REPÚBLICA DE CUBA
MINISTERIO DE COMUNICACIONES

Boletín *Novedades TIC*

Febrero 2019

Contenido

Sistema de Vigilancia Tecnológica

Ministerio de Comunicaciones

INTELIGENCIA ARTIFICIAL

1. ASÍ ESTÁ CAMBIANDO LOS HÁBITOS DE COMPRA LA INTELIGENCIA ARTIFICIAL

Fecha: 25/02/2019

La inteligencia artificial no solo es una herramienta útil para que los comercios en línea detecten las tendencias de compra de sus clientes y mejorar sus servicios, también permite que el usuario encuentre los productos de una forma más cómoda e intuitiva.

La integración de la inteligencia artificial en los móviles está cambiando los hábitos de compra de los usuarios.

La unión del Big Data y la inteligencia artificial en el comercio ha supuesto una auténtica revolución a los dos lados del mostrador virtual de una tienda online aportando una mejor experiencia de compra a los usuarios.

Recomendadores de artículos que aconsejan a los clientes durante el proceso de compra, sistemas de reconocimiento de imágenes para comprar productos, chatbots de atención postventa, etc. Las herramientas basadas en la inteligencia artificial son infinitas tanto del lado del cliente para facilitar el acceso a los mejores productos, como del lado de la tienda en línea para hacer su negocio más amigable para los usuarios.

La inteligencia artificial está cambiando los hábitos de compra de los usuarios que ya pueden comprar cualquier producto mediante el reconocimiento de productos desde su móvil con solo hacerle una foto. Pero también lo está haciendo en la trastienda ofreciendo mejores servicios a sus clientes.

Los principales expertos en usabilidad de páginas web coinciden en que el modelo de búsqueda por palabras en las tiendas en línea es una herramienta poco efectiva que puede acabar con la paciencia de muchos clientes. El principal problema es la elección de las palabras adecuadas para realizar la búsqueda.

Uno de los principales usos que se le está dando a la inteligencia artificial es precisamente el rol de asistente de compras en el que se utilizan sistemas de reconocimiento de objetos para facilitar la compra a los usuarios.

El usuario solo tiene que enfocar con su móvil un determinado objeto para que la inteligencia artificial integrada en la cámara del smartphone lo identifique y le lleve directamente a una determinada tienda online para que pueda comprarlo. ¡Sin escribir una sola palabra!

¿Parece ciencia ficción? Pues no lo es en absoluto. Sistemas de reconocimiento de imágenes mediante inteligencia artificial como HiVision desarrollado por Huawei permiten identificar todo tipo de productos y mostrar las mejores ofertas para comprarlo en Internet.

Un gran salto tecnológico que cabe en tu bolsillo.

Esto que hace solo unos años parecía imposible, actualmente es una realidad gracias al aumento de potencia en los

procesadores de los móviles que, como en el caso del Huawei Mate 20 Pro, incluye una doble unidad NPU o Unidad de Procesamiento Neural, lo cual permite gestionar las funciones de inteligencia artificial de forma separada a los procesos habituales del móvil.

Gracias a esta evolución, la inteligencia artificial se baja de la nube y permite trabajar de forma local en el dispositivo proporcionando una experiencia mucho más directa e inmediata.

La función HiVision se basa en técnicas de machine learning mediante las cuales, el móvil puede identificar todo tipo de productos y realizar una búsqueda en las tiendas de Internet para ofrecer al usuario el camino más rápido a la mejor tienda.

Esto no solo facilita al usuario comparar los precios de los productos de forma inmediata, sino que también puede comprarlos de formas que hasta ahora era imposible.

La moda, el ejemplo perfecto de cómo la IA ha revolucionado la forma de comprar

La moda es uno de los mejores ejemplos de cómo la inteligencia artificial está cambiando los hábitos de compra de los usuarios, ya que es una industria que se mueve en un entorno muy visual basado en la imagen.

Ya sea mediante los conjuntos que visten los influencers de moda en Instagram y otras redes sociales, fotos de desfiles en revistas, e incluso cómo visten los presentadores en televisión.

Los usuarios están recibiendo estímulos de productos que pueden interesarles constantemente .

Buscar la marca o tienda en la que se vende la chaqueta que lucía alguien en una foto puede resultar poco menos que imposible usando un buscador de productos basado en texto.

En cambio, con el sistema de reconocimiento de productos que ofrece la inteligencia artificial integrada en el sistema HiVision, conseguirlo es tan fácil como enfocar con la cámara del móvil y dar un par de toques sobre la pantalla para acceder a la tienda en la que se vende esa prenda.

La evolución de la inteligencia artificial está haciendo posible algo tan intangible como es la detección del diseño y el estilo de una determinada prenda de ropa, algo que parecía imposible para una máquina hace solo unos años.

Este reconocimiento de similitudes ha dado pie a los recomendadores basados en productos del mismo estilo o con un diseño similar.

De ese modo, puedes enfocar con la cámara de tu móvil un determinado producto, como un reloj por ejemplo, para que la inteligencia artificial de HiVision no solo realice la búsqueda de ese producto, sino que también te sugiera otros productos con un diseño o estilo similar aportando un valor añadido a su búsqueda.

No solo encuentra el producto que estás enfocando, sino que también actúa como asistente de compras en tu móvil mostrándote otras alternativas que también podrían gustarte.

Asesores de compras que te conocen mejor que tú mismo

La inteligencia artificial no solo está cambiando la forma en la que compras desde el móvil, también se aplican chatbots y asistentes de compra en las propias tiendas para recomendar productos relacionados con los que estás comprando, pero de una forma más amplia a como lo hacen las búsquedas relacionadas.

La inteligencia artificial, mediante el Big Data, permite detectar tendencias y patrones de consumo, por lo que se convierte en la herramienta perfecta para recomendar a los usuarios qué productos pueden interesarle incluso antes de ser conscientes de que les interesa.

Por ejemplo, siguiendo con el ejemplo de la tienda de ropa en línea, una vez el usuario ha añadido el producto que ha escaneado mediante la inteligencia artificial en su móvil, la tienda puede utilizar el machine learning para detectar lo que otros usuarios tienden a comprar junto a ese producto o que, por estilo, color o material, puede combinar con él.

De ese modo, el usuario obtiene ideas e información sobre nuevos productos relacionados o que combinan con su compra incluso aunque en un principio no entrara en la tienda con idea de comprarlo ajustándose a tu estilo de vestir o al tipo de productos que acostumbras a comprar.

Este tipo de asistente de compras con inteligencia artificial ya puede encontrarse en tiendas como Amazon, donde la inteligencia artificial tiene una gran importancia en la estrategia de ventas y facilita al usuario la experiencia de compra.

Disponible en:
https://computerhoy.com/patrocinado/tecnologia/cambiando-habitos-compra-inteligencia-artificial-377049

2. LA INTELIGENCIA ARTIFICIAL PERMITE LA IDENTIFICACIÓN DE NUEVOS GENES RELACIONADOS CON EL CÁNCER

Fecha: 19/02/2019

Los avances de la tecnología aportan grandes esperanzas en el campo sanitario. La inteligencia artificial, concretamente, va a tener mucho que decir.

