerebro.

La idea es usar la ingeniería genética del cerebro humano y la nanotecnología para transferir imágenes de un cerebro a otro y de un cerebro a una máquina, solo mediante el pensamiento. El objetivo último de este proyecto es crear armas controladas por la mente.

La iniciativa va a ser financiada por la Agencia de Proyectos de Investigación Avanzados de Defensa, más conocida por su acrónimo DARPA, perteneciente al Departamento de Defensa de Estados Unidos y responsable del desarrollo de nuevas tecnologías para uso militar.

En el pasado, DARPA ha desarrollado diversas tecnologías que han tenido un gran impacto en el mundo: satélites, robots y las redes de ordenadores que finalmente alumbraron Internet.

En un comunicado, DARPA ha anunciado que financiará un programa de neurotecnología de próxima generación (N3), con la finalidad de crear un canal bidireccional para una comunicación rápida y perfecta entre el cerebro humano y las máquinas, sin intervención quirúrgica alguna.
Esta tecnología pretende afinar los actuales interfaces entre cerebro y máquina al introducir mayor rapidez en la interacción: se trata de reducir el lapso de tiempo que existe entre una orden cerebral y una mano que mueve una máquina, o entre una orden cerebral y la voz que da una orden a una máquina.

El resultado pretendido es que, mediante un casco o un auricular, los militares puedan dirigir centros de control e incluso percibir en el cerebro intrusiones en una red segura sin necesidad de tocar un teclado, solo con el pensamiento.

Sistema tecnológico

El propósito es experimentar con diferentes combinaciones de campos magnéticos, campos eléctricos, campos acústicos (ultrasonido) y luz para registrar actividad cerebral y comunicarse con el cerebro con mayor velocidad y resolución.

Lo primero que harán es valerse de un vector viral, un virus modificado que hace de vehículo para introducir material genético en el núcleo de una célula: insertará ADN exógeno en determinadas neuronas del cerebro humano.

Usarán dos proteínas insertadas en el ADN de las neuronas para conseguir la comunicación bidireccional. Una de las proteínas absorbe la luz cuando una neurona se activa y permite detectar la actividad cerebral. Un casco recoge entonces la señal y observa lo que esa persona está pensando, viendo, escuchando o decidiendo.

La segunda proteína tiene la finalidad de estimular las neuronas para inducir una imagen o un sonido en la mente de una persona, como respuesta a lo que está pensando, viendo, escuchando o decidiendo.

La estimulación se consigue mediante el envío de nanopartículas magnéticas, ya empleadas en medicina para alterar la actividad neuronal a modo de mini-electrodos. Estas partículas se implantan vía nasal y se orientan dentro del organismo a través de los campos magnéticos para alcanzar las neuronas específicas señaladas por la primera proteína.

Funcionamiento

El resultado previsto de esta investigación será el siguiente: cuando el cerebro se activa ante una circunstancia, el sistema detecta la actividad neuronal y convierte ese impulso nervioso en campos magnéticos que son detectados por el casco o los auriculares del usuario.

A continuación, el casco o el auricular interpretan la señal recibida y reaccionan aplicando otro campo magnético a las neuronas que han enviado el impulso nervioso, y consiguen que la actividad neuronal se oriente en una dirección inducida.

Así se lograría que estas tecnologías puedan leer y escribir en células cerebrales en solo 50 milisegundos (un milisegundo corresponde a la milésima fracción de un segundo) e interactuar con al menos 16 sitios del cerebro a una resolución de 1 milímetro cúbico, (un espacio que abarca miles de neuronas), según explica IEE Spectrum.

Como primer experimento, los científicos planean usar el sistema para transmitir imágenes desde la corteza visual de una persona a la de otra.

Cuando la tecnología esté desarrollada, supuestamente podrá conseguir también que los militares controlen múltiples drones a través de sus pensamientos, procesados con ambas proteínas, campos magnéticos, campos eléctricos, campos acústicos y luz.

Disponible en:
https://www.tendencias21.net/El-pensamiento-sera-la-nueva-arma-del-Pentagono_a45287.html

REPÚBLICA DE CUBA
MINISTERIO DE COMUNICACIONES

Sistema de Vigilancia Tecnológica