REPÚBLICA DE CUBA
MINISTERIO DE COMUNICACIONES

Boletín *Novedades TIC*

Noviembre *2019*

Contenido

Sistema de Vigilancia Tecnológica

Ministerio de Comunicaciones

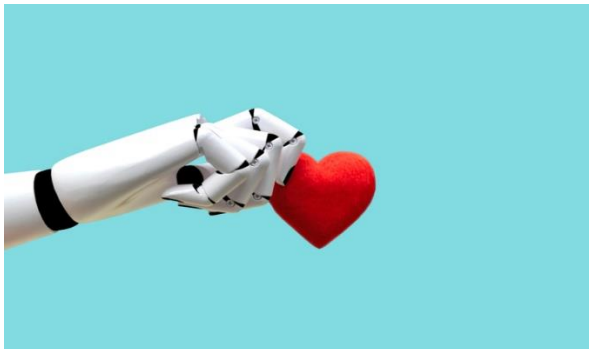
Noviembre, 2019

INTELIGENCIA ARTIFICIAL

1. LOS ROBOTS SON CAPACES DE HERIR NUESTROS SENTIMIENTOS, SEGÚN ESTE ESTUDIO

Fecha: 22/11/2019

Puesto que los droides carecen de conciencia y pensamientos propios, cabría pensar que podemos ignorar sus comentarios críticos con facilidad sin ofendernos o ver lastimados nuestros sentimientos. Un estudio muestra que no es así.



Todavía no tenemos a un robot en la mesa de al lado en la oficina ni desayunamos en un bar repleto de androides, pero la automatización va colonizando lentamente diversos aspectos de nuestra vida. Si creías que los insultos o comentarios despectivos provenientes de una máquina no podían herirte, estabas equivocado.

Pese a que los robots carecen de sentimientos propios o conciencia, un estudio a pequeña escala muestra cómo la crítica de un autómata puede lastimar a un ser humano.

El experimento involucró a 40 participantes humanos expuestos a insultos lanzados por e popular robot humanoide Pepper durante una serie de juegos. El rendimiento humano en el juego fue peor con los comentarios negativos de la máquina y mejor cuando el autómata se mostró más positivo y alentador.

Se trata de un trabajo útil para enseñarnos cómo podríamos usar robots como compañeros o como herramientas de aprendizaje en el futuro. “Este es uno de los primeros estudios de interacción humano-robot en un entorno en el que no están cooperando”, dice el científico informático Fei Fang, de la Universidad Carnegie Mellon (CMU). “Podemos esperar que los asistentes domésticos sean cooperativos, pero en situaciones como las compras online, es posible que no tengan los mismos objetivos que nosotros”.

Los 40 participantes del estudio compitieron en un juego llamado Guardias y Tesoros 35 veces con Pepper. El juego es un ejemplo de un juego de Stackelberg, con un defensor y un atacante. Aunque todos los integrantes de la partida mejoraron en términos de su racionalidad en el transcurso de la prueba, aquellos que fueron insultados por su oponente robot obtuvieron una puntuación más negativa. Los jugadores que se encontraron con un robot crítico también tuvieron una visión más pesimista.

Pepper incluyó comentarios al estilo de “tengo que decir que eres un jugador terrible” o “ te has confundido durante el transcurso del juego”. Los hallazgos coinciden con investigaciones anteriores que muestran que los comentarios críticos o insultos indicen de forma negativa en el juego, aunque en esta ocasión provienen concretamente de una máquina automatizada.

Aunque este estudio sea a pequeña escala, revela la importancia de comprender las reacciones humanas a las máquinas, fundamentales a medida que nuestras interacciones con los robots se vuelven más frecuentes, ya sea a través de un altavoz inteligente en un hogar o como un bot

diseñado para mejorar la salud mental en un hospital.

En situaciones en las que los robots podrían pensar que saben má que nosotros, como obtener instrucciones de A a B, o comprar algo en una tienda, los programadores necesitan profundizar en el manejo de dichos argumentos al codificar un droide.

En el futuro los responsables del estudio quieren analizar las señales no verbales dadas por los robots. Además, indicaron que pese a que en la ejecución del juego muchos participantes eran sofisticados y comprendían que el robot emitía respuestas programadas, se veían igualmente afectados por los comentarios negativos. La investigación, todavía pendiente de publicación, se presentó en la Conferencia Internacional IEEE sobre Robot y Comunicación Interactiva Humana en India.

Disponible en:
https://www.ticbeat.com/tecnologias/robots-capaces-herir-sentimientos/

2. "MAMÁ, EL MUÑECO ME VIGILA", O EL PELIGRO DE LOS JUGUETES CONECTADOS

Fecha: 20/11/2019

Lejos queda la época en la que los entrañables furbies llegaron a ser considerados por la NSA estadounidense como potenciales espías en miniatura, un mito desmentido por la compañía. Ahora sí vivimos en la época de los juguetes conectados al Internet de las Cosas y es necesario extremar las precauciones.