En el Barcelona Supercomputing Center-Centro Nacional de Supercomputación (BSC), la investigadora Nataša Pržulj ha liderado la creación de un nuevo método computacional publicado en Nature Communications, basado en inteligencia artificial que acelera la identificación de nuevos genes relacionados con el cáncer.

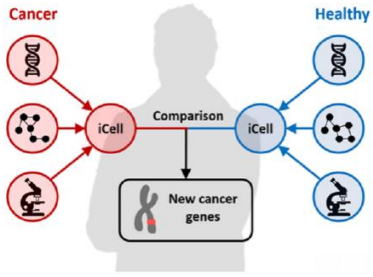
La profesora Pržulj utiliza técnicas de aprendizaje automático (machine learning) para relacionar grandes cantidades de datos ómicos y los recrea en un prototipo computacional.

Específicamente, fusiona tres redes de interacción molecular específicas de tejido: interacción proteína-proteína, coexpresión de genes y redes de interacción genética. La técnica mediante la cual se realiza esta fusión es la Tri-Factorización de Matrices No Negativa, una técnica de machine learning propuesta originalmente para la agrupación y la reducción de la dimensionalidad que se ha utilizado recientemente para la integración de datos.

Este método ya ha sido aplicado por sus autores para reconstruir células de cuatro de los tipos más comunes de cáncer, como son el cáncer de mama, el de próstata, el de pulmón y el de colon, demostrando en todos ellos ser útil para localizar nuevos genes relacionados con estas enfermedades.

El método ha señalado 63 genes y un proceso de validación biológica ha confirmado que al menos 36 de ellos contribuyen al crecimiento irregular de las células. La validación se ha llevado a cabo mediante experimentos de desactivación de genes seguidos de pruebas de viabilidad celular y análisis de datos de supervivencia del paciente.

Alfonso Valencia, profesor ICREA y director del Departamento de Ciencias de la Vida del BSC, afirma que "las iCells de Nataša complementan a la perfección nuestras propuestas de análisis del genoma del cáncer en el BSC, y son solo el primero de los muchos métodos computacionales sólidos que esperamos ver desarrollados por su nuevo grupo en los próximos años ".



"Este nuevo método permite la identificación de genes alterados en el cáncer que no aparecen como alterados en ningún otro tipo de datos. Este descubrimiento pone de manifiesto la importancia de los enfoques integrativos para analizar datos biológicos y allana el camino hacia análisis integrativos comparativos de todas las células" explica Pržulj.

Las posibles aplicaciones de este método van desde el tratamiento de otras enfermedades hasta el envejecimiento, con el objetivo final de descubrir los principios intrínsecos de la organización interna de la vida en la Tierra.

Disponible en:
https://www.computerworld.es/tecnologia/la-inteligencia-artificial-permite-la-identificacion-de-nuevos-genes-relacionados-con-el-cancer?fbclid=IwAR0Dv9nE_exMef9lD7t8Y5q6UiEt13TdSTq43z-8WAkVI9v0Zq5ZxvwjmV4

3. INTELIGENCIA ARTIFICIAL EN LA CADENA ALIMENTARIA: DEL CAMPO A TU INSTAGRAM

Fecha: 19/02/2019

La mayoría de los grandes avances de la humanidad han tenido su origen en algún tipo de industrialización del sector agrario ya que, como principal eje de supervivencia, asegurar la suficiente provisión de alimentos es uno de los principales objetivos del ser humano. La necesidad agudiza el ingenio.

Fue la agricultura la que llevó al ser humano a abandonar la vida nómada, la industrialización del campo la que permitió abastecer de alimentos suficientes a grandes núcleos de población haciendo crecer las ciudades.

Ahora, en plena era digital, una nueva revolución está empezando a cambiar la forma en la que se cultivan los alimentos para optimizar los recursos aprovechando cada gota de agua y cada semilla para obtener más y mejores alimentos.

La inteligencia artificial, de una forma u otra, está presente en todo el ciclo de producción, distribución y consumo de los alimentos. Desde las semillas que se plantan en el campo, a las fotos de tu desayuno que compartes en Instagram.

Las últimas tecnologías para optimizar cosechas

Puede sorprender ver a un agricultor con su portátil bajo el brazo dirigirse a su plantación, pero es algo cada vez más habitual en un sector primario preocupado por la rentabilidad de las cosechas y por la escasez de recursos naturales.

La inteligencia artificial está permitiendo desarrollar lo que ya se denomina agricultura de precisión, en la que el uso de Big Data y sensorización de plantaciones está a la orden del día, permitiendo un mejor control, evaluación y seguridad para las cosechas.

Todos los datos que se recogen en las plantaciones se procesan mediante inteligencia artificial para la toma de decisiones en tiempo real, de forma que se le da a la planta justo lo que necesita y en el momento que lo necesita: control de riegos, tratamientos fitosanitarios, estado del fruto y punto de recolección.

La agricultura de precisión permite ahorrar recursos naturales de forma drástica ya que solo se utilizan los sistemas de riego cuando y en la cantidad que la planta necesita. Esto tiene un impacto positivo en el medio ambiente al aprovechar mejor los recursos disponibles.

Pero la inteligencia artificial no solo se aplica al tratamiento y cultivo de la planta, la automatización de la maquinaria del sector agrario se está llevando a cabo con una alta tasa de éxito en la creación de granjas inteligentes, haciendo que el producto llegue de forma óptima del campo a la cadena de distribución.

La cadena de distribución tampoco se olvida de la inteligencia artificial ya que esta tecnología cada vez está más presente en el proceso de compra.

Desde recomendadores de productos basados en inteligencia artificial integrados en las tiendas online, que se basan en la tendencia de compra de los clientes y en las compras anteriores de cada usuario, hasta sistemas de reconocimiento de objetos integrados en las cámaras de móviles de última generación como el Huawei Mate 20 Pro.

Gracias a su sistema de reconocimiento de objetos, basta con enfocar el objeto que quieres comprar para que la inteligencia artificial integrada lo reconozca y ofrezca al usuario la posibilidad de comprarlo online en diferentes tiendas.

Del campo a la cocina más inteligente

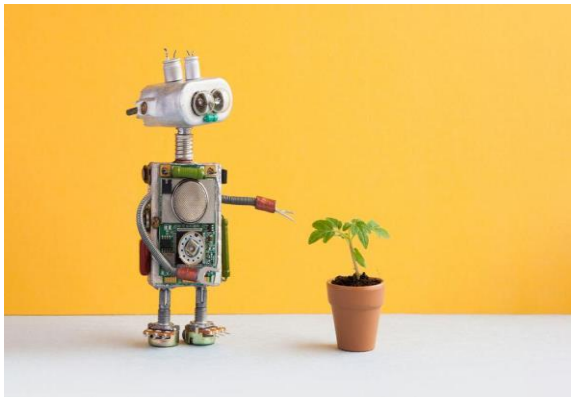
Como media, una persona que cocine habitualmente es capaz de realizar correctamente entre 10 y 15 recetas, mientras que un chef profesional es capaz de recordar más de 100 sin demasiado esfuerzo. ¿Imaginas tener en tu casa un cocinero capaz de crear más de 10.000 recetas teniendo en cuenta la textura y los sabores de más de 2.000 ingredientes diferentes?