Que una muñeca de porcelana te guiñe un ojo en medianoche o los juguetes se rebelen como en Toy Story forma parte del imaginario infantil colectivo, pero a día de hoy, proliferan muchos juguetes y dispositivos de ocio conectados que pueden jugar una mala pasada a pequeños y mayores de la casa. Desde muñecos interactivos, robots infantiles y drones a videoconsolas o tabletas, las amenazas cibernéticas acechan con la expansión global del Internet de las Cosas.

A día de hoy nos enfrentamos, por una parte, a un mercado lúdico infantil cada vez más amplio y segmentado -en el que los juguetes conectados son muy demandados por los niños-, y la carencia de soluciones de ciberseguridad suficientes para que estos juguetes protejan a sus consumidores, convirtiendo a muchos productos en brechas que abren el paso a potenciales peligros.

Algunos casos sonados de juguetes peligrosos

En los últimos tiempos saltaron a la fama por motivos poco honrosos juguetes peligrosos como el Smart Toy Bear de Fisher Price, un peluche aparantemente inofensivo con un mini ordenador incorporado con Android 4.4 que no estaba lo suficientemente protegido, por lo que a través de él era posible acceder a las imágenes y vídeos que captaba su cámara incorporada e incluso al micrófono que permitiría escuchar al niño.

También se podía penetrar en la plataforma de registro de clientes y tener acceso a los datos del niño que utilizaba el juguete o conocer los momentos en los que lo usaba. Y aunque el fabricante ha reparado a día de hoy el problema de software, no es ha sido un caso aislado.

Por su parte, un reciente estudio realizado por el Consejo de Consumidores Noruego (Forbrukerradet), revela que dos juguetes conectados a la red: la muñeca Cayla y el robot i-Que también presentan fallos preocupantes relativos a la seguridad y la privacidad de los menores, ya que siguiendo algunas pautas sencillas cualquiera podría tomar el control de los juguetes mediante un smartphone, hablando y escuchando a través del producto sin necesidad de acceder físicamente al mismo.

Una de las averiguaciones de Forbrukerradet es que las cosas que el niño le dice a la citada muñeca son transferidas a la compañía estadounidense Nuance Communications, especializada en tecnologías de reconocimiento de voz, reservándose la compañía el derecho de utilizar esta información con terceros.

Además, la muñeca viene con determinadas frases preprogramadas que promocionan diferentes productos, entre ellos, películas norteamericanas de dibujos animados con los que el proveedor de la aplicación tiene una relación comercial.

Consumerist o la OCU se han hecho eco de esta información y han advertido de los riesgos de estos juguetes.

"Los consumidores deben entender que mientras un dispositivo pueda estar conectado a la web u otros dispositivos y no esté asegurado, se puede acceder sigilosamente y usarse para la ventaja de un ciberdelincuente", dice Nick FitzGerald, investigador principal de la compañía ESET, que reveló que en Australia, cada hogar tiene 9 dispositivos conectados.

Toma las siguientes precauciones con las compras navideñas "conectadas" de tus hijos:

1- Hay que cambiar la contraseña de acceso tras abrir el juguete y sacarlo de la caja: Debes tener en cuenta que todos estos dispositivos vienen de fábrica con un usuario y clave predeterminada más sencilla de averiguar por parte de los hackers. Aquí te hablamos de algunas características esenciales para lograr las contraseñas seguras. Entre ellas, mayúsculas y minúsculas, caracteres especiales y números, extensión larga y ausencia de referencias personales.

2- Compra juguetes asociados a la edad de los niños: Para ello, revisa la edad recomendada en el etiquetado del dispositivo.

3- Controla a los amigos virtuales de tus hijos: Para evitar a ciberdelincuentes, acoso en la red y problemas de ciberbullyng, revisa las solicitudes de amistad o los chats internos de los juegos, para saber de qué habla y con quién habla el menor.

4- Actualiza siempre el software, puesto que las actualizaciones incluyen parches de seguridad útiles para la protección del usuario ante riesgos como el malware, que afecta a la mitad de dispositivos de los españoles.

5- Comprueba la política de privacidad de los gadgets: Aquellos dispositivos que soliciten direcciones, nombres, números de teléfono y detalles sobre la vida de los niños también podrían constituir un punto de acceso para los gadgets.

6-Investiga si el modelo de juguete u otros productos de la marca han experimentado vulnerabilidades de seguridad o riesgos de privacidad anteriores. Para ello, busca en Google el nombre de la compañía acompañado de alguna palabra clave como estafa, fraude, vulnerabilidad o seguridad. ¿Merece la pena? Si la respuesta es afirmativa, al menos realiza todos los cambios de configuración posibles para apuntalar su privacidad.

7- Bloquea las cámaras y apaga el juguete o gadget por completo cuando no esté siendo usado. Además, ignora y desactiva las características del gadget consideradas de alto riesgo.

8- Utiliza redes WiFi protegidas y de confianza y ten una buena clave para proteger tu router doméstico de posibles ladrones o gorrones-

9- No proporciones datos de medios de pago online como Paypal a tus hijos, ni les des acceso a tu tarjeta bancaria o claves de aplicaciones fintech. De lo contrario, podrían realizar compras dentro de la aplicación.

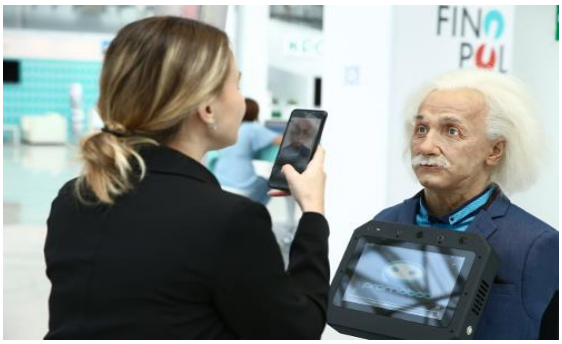
10- Blinda con soluciones de seguridad todos tus wearables y dispositivos conectados para que no se conviertan en un coladero para las ciberamenazas: De lo contrario, los hackers podrían acceder a tus datos personales mediante móviles o tabletas, que estén previamente conectados con los juguetes de los más pequeños, y realizar acciones de phishing, secuestro o robo de datos personales e introducción de malware.

Disponible en:
https://www.ticbeat.com/seguridad/peligros-riesgos-juguetes-conectados/

3. UNA STARTUP RUSA FABRICA ROBOTS AUTÓNOMOS IDÉNTICOS A QUIEN TÚ QUIERAS

Fecha: 04/11/2019

Pronto robots con apariencia idéntica a famosos artistas, deportistas o escritores podrán pulular por las calles del mundo gracias al proyecto de la peculiar startup rusa de automatización Promobot.



La startup rusa Promobot ahora está vendiendo androides autónomos, cuyo aspecto puede ser personalizado y encargado por los compradores para que el bot se parezca a quien desee. Cualquier persona podrá solicitar un robot con cualquier apariencia. Se puede “imaginar una réplica de Michael Jordan vendiendo baloncesto, uniformes y William Shakespeare leyendo sus propios textos en un museo”, dijo Aleksei Iuzhakov, presidente de la Junta Directiva de Promobot.

El Robo-C de Promobot no puede caminar, pero su cuello y su torso tienen tres grados de libertad de movimiento, según indican desde el sitio web de la startup. Su cara tiene 18 partes móviles, que permiten al robot producir 600 microexpresiones, y su software de Inteligencia Artificial cuenta con 100.000 módulos de voz.

“El momento clave en el desarrollo de Robo-C es la digitalización de la personalidad y la creación de una apariencia individual”, dijo el cofundador de

Promobot, Oleg Kivokurtsev, a CNBC. “Como resultado, la inmortalidad digital, que podemos ofrecer a nuestros clientes”. Un proyecto que a muchos puede resultar siniestro y a otros, funcional y atractivo. Por el momento, Promobot ya se encuentra recibiendo pedidos de Robo-C y ha comenzado a construir cuatro clones de robots.

Uno de los bots estará estacionado en un centro de servicio del gobierno donde realizará varias funciones, incluyendo la tarea de escanear pasaportes. Otro se tratará de un clon de Albert Einstein para una exposición de robots. Los dos últimos serán clones de robots del padre y la madre en una familia del Medio Oriente, que ha encargado a los autómatas con el extraño propósito de “saludar a los invitados”. ¿Quiénes serán los próximos?

Disponible en:
https://www.ticbeat.com/innovacion/startup-rusa-robots-autonomos-clones/

4. DESARROLLAN UN CRONÓMETRO PARA LLEVAR EN LA PIEL COMO UN TATUAJE TEMPORAL

Fecha: 03/11/2019

Un equipo de investigadores chinos ha desarrolado un dispositivo flexible y adhesivo que te permite llevar un cronómetro directamente pegado a tu piel. Así es cómo funciona.

Esta solución la agradecerán especialmente los deportistas, ya que tendrán la posibilidad de contabilizar su tiempo mirando el dorso de su mano, sin necesidad de llevar encima el teléfono móvil, el reloj inteligente o la pulsera de actividad.

Los últimos avances tecnológicos han permitido a los científicos desarrollar unos dispositivos flexibles emisores de luz conocidos como pantallas electroluminiscentes de corriente alterna (ACEL por sus siglas en inglés). Estas pantallas se pueden adherir a la piel como si fueran un tatuaje temporal, así como a otras superficies, para funcionar como dispositivos wearables.