Gracias a la inteligencia artificial cognitiva es posible que un agente de inteligencia artificial sea capaz de crear nuevas recetas de cocina basadas en la armonía de sabores y texturas de sus ingredientes.

No hablamos de simples robots capaces de preparar con mayor o menor precisión una serie de recetas establecidas. Hablamos de una inteligencia artificial capaz de

"imaginar" nuevas recetas basándose en la correcta combinación de sus ingredientes para crear platos innovadores en los que se "emula" el proceso creativo de los grandes chefs.

Esta inteligencia artificial, que todavía está lejos del alcance de la mayoría de usuarios, contrasta con la que se integra en cada vez más electrodomésticos que ya están llegando a las cocinas, siendo cada vez más habitual que el frigorífico añada los productos que se van agotando a la lista de la compra e incluso que pueda hacer la compra por ti.



Pero el principal aporte de la inteligencia artificial integrada en estos electrodomésticos es la posibilidad de hacer que trabajen de forma conjunta ya que muchos de ellos ya integran inteligencia artificial en forma de asistentes de voz.

Por ejemplo, ya existen frigoríficos en el mercado que permiten buscar recetas que puedes hacer con los ingredientes que guardas en su interior. Una vez seleccionada, puedes enviar esa receta al horno para que ajuste la temperatura y el tiempo de funcionamiento de forma automática.

Mientras, puedes continuar cocinando mientras un altavoz equipado con asistente de voz te va guiando en cada paso de la receta. Cuando el horno ha terminado su trabajo puede realizar una autolimpieza y enviará información al lavavajillas que prepararía un programa de lavado adecuado para que no quede ni rastro de la salsa de tomate en los platos donde te has comido la lasaña que acabas de cocinar.

Los dispositivos inteligentes son una gran ayuda en la cocina y pueden ayudarte a planificar mejor tus menús. Sobre todo si cuidas tu dieta y mantienes un control de las calorías de cada comida.

En ese sentido, no importa si preparas tú mismo tu comida o sales a cenar con los amigos, la tecnología te ayuda a conocer el aporte calórico de los alimentos en cuestión de segundos.

De nuevo, la inteligencia artificial integrada en la cámara de los Huawei Mate 20 Pro se encarga de identificar los alimentos que vas a comer y te indica de forma clara y sencilla, cuantas calorías tienen. Esto te ayudará a calcular mejor el aporte calórico de cada comida, evitando que te pases, pero lo que es más importante, evitando un déficit en la energía que tu cuerpo necesita para funcionar correctamente y mantenerte sano.

La nutrición y sociedad, cuando la experiencia gastronómica no termina en el plato

Para muchos, la comida es mucho más que un simple alimento. Supone una expresión de creatividad que bien merece ser inmortalizada en una foto y compartida en las redes sociales.

Las experiencias gastronómicas se han convertido en una tendencia de moda en la que los ingredientes tienen que estar perfectamente integrados en el plato no solo a nivel nutritivo o de sabor, sino que también deben hacerlo a nivel estético.

Es este componente estético de la comida el que ha conseguido que millones de

personas compartan a diario en redes sociales las fotos de los menús que se disponen a degustar. Incluso esto se ha convertido en una tendencia y para dar cumplida respuesta, la tecnología se ha adaptado a ese tipo específico de fotografía consiguiendo resultados de una calidad excepcional.

En el caso de la fotografía de comida, el plato no solo tiene que estar delicioso, también debe parecerlo y un ajuste erróneo de los parámetros de disparo puede deslucir por completo el aspecto del plato. Para evitarlo, la inteligencia artificial integrada en la cámara del móvil dispone de un modo de disparo específico que destaca los colores de los ingredientes y reduce la profundidad de campo añadiendo una perspectiva más natural a la fotografía.

El resultado es una fotografía de tu comida que querrás subir a tus redes sociales para que a tus seguidores se les haga la boca agua. ¡Buen provecho!

Disponible en:
https://computerhoy.com/patrocinado/tecnologia/inteligencia-artificial-cadena-alimentaria-campo-instagram-375027?fbclid=IwAR3j60L6JKmp73opwtmwvxIQmPCpJG6NMLldXDS3oqXzGww5l0atoG1F4x0

TELEFONÍA MÓVIL

1. SONY LANZÓ EL XPERIA 1, EL PRIMER MÓVIL CON PANTALLA OLED 4K HDR DEL MUNDO

Fecha: 25/02/2019

En un nuevo intento por retomar lo que alguna vez fue un sitial alto en la telefonía móvil, Sony lanzó el Xperia 1 en el Mobile World Congress en Barcelona.

El equipo tiene las especificaciones que se pueden esperar de un gama alta premium en 2019, con el procesador Qualcomm Snapdragon 855, 6 GB de RAM y 128 GB de almacenamiento, con una batería de 3300 mAh, pero su novedad no está en esos fierros.

La gran gracia es su formato de pantalla ultra alargada y sin notch/muesca, con una relación de aspecto de 21:9. O sea, es largo, muy largo.

Además es el primer móvil del mundo en contar con un panel OLED 4K HDR, prometiendo una experiencia cinematográfica.

Junto a la anterior, el equipo tiene triple cámara, una gran angular, una normal y una teleobjetivo, todas con la tecnología de las cámaras Alpha de Sony, por lo que sin duda habrá que probarlo para ver cómo llevan esa experiencia a un celular.

¿Grabación de video? Sí, por supuesto y a 4K HDR en 24 cuadros, todo muy cine. Esto acompañado de un sistema híbrido de estabilización de imagen.

Aún no hay fecha de lanzamiento ni precio oficial, pero se espera que esté en el rango de los mil dólares.

Disponible en:
https://fayerwayer.com/2019/02/xperia-x1-oled-4k-hdr/

SEGURIDAD INFORMÁTICA

1. ¿CÓMO GESTIONAR LA SEGURIDAD INFORMÁTICA EN 2019?

Fecha: 27/02/2019

Durante los últimos dos años hemos visto cómo empresas de distintos sectores fueron víctimas de ataques informáticos en diversas escalas.

Esto ha generado mayor conciencia en las organizaciones que ahora consideran la ciberseguridad como uno de los temas prioritarios en sus agendas. Según la última edición de la encuesta global a CIOs que realiza Logicalis cada año, los directivos destacan que los ataques externos son una de las principales preocupaciones y el 93% señala que emplea entre un 10% y 50% de su tiempo específicamente a temas vinculados con la seguridad de la información.