No obstante, las pantallas ACEL tienen el problema de que requieren voltajes bastante altos para conseguir un brillo suficiente, una característica que puede derivar en problemas de seguridad. Para superar este inconveniente, el equipo de científicos chinos se ha propuesto diseñar un dispositivo flexible similar pero que no necesite voltaje elevado para funcionar.

Su solución utiliza una capa electroluminiscente hecha de micropartículas emisoras de luz dispersas en un material dieléctrico elástico Este compuesto se trata de u nuevo material dieléctrico en forma de nanopartículas cerámicas incrustadas en un polímero gomoso, lo que permite aumentar el brillo en comparación con las pantallas ACEL existentes.Después, los investigadores han intercalado esta capa luminiscente entre dos electrodos flexibles de nanocables de plata, y han creado un cronómetro de cuatro dígitos adherido a la mano de un voluntario.

Gracias a su tecnología, la pantalla ha demostrado que a bajos voltajes es lo suficientemente brillante a para su visualización en interiores. Todavía queda trabajo por hacer para optimizar y desarrollar más esta solución, pero los resultados son prometedores Este tipo de pantallas flexibles adhesivas que funcionan a bajo voltaje puede tener infinidad de aplicaciones interesantes, desde prendas de vestir inteligentes hasta interfaces hombre-máquina o robótica suave.

Disponible en:
https://www.ticbeat.com/innovacion/desarrollan-un-cronometro-que-puedes-en-la-piel-como-un-tatuaje-temporal/

SEGURIDAD INFORMÁTICA

1. LOS 'HACKERS' PUEDEN APODERARSE DE TU CELULAR A TRAVÉS DE LOS AURICULARES

Fecha: 18/11/2019

Los auriculares que utilizan 'bluetooth' en vez de un cable para conectarse son una buena noticia para los 'hackers', según han informado los especialistas en ciberseguridad de la Universidad Purdue en Iowa (EEUU).

En particular, están en peligro los smartphones con el sistema operativo Android, puesto que los delincuentes pueden acceder a ellos usando la interfaz AT, la que controla las interacciones inalámbricas de los dispositivos, señalan los investigadores estadounidenses.

Para hacerse con acceso al smartphone de su víctima, los maleantes envían unos determinados comandos a esta interfaz, momento en el que el celular pasa a tener conexión insegura, lo que les permite interceptar las conversaciones y acceder a los datos.

Esto se aplica no solo a los auriculares, sino también a los populares relojes inteligentes, según dijo el experto en ciberseguridad ruso Alexéi Grishin. La mala jugada que se lleva el usuario es posible porque estos pequeños dispositivos entran en la llamada zona de confianza del celular, explicó el experto.

Grishin añadió que los auriculares son especialmente atractivos para los piratas informáticos porque a través de ellos se pueden interceptar conversaciones sin que la víctima se dé cuenta. Y este no es el único peligro de los auriculares inalámbricos. Así, el analista jefe de ciberseguridad de la empresa Webroot, Tyler Moffitt, indicó que muchos celulares cuentan con una función de bloqueo inteligente que permite mantenerlos desbloqueados mientras están conectados a un dispositivo con bluetooth. Por lo cual, con los auriculares de este tipo el teléfono es vulnerable a los ataques de los hackers.

Afortunadamente hay algo que todos pueden hacer para protegerse mejor de esta amenaza: instalar siempre las últimas actualizaciones de los sistemas operativos. Según indican los especialistas, los desarrolladores mantienen el pulso a las vulnerabilidades de sus sistemas operativos y lanzan con frecuencia actualizaciones que los protegen mejor.

Disponible en:
https://mundo.sputniknews.com/tecnologia/201911181089353577-los-hackers-pueden-apoderarse-de-tu-celular-a-traves-de-los-auriculares/

2. LOS EMAILS DE PHISHING SOBRE TU CONTRASEÑA EN PELIGRO SON LOS MÁS EXITOSOS

Fecha: 11/11/2019

El phishing se trata actualmente de una de las ciberamenazas más socorridas por parte de los delincuentes para suplantar la identidad de usuarios, marcas y corporaciones. Y si te asustan sobre tu contraseña o te hacen sentir en peligro, es más que probable que hagas clic.

No han sido pocas las ocasiones en las que hemos alertado del incremento y sofisticación del phishing, una amenaza que

`pesca´ tus datos mediante técnicas de ingeniería social y suplantación de la identidad de terceros -desde el CEO de tu empresa a Netflix o tu propia entidad bancaria- mediante el email o las redes sociales. En la actualidad uno de cada 99 emails enviados se trata de una amenaza de phishing. Entre los correos electrónicos fraudulentos de esta índole, cerca de un tercio sortea las prohibiciones por defecto. El phishing, además, es el principal transmisor de malware: un 92% de código malicioso llega a través de esta técnica.