Estas amenazas, lejos de desaparecer, se vuelven cada vez más sofisticadas y de mayor alcance. Frente a este panorama las empresas deben prepararse para enfrentar esta situación, considerando cuatro aspectos fundamentales. Las brechas de seguridad son cada vez más importantes. El ataque a la cadena de hoteles Marriot que comprometió los datos de 500 millones de clientes es un ejemplo.

Podemos explicar esto analizando el crecimiento de la cantidad de vulnerabilidades (16.000 en 2018). Significa que nuestra identidad digital está más expuesta y carece de sentido autenticarnos en algunos sitios. Si usamos las mismas credenciales en diferentes ambientes aumentamos exponencialmente el riesgo de exposición; ya una vez vulnerado el dato puede ser usado en otra plataforma. Las brechas van a seguir creciendo, lo importante entonces sería almacenar sólo la información indispensable de los usuarios, reduciendo así el impacto de una potencial exfiltración de datos.

Los dispositivos IoT seguirán en riesgo

Algunos dispositivos (hogareños o industriales) con capacidad de conectarse a la red, no siempre cumplen con los requisitos necesarios para estar protegidos en ese contexto. La consecuencia son millones de equipos con vulnerabilidades que son usados por los atacantes para denegar servicios en forma masiva.

No sería descabellado que pronto veamos nuestros TVs o teléfonos celulares infectados con algún malware y que tengamos que pagar un rescate para utilizarlos de nuevo. Los fabricantes podrían elevar los controles de calidad en términos de cyberseguridad y a futuro esto representaría una ventaja competitiva y un argumento que exigiremos los usuarios a la hora de elegir.

La nube

La adopción de servicios cloud crecerá y, con ello, también los riesgos asociados a errores de configuración y, por ende, de seguridad. Es cierto que, bajo las premisas de recursos ilimitados, los proveedores de nubes públicas priman la disponibilidad,

mientras delegan en el usuario la capa de diseño, acceso y control (después de todo es nuestra infraestructura si pagamos por ella). Esta división de responsabilidades va a obligar a incorporar recursos con skills especializados (por ejemplo, SecDevOps) al equipo de IT para garantizar que las aplicaciones y servicios que migramos al ambiente de la nube sigan cumpliendo las políticas de seguridad de la compañía. Esto es algo que se vuelve prioritario y que las empresas deben empezar a trabajar a lo largo del año.

Las nuevas regulaciones

En un escenario cada vez más global confiamos en estándares más que en empresas o Estados. Normas como la General Data Protection Regulation (GDPR, por sus siglas en inglés) son cada vez más implacables, lo que obligara a las organizaciones a tomar recaudos para no incumplirlas y evitar así, incurrir en severas multas económicas. Este año veremos que muchas empresas locales adoptarán normas internaciones dado que su alcance incluye a subsidiarias y también a proveedores y, en algunos casos, incluso a clientes. Es responsabilidad de todos estar informados respecto de qué normativa nos afecta, estudiar y adoptarla lo antes posible dado que alcanzar este grado de cumplimiento, y mantenerlo, demanda incorporar procesos y tecnología, muchas veces adicionales al presupuesto planificado.

Cada vez más vemos que el abordaje de la seguridad está cambiando de un modelo de seguridad perimetral a un modelo de seguridad centrado en el dato. Esto va a requerir de un conocimiento y procesos que acompañen la estrategia de cada empresa. El desafío estará en poder y saber generar un diseño seguro de arquitecturas cloud, en la gestión de vulnerabilidades, la automatización en tratamiento de incidentes de seguridad y, finalmente, la mitigación de riesgos.

Disponible en:
http://www.tynmagazine.com/como-gestionar-la-seguridad-informatica-en-2019/

2. CIBERSEGURIDAD DE EXTREMO A EXTREMO EN EL SECTOR SALUD

Fecha: 26/02/2019

La Ciberseguridad en el sector salud se enfrenta a dos problemas, de los cuales ninguno se puede resolver utilizando solo la mejor tecnología. De hecho, estos problemas tienen más que ver con la economía que con la ciberseguridad.

Sólo este año en el Consumer Electronics Show (CES), más de 500 compañías presentaron soluciones innovadoras para diagnosticar, monitorear y tratar enfermedades, así como avances en la prestación de asistencia médica remota. El problema es que algunos de estos dispositivos dejan la información médica y los datos de los pacientes expuestos en línea, permitiendo que sean utilizados por cibercriminales.

El primer problema es que la atención médica es una parte crítica de la economía. Según recientes estudios los registros electrónicos de salud EHR (Electronic Health Record, por sus siglas en inglés) son altamente lucrativos. Para dar un ejemplo claro, una historia clínica completa de un paciente puede oscilar entre 300 y 3.000 dólares; ante este panorama es

imprescindible que las organizaciones aumenten las inversiones en materia ciberseguridad y trabajen para que los datos almacenados en la nube estén protegidos, y que toda la información sea segura y privada.

En este caso, el tipo de ataque más habitual que utilizan los cibercriminales es el ransomware, un tipo de malware que encripta los archivos y restringe su acceso a ellos a cambio de un rescate económico.

Aunque la única amenaza no proviene solo de los ataques informáticos, también se puede producir una violación de la privacidad de los datos por el abuso de un miembro del personal interno que tiene acceso a la información del paciente y la transmite al exterior con ánimo de lucro o por errores no intencionados.

La confidencialidad es el principio básico de la política de seguridad del entorno sanitario, lo que obliga al profesional de la salud o a cualquier otra persona a no revelar información suministrada por el paciente.

El segundo problema es que, incluso dentro de un solo hospital, la seguridad es una responsabilidad compartida. Cuando un recurso se comparte comúnmente, el incentivo de cada parte es obtener el mayor beneficio posible y al mismo tiempo incurrir en el menor costo posible. Este problema se conoce como la “tragedia de los bienes comunes”. “Tomemos el ejemplo de un proveedor de atención médica que se basa en una bomba de infusión para tratar a los pacientes diabéticos. ¿La responsabilidad de asegurar ese dispositivo descansa sobre los hombros del fabricante o del proveedor de atención médica? ¿Quién es el propietario de asegurar la transmisión de datos de la bomba? La respuesta a estas preguntas depende de a quién le preguntes, “afirmó Mike Nelson, vicepresidente de seguridad de la IoT de DigiCert.

Para agregar aún más complejidad, una red de atención médica puede usar dispositivos de 50 fabricantes diferentes. ¿Quién es el responsable en este caso? Desafortunadamente, las preguntas no se detienen ahí. ¿Los proveedores del software EHR proporcionan actualizaciones seguras? ¿se confía en la integridad del código que se carga en los dispositivos?

¿Qué medidas tiene implementadas para garantizar que solo las personas adecuadas tengan acceso a los datos del paciente. Lamentablemente, los seres humanos tienden a hacer cambios sólo cuando se presentan incentivos atractivos o cuando el problema con el que se enfrentan se vuelve lo suficientemente doloroso.

Los dos problemas descritos anteriormente apuntan a la necesidad de una autenticación de extremo a extremo, que es el proceso de probar la validez de todas las conexiones digitales, desde un inicio de sesión seguro del sistema para enfermeras y médicos, las comunicaciones entre dispositivos, la red y los servicios externos o las bases de datos tales como las EHRs. Podría ser útil ver estas conexiones como dos partes en un solo sistema.

En la parte frontal, se debe verificar la identidad de cualquier persona que use un dispositivo o acceda a los datos del paciente, como médicos y enfermeras. En el extremo posterior, es igualmente crucial autenticar las conexiones entre los dispositivos y los servidores, EHR,

farmacias etc, es decir con los que se interactue constantemente.

La base para la autenticación de extremo a extremo es la infraestructura de clave pública (PKI). Al utilizar certificados digitales, PKI auténtica usuarios, sistemas y dispositivos sin la necesidad de tokens, políticas de contraseña u otros factores incómodos iniciados por el usuario. Esto descentraliza la autenticación y permite que ocurra en sistemas dispares.

Los proveedores de seguridad, como Imprivata, han introducido varias soluciones en la interfaz descrita anteriormente. Estos incluyen el inicio de sesión único, la autenticación multifactorial y la identificación del paciente para establecer la confianza entre los usuarios, la tecnología y los datos transmitidos en todo el ecosistema de atención médica. La mayoría de los pacientes médicos no se preocupan por su seguridad cuando van al médico; simplemente esperan que su información y su salud se ocupen del uso de medidas de seguridad confiables.

El Instituto Ponemon ha descubierto que más de la mitad de las compañías han experimentado un incidente de seguridad debido a un empleado descuidado. La PKI puede mitigar esta amenaza al exigir que las enfermeras y los médicos utilicen varias capas de autenticación para acceder a los datos del paciente.

En el extremo posterior, algunas autoridades de certificación (CA) modernas, como DigiCert, han construido una infraestructura capaz de implementar miles de millones de certificados en los dispositivos conectados. Además de proporcionar garantía de identidad para dispositivos que se conectan a servidores, sistemas y bases de datos, estas CA ofrecen soluciones para garantizar la integridad del código y la confiabilidad de las actualizaciones de software.

En un evento realizado este mes por la Sociedad de Sistemas de Información y Gestión de la Salud (HIMSS) en Miami, se presentó una encuesta.

La Sociedad de Sistemas de Información y Gestión de la Salud (HIMSS), realizada entre 166 organizaciones de salud en los Estados Unidos, confirmó los supuestos: seguridad los incidentes son casi una experiencia universal y la proporción de presupuestos de TI destinados a la protección de datos aumenta.

El ex jefe de seguridad informática de la Casa Blanca durante la administración de Barack Obama, Greg Touhill, ofreció consejos clave para hospitales, sistemas de salud y otras entidades médicas. Entre ellos: adoptar un esquema de “confianza cero” para hacer frente a los ataques cada vez más sofisticados; mejorar la autenticación multifactor (como ya lo hacen otras industrias); y seguir el ejemplo del sector financiero, fortaleciendo la detección automática de fraudes.

La autenticación de extremo a extremo no se materializará en la industria de la salud hasta que los fabricantes de dispositivos, hospitales, compañías de seguros, proveedores de software y proveedores de seguridad reconozcan su responsabilidad compartida y comiencen a trabajar en colaboración.

Debido a la creciente cantidad de explotaciones en la atención médica, la ciberseguridad se está convirtiendo en un punto de dolor para quienes trabajan en la industria.

Este dolor está causando que algunos actúen y tengan una mejor seguridad en su lugar. Sin embargo, la industria tiene un largo camino por recorrer. Por ahora, solo queda una pregunta: ¿responderemos a otra cosa que no sea el dolor?

Disponible en:
http://www.tynmagazine.com/ciberseguridad-de-extremo-a-extremo-en-el-sector-salud/

3. ASÍ SERÍA EL RANSOMWARE MÁS DESTRUCTIVO IDEADO HASTA AHORA

Fecha: 20/02/2019

Un estudio del proyecto de Cyber Risk Management (CyRiM) de Singapur ha simulado un posible escenario para mostrar las catastróficas consecuencias que podría tener un ataque avanzado de ransomware sobre la economía global.

Este consistiría en un archivo adjunto oculto en un email bajo la suplantación de identidad del departamento de finanzas de tu empresa: si el 43% de los dispositivos se viesen afectados -escenario calificado como el mejor de los casos-, las pérdidas ascenderían a los 85.000 millones de dólares.

Si el anterior es el mejor caso, el peor de los escenarios es aquel en el que Bashe, nombre con el que se describe este ransomware a gran escala, afecta al 97% de los dispositivos a nivel global, con un coste de 193.000 millones de dólares.

Esta ciberamenaza se aprovecharía de una vulnerabilidad sin parche, sin posibilidad de que se descubra un "kill switch" online, como sucedió en el sonado caso de WannaCry el pasado 2017, el cual afectó a más de 100 países y 57.000 entidades .

La campaña de malware se basaría en un PDF malicioso pero de apariencia inocua y nombrado como "Bono de final de año", capaz de imitar el dominio del correo electrónico de la víctima, y así engañar el apartado de la dirección del remitente.

Así se logra suplantar la identidad de la compañía en la que trabaja el internauta afectado.

En el caso de abrirlo, se ejecutaría el malware con la pertinente descarga del gusano de ransomware, cifrando todos los datos en todos los equipos que comparten la red con el dispositivo infectado. Se solicitaría un rescate de 700 dólares y además, el gusano reenviaría automáticamente el correo malicioso a todos los contactos de la víctima, viralizando la ciberamenaza.

En el escenario más pesimista, Bashe conseguiría cifrar en tan solo 24 horas los datos de cerca de 30 millones de dispositivos en todo el mundo.

Los sectores más afectados

Las industrias más afectadas serían los sectores manufacturero, minorista y sanitario. Tal y como detallan desde Panda Security, en el caso minorista, los costes vendrían de sistemas de pago cifrados, y el

paro de comercio electrónico debido a la caída de las webs.

El sector sanitario sería un blanco de los hackers por la antigüedad de sus sistemas, muchos de ellos obsoletos, mientras que la industria manufacturera pagaría caro el cifrado de las máquinas y los problemas en la entrega de mercancía, logística e inventariado.

El estudio muestra cómo el 8% de ellas pagaría el rescate para volver con rapidez a la normalidad, lo que permitiría a los cibercriminales hacerse con una cantidad situada entre 1,14 y 2,78 mil millones de dólares: las pymes serían las más proclives a realizar el pago, mientras que se incrementaría a raíz del ataque la demanda de seguridad informática, subiría la desconfianza en los dispositivos conectados, habría controles más estrictos sobre el uso del email corporativo y la formación en ciberseguridad se convierte en una asignatura obligatoria en el seno de todas las organizaciones.

Desde Panda Security subrayan que para mantenerse a salvo de los ciberataques avanzados es fundamental que las compañías formen a sus empleados, todas las plantillas tomen conciencia de la precaución frente a los mensajes de phishing –aprendiendo a detectar las ciberamenazas especialmente por email-, alertar al equipo de ciberseguridad de la compañía ante esta amenaza -el 87% de las organizaciones han sufrido email phishing- y emplear soluciones de seguridad avanzadas para proteger los datos sensibles y dispositivos corporativos.