Si bien la táctica más efectiva el año pasado entre los asuntos de email con phishing era que el concepto incluyese la palabra factura, en 2019 las tornas han cambiado y existe otra estrategia que hace las delicias de los cbiberdelincuentes: se trata de aludir a la seguridad. Según una investigación llevada a cabo por KnowBe4, si te hacen pensar que has sufrido una brecha de datos o que existe algún problema con tu contraseña, la tasa de éxito es mucho mayor.

Para el estudio, la empresa realizó un experimento enviando miles de emails de phishing simulados con varios asuntos, con el objetivo de percatarse de cuáles obtenían un mayor número de clics. También analizaron correos electrónicos reales que víctimas habían reportado a sus departamentos informáticos. El asunto que se reveló como más eficaz para perpetrar amenazas de phishing es el que reza "comprueba de inmediato tu contraseña". Casi la mitad de los usuarios (43%) se fiaron e hicieron clic.

Otros asuntos que convencieron a las víctimas fueron "Se hizo un intento de entrega" o "Desactivación de [email] en progreso", que engañaron al 9% de los usuarios. Las políticas corporativas también tienen cabida en el phishing. Así, conceptos como "beneficios para el empleado actualizados", "evaluación del personal 2018", "nuevos cambios organizacionales" o "política de vacaciones y baja por enfermedad" también causaron estragos.

"Mientras sigue habiendo amenazas de ciberseguridad, cada vez más usuarios se vuelven conscientes de la importancia del papel de la seguridad. Tienen gran interés en proteger sus vidas online, y por eso, un mensaje que parece urgente relacionado con su contraseña puede incitar a los usuarios a hacer clic. Los atacantes siempre buscan formas inteligentes para engañar a los usuarios, así que estos tienen que permanecer vigilantes", apunta Stu Sjouwerman, CEO de KnowBe4.

Cabe recordar que la concienciación y la prevención son las bazas esenciales contra el phishing. A la hora de detectar un ataque hay que prestar atención al emisor del mensaje -para detectar ortografía errónea, dominio raro o exceso de consonantes-, hora de envío, coherencia en el asunto, no caer en enlaces extraños y archivos adjuntos o sensación de urgencia. Otros elementos sospechosos son un idioma distinto, traducción automática o fallos gramaticales.

Disponible en:
https://www.ticbeat.com/seguridad/los-emails-de-phishing-sobre-tu-contrasena-en-peligro-son-los-mas-exitosos/

3. INSTAGRAM, ANZUELO DE LOS TRAFICANTES DE PERSONAS PARA VENDER ESCLAVOS EN EL MERCADO NEGRO

Fecha: 05/11/2019

Una investigación llevada a cabo por un equipo de la BBC News Arabic revela que plataformas nacidas en Slicon Valley como Instagram amparan el comercio de esclavos contemporáneo.

La esclavitud no está abolida ni mucho menos, sino que sus formas han evolucionado de forma perversa en este siglo XXI, algunas de ellas amparadas por la tecnología. Haciéndose pasar por marido y mujer, un equipo de BBC News Arabic descubrió que era inquietantemente fácil descubrir traficantes de personas que vendían esclavos en línea en Instagram y otras aplicaciones populares

“En el Golfo, las mujeres empleadas como trabajadoras domésticas se venden online a través de aplicaciones aprobadas y proporcionadas por Google y Apple”, dicen los investigadores en un vídeo publicado el pasado jueves y que puedes apreciar a continuación, colgado en la plataforma YouTube.

Los investigadores contactaron y se reunieron con varias de las personas que anunciaban la venta de trabajadoras domésticas online, incluida una en Kuwait que ofreció venderles a Fatou, una niña de 16 años de Guinea, África Occidental, por 3.800 dólares. “Este es el ejemplo por excelencia de la esclavitud moderna”, dijo Urmila Bhoola, relatora especial de la ONU, Formas contemporáneas de la esclavitud, a BBC News Arabic. “Aquí vemos a un niño que se vende y comercializa como una propiedad”. Mostrando esta realidad parcialmente oculta en las redes sociales, la investigación demuestra cómo el uso de la tecnología también puede tener finalidades perversas. Tras su salida a la luz, las autoridades de Kuwait habrían convocado a varias de las personas responsables de las cuentas de las redes sociales que vendían esclavos. Las autoridades obligaron a los titulares a retirar sus anuncios y firmar un acuerdo legal que promete no participar nuevamente en esta actividad ilegal.

Sin embargo, la actualización publicada por BBC News no menciona ningún tipo de castigo o ramificaciones legales para esta venta de esclavos, a pesar de que Nasser al-Mousawi, Jefe de la Oficina de Trabajadoras Domésticas de Kuwait, le dijo al equipo árabe de BBC News durante su investigación que “cualquiera que se ocupe de este tipo de los negocios serán castigados “.

Mientras tanto, Instagram le dijo a BBC News que había eliminado más contenido de este tipo en Facebook e Instagram, así como que tomaría acciones para evitar la creación de nuevas cuentas diseñadas para ser utilizadas en el mercado de esclavos online.