Disponible en:
https://computerhoy.com/noticias/tecnologia/seria-ransomware-destructivo-ideado-ahora-376531?fbclid=IwAR2_fMjwbkt0xZecN1wQ1LUgsYqRcDOnt0EdIvbAyio_pP58RS7n9PEOlng

4. EL FACTOR HUMANO, CAUSA Y SOLUCIÓN DE LA CIBERSEGURIDAD

Fecha: 18/02/2019

Más del 43% de los ciberataques buscan explotar el factor humano para sobrepasar las defensas empresariales, pero los trabajadores también pueden ser la respuesta para vencer la guerra al cibercrimen.

Las ciberamenazas y la ciberseguridad constituyen la particular dialéctica que protagoniza muchas conversaciones de la actualidad tecnológica.

Tan solo hemos de atenernos a algunos datos para darnos cuenta de ello: según Cybersecurity Ventures, el gasto mundial en seguridad cibernética aumentará de manera constante para superar el billón de dólares (1 trillion, para los anglosajones) entre 2017 y 2021, mientras que el polo opuesto, el del cibercrimen, supondrá un coste a escala global de 6 trillones al año para 2021.

Inherentemente, algo está mal con cualquier predicción que correlaciona el aumento del gasto en prevención con el aumento de los daños por la penetración exitosa de esas mismas defensas. O dicho de otro modo, no se puede entender que el cibercrimen aumente más rápido conforme invertimos más en defensa.

La causa de esta aparente disonancia está en el fondo de la cuestión. La industria de la seguridad cibernética hoy en día funciona

como una carrera armamentística: cuando se revela una nueva amenaza, se lanza un nuevo parche o actualización para solucionarlo y el ciclo se repite.

De este modo, la inversión en seguridad cibernética continúa aumentando, pero también lo hace el volumen de amenazas.

Para salir de este círculo poco virtuoso se necesita un cambio de paradigma en la forma en que abordamos la ciberseguridad y capacitar a los defensores cibernéticos con las herramientas adecuadas para mitigar la embestida de los ataques digitales.

El peligro humano

Uno de los factores que se minusvaloran y que podría ser un vector importante en ese cambio de paradigma es el factor humano como puerta de entrada de los ataques y violaciones de datos.

Según recoge el Atlantic Council, cada empresa promedio tiene alrededor de 23.000 dispositivos móviles en uso por parte de los empleados.

Por si fuera poco, un reciente informe de Verizon apela a que más del 43% de las violaciones de datos fueron ataques sociales; es decir, que se enfocaron en explotar el punto humano de debilidad en las defensas de seguridad de una organización.

Ahí es donde las compañías han de hacer revisión de sus protocolos, porque todos los analistas destacan la falta de visibilidad y contexto sobre cómo y dónde se usan los datos a medida que éstos se extienden a través de aplicaciones y dispositivos emitidos por la entidad.

Este complejo escenario ofrece a los ciberdelincuentes un campo rico para atacar. Independientemente de cómo se originen los ataques, todos conducen a las mismas intersecciones finales, donde pueden infligir el mayor daño.

Estas intersecciones son puntos en los que las personas interactúan con datos empresariales críticos y propiedad intelectual. Estos “puntos humanos” de interacción tienen el potencial de socavar incluso los sistemas de diseño más completos en un solo acto malintencionado o no intencional.

La salvación humana

Hasta aquí la lectura negativa, pero también hay un hueco para el optimismo. Y es que esos mismos humanos también pueden ser la línea de defensa más fuerte y actuar como señales de advertencia del ciberespionaje y los ataques.

Así pues, implementar un enfoque de seguridad centrado en el ser humano puede hacer sonar la alarma en función del comportamiento cibernético del ser humano y permitir a los defensores mitigar o prevenir la pérdida de datos críticos, independientemente de si la red fue violada.

Nos explicamos: los equipos de seguridad reciben miles de alertas en un día determinado y, como resultado, pierden la batalla cibernética.

Los avances en el comportamiento humano y los análisis de riesgo permitirán a estos cibernéticos identificar más rápidamente las anomalías y obtener el contexto necesario para analizar las alertas de actividad de red maliciosas o malintencionadas.

Y ahí es donde entran en juego las políticas de cumplimiento automatizadas y adaptadas al riesgo que pueden restringir o impedir el acceso a IP confidenciales, dependiendo del nivel de riesgo observado.

En este modelo, además, los equipos de seguridad acumulan la capacidad de comprender, predecir y actuar ante posibles amenazas a medida que se desarrollan… no semanas, meses o años después del incidente.

Finalmente, al cambiar el enfoque de seguridad del modelo tradicional de protección de infraestructura al entendimiento del comportamiento humano, los empleados también pueden ser reclutados para ayudar a asegurar los activos de misión crítica y corporativos.

Esto permite no solo una mayor eficacia de seguridad dentro de una organización, sino que también se compromete con la primera línea de defensa de la organización, los empleados, y los incluye continuamente en la ecuación de seguridad.

Disponible en:
https://www.ticbeat.com/seguridad/el-factor-humano-causa-y-solucion-de-la-ciberseguridad/?fbclid=IwAR2midoIeiqbTaGmLe-azm9O8EgNiSFKsharMNUpaJMBUM9iJVPgZMd-XR8

5. ESTA ES LA NOVEDOSA HERRAMIENTA DE GOOGLE QUE TE DICE CUÁNDO CAMBIAR TU CONTRASEÑA

Fecha: 06/02/2019

Google ha lanzado su nuevo complemento para Chrome llamado Password Checkup. Esta herramienta te avisará cuando tu contraseña sea susceptible de ser robada para que la cambies.

Google ha lanzado una nueva función llamada Password Checkup que se puede instalar en el Chrome. Esta nueva herramienta de Google te dice cuándo cambiar tu contraseña para que esta siga siendo segura.

Este martes el gigante tecnológico anunció su nueva herramienta que avisará a sus usuarios cuando tengan que cambiar sus contraseñas debido a que podrían haber sido robadas.

Este complemento que ya se puede instalar en Chrome de forma sencilla te informa por tanto si es necesario cambiar la contraseña de la cuenta.

“Si detectamos que un nombre de usuario y una contraseña en un sitio que usa es una de las más de 4 mil millones de credenciales que sabemos que se han comprometido, la extensión activará una advertencia automática y le sugerimos que cambie su contraseña”, han explicado desde Google.

Para instalarlo, debes seguir los siguientes pasos:

1. En el navegador Chrome, instala la nueva herramienta de comprobación de contraseña de Google.
2. Presiona “agregar a Chrome”.
3. Confirma que quieres agregar el complemento a Chrome.
4. Saldrá un icono de pantalla en la parte superior derecha de Chrome cuando esté instalado.