La abogada internacional estadounidense Kimberley Motley ha asumido el caso legal de Fatou, a quien las autoridades localizaron después de la investigación y la deportaron a su hogar en Guinea, donde una familia local la adoptó. En opinión de la jurista, las grandes compañías tecnológicas que facilitaron el comercio de esclavos deberían proporcionarle una compensación monetaria. “En la Apple Store proclaman que son responsables de todo lo que se pone en su tienda. Y nuestra pregunta es, ¿qué significa esa responsabilidad?”, declaraba la abogada.

Disponible en:
https://www.ticbeat.com/socialmedia/instagram-anzuelo-de-los-traficantes-de-personas-para-vender-esclavos-en-el-mercado-negro/

USO SOCIAL DE LAS TIC

1. TELEFÓNICA Y FACEBOOK SE ALÍAN CON GOOGLE PARA LLEVAR INTERNET A LA AMAZONÍA

Fecha: 30/11/2019

Loon, IpT y Telefónica han explicado en una nota de prensa que el proyecto inicial ofrecerá internet para unas 200.000 personas que residen en un área del 15% de la superficie del departamento de Loreto, región en la que alrededor de la cuarta parte ahora carecen de un servicio 3G o superior.

Loon y Telefónica iniciaron su colaboración en Perú en 2014 con las primeras pruebas de esta tecnología mediante globos, e IpT inició sus operaciones en mayo de 2019 como un operador de infraestructura móvil rural mayorista.

Los globos de Loon operan a 20 kilómetros sobre el nivel del mar, por encima del tráfico aéreo, la vida silvestre y los fenómenos climáticos.

Los globos estratosféricos sirven como torres de telefonía flotantes que transmiten el servicio de un operador directamente a los dispositivos 4G/LTE de los usuarios.

IpT y Loon esperan ahora el permiso regulatorio del Ministerio de Transporte y Comunicaciones de Perú para lanzar el servicio.

Perú es el segundo país, tras Kenia, en el que Loon ha firmado un acuerdo de colaboración para el uso de globos en la expansión de internet.

En Kenia también Loon está a la espera de la aprobación regulatoria para completar la integración de su red con el operador Telkopm Kenya y empezar a volar.

Cuando un globo quiera ponerse fuera de servicio, se le hace aterrizar mediante un paracaídas, tras liberar el gas de elevación que lo haya mantenido a flote.

Loon ya ha aterrizado cientos de globos en Perú en las pruebas que hace desde hace varios años.

Disponible en:
https://www.tynmagazine.com/telefonica-y-facebook-se-alian-con-google-para-llevar-internet-a-la-amazonia/

2. GOOGLE CREA ROBOTS QUE SEPARAN LA BASURA ORDINARIA DE LA OFICINA

Fecha: 30/11/2019

El reciclaje es una de las mejores formas de reducir la contaminación, pero muchas veces no la llevamos a cabo correctamente, lo cual atrasa y perjudica la eficiencia de este proceso. Google ha desarrollado autómatas capaces de separar correctamente los residuos de la oficina.

Las pautas de consumo que llevamos a cabo son insuficientes para controlar los residuos que generan las personas en su día a día, es por ello por lo que las grandes compañías quieren abrirse hueco en esta lucha conjunta y ahora Google ha creado robots que separan la basura ordinaria de la oficina.

Estos robots desarrollados bajo el paraguas de Alphabet X son muy eficientes en su trabajo, ya que son capaces de clasificar los residuos y separar aquellos que van al contenedor de orgánicos de los productos que sí pueden reciclarse.

Forman parte del denominado Proyecto Every Robot de Alphabet X que Google ha anunciado en su blog, una iniciativa de investigación destinada a tratar de introducir la ayuda de los robots en la vida cotidiana de las personas.

Estos robots son autodidactas: estuvieron aprendiendo por sí mismo durante varios meses a separar la basura. Google decidió que en lugar de programas instrucciones muy complicadas sobre cómo identificar los diferentes tipos de elementos, fueran los robots lo que intentaran resolver esta situación a través de pruebas de acierto/error.

El alto porcentaje de contaminación que se ha conseguido reducir gracias a la ayuda de estos robots demuestra que los altos niveles de contaminación se deben en gran medida al error en la clasificación de los elementos que se pueden reciclar de los que no, y al final se acaban todos mezclando con la basura corriente.

La prueba de error/acierto ha sido la mejor manera de que los robots trabajen de forma excelente. En el proyecto se observaba el comportamiento de los robots y su forma de clasificar la basura y marcaban las elecciones correctas y las incorrectas. Su inteligencia artificial ha ido mejorando gracias a los datos que se generaban cada día, que se integraba en al software que ejecuta los robots de tal forma que cada día aumentaba más su rendimiento.

Los ingenieros de Google creen que estos robots aseguran que pueden integrarse en muchas tareas cotidianas y ayudar a las personas en su día a día gracias a la IA, y no necesitan reglas estrictas de antemano: simplemente aprenden bajo el procedimiento de acierto-error

Disponible en:
https://www.ticbeat.com/innovacion/google-crea-robots-que-separan-la-basura-ordinaria-de-la-oficina/

3. QUÉ ES YUKA, LA APP QUE PONE EN APRIETOS A LOS SUPERMERCADOS

Fecha: 01/11/ 2019

Si ves gente que escanea el código de barras de los productos con su móvil, es fácil que estén usando Yuka, una app que analiza la calidad de los alimentos y cosméticos. Su popularidad es tan alta que está comenzando a poner en jaque a fabricantes y establecimientos como Mercadona.

Yuka es una app de origen francés que ya supera las 5 millones de descargas en Google Play. También está disponible para iOS. Analiza el valor nutricional de los alimentos, así como la presencia de aditivos artificiales y su composición orgánica (si es o no ecológico). En el caso de los cosméticos otorga una puntuación de riesgo según el peligro de sus componentes químicos.

Tal como nos cuentan en Business Insider, la base de datos de Yuka recopila más de 600.000 productos alimenticios y 200.000 productos cosméticos. Solo hay que escanear el código de barras de un

producto para obtener su ficha con el análisis nutricional.

Yuka ha cosechado un gran éxito tanto por su enorme base de datos de artículos que usamos todos los días, como por la claridad y sencillez con la que muestra los resultados.

En pantalla aparece la lista de aditivos o productos químicos, y su riesgo para la salud. Además hay una puntuación que en el caso de los alimentos se obtiene al sumar el 60% de los puntos de la nutrición, el 30% de la presencia de aditivos más o menos perjudiciales, y el 10% si es un producto ecológico. Además cuando un artículo tiene una mala puntuación, ofrece alternativas más saludables.

Tanta gente se ha aficionado a usar Yuka para escanear la compra, que supermercados como Mercadona o Carrefour están comenzando a sufrir las consecuencias. Muchos usuarios no compran un producto, si no ha sido aprobado por Yuka…

Los responsables de Yuka aseguran que son 100% independientes: no están influidos ni financiados por ninguna marca, no trafican con los datos que se usan en la app, y las recomendaciones que hacen se basan únicamente en valores nutricionales y presencia de aditivos. Su único medio de financiación es la versión Premium de pago, que ofrece más funciones.

A la hora de valorar los análisis de Yuka, hay que decir que todos los productos que se venden en los supermercados han pasado estrictos controles sanitarios, y si un producto tiene cierto aditivo o cierta composición química, es porque resulta seguro.

Pero es verdad que las alternativas más saludables que propone la app de Yuka pueden ser útiles, aunque hay que valorar también a qué coste. A veces son más caras, o no tienen otros beneficios.

Por otro lado hay que saber que muchos datos de los productos que aparecen en Yuka son subidos por los propios usuarios, y en ocasiones se han encontrado datos erróneos o inconsistencias.Aún así puede resultar útil para descubrir productos que no se ajustan a lo que buscábamos, o para encontrar alternativas más saludables.

Disponible en:
/https://www.ticbeat.com/tecnologias/yuka-app-supermercados/ Las empresas con

BANDA ANCHA

1. NOKIA Y ERICSSON LOGRAN CONTRATOS DE 5G EN CHINA

Fecha: 20/11/ 2019

Nokia ha obtenido contratos valorados en 15.700 millones de yuanes (casi 2.300 millones de euros) para suministrar equipamientos de 5G a las tres principales operadoras de China, una semana después de que éstas lanzasen comercialmente su servicio de telefonía móvil de nueva generación. Su rival Ericsson también ha formalizado acuerdos. La firma finlandesa ha declarado a Mobile World Live que ha firmado acuerdos marco de cooperación en 5G con China Mobile, China Telecom y China Unicom para el año 2020. Dichos contratos cubren despliegues integrales de

redes, equipamiento y servicios para la 5G, banda ultra ancha, redes básicas, óptica, propiedad intelectual, programas y servicios gestionados.

Shine, un portal de noticias chino, informa de que Ericsson también ha cerrado acuerdos marco con las tres operadoras, si bien no se han revelado los detalles financieros de la operación. Las operaciones se han formalizado durante la feria China International Import Expo 2019, celebrada en Shanghai hasta el domingo 10 de noviembre. China Daily ha indicado que la adjudicación de contratos a proveedores no nacionales pone de relieve la "actitud abierta del país hacia todos los actores internacionales" en el despliegue de la tecnología, a diferencia de países como Estados Unidos, Australia y Japón, que han prohibido que las empresas chinas Huawei y ZTE participen en las licitaciones por la 5G.