Con este complemento, cuando estés navegando en internet y Password Checkup detecte que estás utilizando una contraseña que está en peligro de ser robada, te mostrará una advertencia para que cambies esa contraseña en Google Chrome.

Disponible en:
https://www.ticbeat.com/lab/esta-es-la-novedosa-herramienta-de-google-que-te-dice-cuando-cambiar-tu-contrasena/?fbclid=IwAR1SlDhO_h3lw6V9E_NQbH3YamXfmxePNx50aWKEzaYYskF4U5iTg-wP-8k

TENDENCIAS Y PROYECCIONES TIC

1. SEIS FÓRMULAS PARA MEJORAR NUESTROS HÁBITOS DIGITALES EN 2019

Fecha: 25/02/2019

Los robos de datos, los ataques generalizados con malware y la publicidad ultrapersonalizada fueron los puntos débiles de la vida digital en 2018.

A medida que las tecnologías cambian, también lo hacen las recomendaciones de los expertos sobre seguridad. Acompañando el comienzo del año he elaborado una breve lista de sugerencias que nos permitirán mantener la vida digital a salvo y libre de desinformación manipulativa.

1. Establezca sus límites y no los ignore

Recientemente, como parte de mi investigación, mantuve conversaciones con varios trabajadores sexuales de Europa sobre su privacidad y seguridad digital. Una de las ideas más repetidas fue la siguiente: “La mejor manera de permanecer seguro es establecer unos límites”.

Decida en base a sus preferencias, y anticipándose a las posibles consecuencias, qué datos está dispuesto a compartir en las aplicaciones y en los servicios online y cíñase a esos límites.

De esta forma, cuando la última app del mercado le pida permiso para compartir algo que usted no quiere compartir, estará más preparado para dar una respuesta.

De igual manera, también es buena idea establecer límites en las discusiones en redes en las que está dispuesto a participar. Abandone aquellas conversaciones que, más que ayudarle, le perjudiquen.

También puede resultar útil poner límite al tiempo que queremos dedicar a nuestra seguridad digital, porque de lo contrario puede convertirse en una tarea eterna.

2. Salga de la burbuja informativa

Aquellas personas que acceden a las noticias principalmente (o exclusivamente) a través de las redes sociales están sometidas a los caprichos de los algoritmos que deciden qué mostrar a cada usuario.

Debido al diseño de estos algoritmos, es probable que los lectores solo consuman artículos procedentes de fuentes informativas de su agrado y con las que tienden a estar de acuerdo.

Este aislamiento respecto a otras fuentes informativas con puntos de vista diferentes y de argumentos que podrían modificar su perspectiva contribuye al establecimiento

de niveles sin precedentes de partidismo y confrontación en la sociedad contemporánea.

Existen herramientas gratuitas online, como AllSides o PurpleFeed, que muestran noticias y publicaciones sociales con puntos de vista ideológicos diferentes e identifican la información aceptada por todo el espectro político.

3. Gestione sus contraseñas de manera eficaz

La mayor amenaza para la seguridad de las contraseñas ya no es su complejidad, sino el hecho de que mucha gente reutiliza las mismas claves para todas o la mayoría de sus cuentas. Los investigadores están hartos de crear notificaciones para avisarle cuando una de sus contraseñas ha sido filtrada. Es más seguro utilizar diferentes combinaciones alfanuméricas, especialmente para proteger sus cuentas más valiosas.

Para recordar todas sus contraseñas puede usar un software que las administre o bien optar por el clásico método de baja tecnología: apuntarlas en un papelito.

Aunque le pueda parecer increíble, es mucho más seguro escribirlas que reutilizar la misma clave en todos lados. Obviamente, este sistema solo funcionará si usted confía en que sus allegados no van a intentar entrar en sus cuentas.

4. Active la autenticación multifactor

Añadir un paso extra para el inicio de sesión en sus redes sociales favoritas, sus cuentas de correo o sus cuentas bancarias puede implicar un plus de seguridad.

Los sistemas de autenticación de múltiples factores son los que incluyen un mensaje que contiene un código de seis dígitos que el usuario debe introducir como parte del proceso de inicio de sesión.

Ninguna autenticación multifactor es mejor que otra, pero los mensajes de texto pueden ser fácilmente interceptados o espiados.

Un camino aún más seguro es la utilización de apps que generan códigos de un solo uso.Un elemento físico es un valor añadido para la protección durante el inicio de sesión. Bautsch.

Las personas que cambian a menudo de teléfono móvil o de tarjeta SIM, o simplemente aquellas que deseen una protección adicional, pueden considerar la posibilidad de usar una llave física que se conecta al ordenador para autorizar el inicio de sesión. Su configuración inicial puede llevar algo de tiempo pero, una vez superado el primer paso, funcionan mucho más rápido que los demás métodos.

5. Elimine las aplicaciones que no use

Las aplicaciones para smartphones conocen su ubicación de manera precisa y la comparten con empresas de publicidad y marketing. Solo con llevar el teléfono móvil en el bolsillo, las empresas de seguimiento obtienen información sobre a dónde vamos o cuánto tiempo permanecemos en cada lugar. Además, ciertos detalles técnicos del terminal pueden dar pistas sobre la identidad de su poseedor.Si tiene una app que no utiliza nunca, desinstálela de su teléfono. Si la volviera a necesitar siempre la podrá descargar de nuevo en un momento, pero entretanto no estará

ofreciendo información personal por todas partes.

6. Actualice las aplicaciones que use

Las compañías de software no siempre conocen todas las vulnerabilidades de sus programas. Cuando lanzan actualizaciones, los usuarios no suelen saber si están solucionando un problema grave o un bug irrelevante.

En cualquier caso, los expertos aconsejan actualizar el software sistemáticamente, tanto de los ordenadores como de los dispositivos móviles.

Ya que hemos pasado el 2018 preocupados por si los hackers, los ejecutivos de las grandes tecnológicas y los programadores ávidos de información han estado tratando de robar nuestros datos y explotar nuestras debilidades digitales, intentemos estar más seguros en 2019.

Disponible en:
https://www.ticbeat.com/lab/seis-formulas-para-mejorar-nuestros-habitos-digitales-en-2019/?fbclid=IwAR3_9jDP-YZSkDA7UkU6fpOvaiU3YRj499OZMNRPyQtScLSVbbL8KXyzw78

2. EL SILENCIOSO PERO DEFINITIVO AVANCE DE LOS GEMELOS DIGITALES

Fecha: 20/02/2019

El 75% de organizaciones que implementan proyectos relacionados con el internet de las cosas ya utilizan la tecnología de 'gemelos digitales' o planifican hacerlo en el plazo de un año, según Gartner.

Los gemelos digitales –patrones de diseño de software que representan objetos físicos con el objetivo de comprender el estado del activo, responder a los cambios, mejorar las operaciones de negocio y añadir valor– empiezan a ser usados de forma generalizada.

Así lo pone de manifiesto un reciente informe de Gartner que asevera que el 13% de las organizaciones que implementan proyectos de Internet de las cosas ya utilizan esta tecnología, mientras que el 62% está en el proceso de implantar esta tecnología o planea hacerlo. Como indica Benoit Lheureux, vicepresidente de análisis de Gartner, "los gemelos digitales están entrando lentamente en el mercado.