Inicio rápido

Las tres operadoras chinas afirman que han efectuado el mayor despliegue de 5G conocido hasta la fecha, con cerca de 86.000 estaciones base desplegadas en 50 ciudades en el momento del lanzamiento. Se espera que dicha cifra supere los 130.000 a finales de año, lo que supondría un rápido crecimiento tras la concesión de licencias en junio. GSMA Intelligence prevé que China tendrá 460 millones de abonados de 5G para 2025, lo que representaría el 36% del total mundial.

Disponible en:
https://www.tynmagazine.com/nokia-y-ericsson-logran-contratos-de-5g-en-china/

2. VIVO DOMINA EL INCIPIENTE MERCADO CHINO DE 5G

Fecha: 16/11/2019

Según IDC, las ventas de smartphones 5G en China rozaron el medio millón de unidades en el tercer trimestre, aunque las tres principales operadoras de telefonía móvil del país no lanzaron oficialmente sus servicios 5G hasta finales de octubre.

Las operadoras abrieron las suscripciones a servicios 5G en setiembre y, según la información disponible, ya habían registrado a más de 10 millones de usuarios a principios de octubre. El gobierno chino les había concedido licencias comerciales en junio.

IDC estima la venta de dispositivos 5G en 485.000 unidades, en su mayoría dispositivos emblemáticos de gama alta si bien observa que también ha habido movimiento en los niveles de precios más bajos.

Vivo salió con ventaja al lanzar un modelo de gama alta por más de 700 dólares (**) y un dispositivo de precio más bajo en el rango de 450-550 dólares (**).

En el período comprendido entre julio y septiembre logró una cuota del 54,3% en ventas de teléfonos 5G, seguida por Samsung (29%), Huawei (9,5%), Xiaomi (4,6%), ZTE (1,5%) y China Mobile (1,1%).

Huawei y Samsung se han centrado en el segmento de gama alta, mientras que ZTE y China Mobile han ofrecido dispositivos de 600-650 dólares (**).

La demanda crece

Se espera que la demanda de dispositivos 5G acelere con rapidez tras el lanzamiento comercial.

GSMA Intelligence prevé que China cuente con 460 millones de abonados a 5G en

2025, lo que supondría el 36% del total mundial.

Hace poco, Qin Fei, director general del Instituto de Investigación en Telecomunicaciones de Vivo, anunció planes para lanzar en 2020 por lo menos cinco modelos 5G centrados en la gama media, así como el y al lanzamiento de dispositivos en China por un precio de 2.000 yuanes (unos 260 euros).

Disponible en:
ttps://www.tynmagazine.com/vivo-domina-el-incipiente-mercado-chino-de-5g/

3. CHINA (Y NO ESTADOS UNIDOS) LIDERA EL DESPLIEGUE DE 5G

Fecha: 6/11/ 2019

El año que viene, los operadores chinos tendrán 143 millones de suscriptores, aglutinando un 70 % de todas las conexiones mundiales.

A medida que se realizan las primeras incursiones de la tecnología 5G, operadores, fabricantes de hardware, usuarios y países van tomando posiciones. Y China es quien lidera.

Así lo desvela ABI Research, que, además, adelanta qué sucederá en 2020. Según esta compañía, los operadores chinos alcanzarán los 143 millones de suscriptores a finales del año que viene, lo que significa aglutinar el 70 % de todas las conexiones que existirán en el mundo. Estados Unidos, en comparación, se quedará en los 28 millones. Cinco años más tarde, en 2025, China habrá alcanzado los 1 100 millones de suscriptores 5G mientras que Estados Unidos se situará para entonces en los 318 millones.

Eso sí, "aunque la mayoría de los suscriptores móviles de 5G estarán en China, los ingresos de los proveedores de servicios móviles seguirán siendo más altos en Estados Unidos en 2025, principalmente debido a precios de suscripción más altos", apunta Dimitris Mavrakis, director de investigación en ABI Research.

"A nivel mundial, ABI Research espera que los proveedores de servicios móviles gasten cerca de 1,2 billones de dólares en los próximos 5 años en construir sus redes y que generen cerca de 6,2 billones de dólares en ingresos por servicios solo del mercado de consumo", añade Mavrakis.

De los 12 millones de conexiones 5G que habrá en diciembre de este año se pasará a los 205 millones doce meses más tarde y a los 3 000 millones en 2025, justo cuando rebasará al 4G y sus 2 200 millones de conexiones previstas.

"A pesar de los desafíos que enfrentan los primeros usuarios y los precios relativamente altos de los smartphones con capacidad 5G en 2019, ABI Research espera que 5G llegue al mercado masivo a mediados de 2020, momento en el que China comenzará a dominar en términos de conexiones y, como resultado, en interés de mercado y experiencia tecnológica", indica Mavrakis.

Disponible en:
https://www.silicon.es/china-y-no-estados-unidos-lidera-el-despliegue-de-5g-2407551

REPÚBLICA DE CUBA
MINISTERIO DE COMUNICACIONES

Sistema de Vigilancia Tecnológica