Predijimos que para 2022 más de dos tercios de las empresas que han implementado IoT habrán desplegado al menos un gemelo digital en producción. Pero podríamos alcanzar ese número en un año".

Valor comercial real

Este rápido crecimiento en la adopción no solo se debe al marketing y evangelización de los proveedores de tecnología, sino también a que los gemelos digitales están aportando valor comercial real, según la firma de análisis, "y se han convertido en parte de la internet de las cosas empresarial y de las estrategias digitales".

Lheureux apunta que aunque la adopción de esta tecnología es idónea para cualquier empresa, lo cierto es que las más avanzadas al respecto son aquellas dedicadas a fabricar productos conectados.

"La oportunidad de diferenciar sus productos y establecer nuevos servicios y flujos de ingresos es un claro motor comercial", según el analista.Por otro lado,

los gemelos digitales sirven a una amplia gama de objetivos empresariales.

"Los diseñadores de gemelos digitales deben tener en cuenta que probablemente necesitarán acomodar a múltiples consumidores de datos y proporcionar puntos de acceso de datos apropiados".

Desde Gartner observan que los gemelos digitales se despliegan cada vez más junto con otros gemelos digitales para adquirir bienes o equipos relacionados. "Sin embargo, la verdadera integración sigue siendo relativamente complicada y requiere habilidades de gestión de la información. La capacidad de integrar gemelos digitales entre sí será un factor diferenciador en el futuro, a medida que evolucionen los activos físicos y los equipos", añade el analista.

Disponible en:
https://www.computerworld.es/tecnologia/el-silencioso-pero-definitivo-avance-de-los-gemelos-digitales?fbclid=IwAR1rLQMa06ls98UiTXMqYcAQdiB6kv6uCFrXihmh32gFHmntbBr3IRwNG5o

USO SOCIAL DE LAS TIC

1. LOS NIÑOS QUE PASAN DEMASIADO TIEMPO DELANTE DE UNA PANTALLA TIENEN UN DESARROLLO COGNITIVO MÁS LENTO, AFIRMA UN ESTUDIO

Fecha: 16/02/2019

Los niños pequeños que pasaron más tiempo mirando una pantalla a los dos años de edad obtuvieron peores resultados en los marcadores de desarrollo que aquellos que pasaron menos tiempo mirando una pantalla.

La ciencia arroja cada vez más luz sobre los negativos efectos de las pantallas (televisores, tablets y, por encima de todo, smartphones) sobre el crecimiento y la vida de los más pequeños de la casa.

El último estudio en unirse a la lista es el realizado por los investigadores canadienses de la Universidad de Waterloo, la Universidad de Calgary y el Instituto de Investigación del Hospital Infantil de Alberta, según el cual existe una relación directa entre el desarrollo cognitivo de los niños y el tiempo que pasan frente a las pantallas.

Así pues, de acuerdo a su trabajo -publicado en la revista JAMA Pediatrics– los niños pequeños que pasaron más tiempo mirando una pantalla a los dos años de edad obtuvieron peores resultados en los marcadores de desarrollo que aquellos que pasaron menos tiempo mirando una pantalla.

Una conclusión extremadamente preocupante si tenemos en cuenta que los niños de dos años pasaban unas 17 horas a la semana frente a una pantalla.

Esa cantidad aumenta a 25 horas por semana a los tres años antes de caer a 11 horas por semana a los 5 años. Al menos así ocurrió con la muestra de 2.400 pequeños que utilizaron los científicos para su investigación.

"Cuando los niños pequeños están observando pantallas, pueden perder

oportunidades importantes para practicar y dominar las habilidades interpersonales, motoras y de comunicación“, explica el documento, no exento de críticas.Y es que, algunos expertos han denunciado que el estudio no toma en cuenta para qué usaban los niños las pantallas u otros factores, como el patrón de sueño o los ingresos familiares.

Muchas pistas negativas

Sea del todo preciso o peque de algún fallo metodológico, este estudio no está solo al exponer los riesgos de las pantallas en la vida de los pequeños.Hace poco recogíamos otro estudio de la también canadiense Universidad de Guelph, según el cual los niños cuyo tiempo de pantalla está controlado como una recompensa o un castigo pasan más tiempo frente a sus dispositivos electrónicos que aquellos niños que no están disciplinados de esa manera.

Más grave si cabe es el trabajo del Instituto Suizo de Salud Tropical y Pública (Swiss TPH) que sugiere que la radiación de los teléfonos inteligentes está impactando negativamente en la memoria de los adolescentes, fomentando las pérdidas de memoria a corto plazo. En concreto, los científicos estiman que un año de radiación podría ser suficiente para dañar la parte del cerebro que interpreta imágenes y formas.

Disponible en:
https://www.ticbeat.com/educacion/los-ninos-que-pasan-demasiado-tiempo-delante-de-una-pantalla-tienen-un-desarrollo-cognitivo-mas-lento-afirma-un-estudio/

2. BRUSELAS PROMUEVE EL INTERCAMBIO DE HISTORIALES MÉDICOS ELECTRÓNICOS EN LA UE

Fecha: 06/02/2019

La Comisión Europea lanza unas recomendaciones para desarrollar un sistema seguro que permita a los ciudadanos de la UE acceder a sus historias médicas electrónicas en todos los Estados miembros.

Las personas reclaman un acceso en línea seguro y completo a sus propios datos sanitarios, dondequiera que estén. Los profesionales de la salud necesitan un historial médico fidedigno para prescribir tratamientos con mayor rapidez y conocimiento de causa. Nuestros sistemas sanitarios necesitan los mejores recursos para ofrecer la mejor atención personalizada.

Juntos, debemos agilizar y fomentar el intercambio seguro de historiales médicos electrónicos en toda la UE. Esto mejorará la vida de los ciudadanos y ayudará a los innovadores a encontrar la próxima generación de soluciones digitales y tratamientos médicos”, en palabras del vicepresidente Andrus Ansip, responsable de Mercado Único Digital.

En la actualidad, la capacidad de los ciudadanos europeos de acceder a esos historiales en toda la UE varía considerablemente según los países. Algunos ciudadanos pueden acceder a parte de sus historiales médicos electrónicos a nivel nacional o transfronterizo, pero otros tienen un acceso digital limitado o nulo.

Con las nuevas recomendaciones de la Comisión se facilitará un acceso transfronterizo seguro y en plena conformidad con el Reglamento general de protección de datos.

Los Estados miembros ya han empezado a hacer accesibles e intercambiables a través de las fronteras algunas partes de los historiales médicos electrónicos.

Desde el 21 de enero de 2019, los ciudadanos finlandeses pueden comprar medicamentos utilizando sus recetas electrónicas en Estonia y los médicos luxemburgueses pronto podrán acceder a los historiales médicos de los pacientes checos. Las recomendaciones presentadas hoy proponen que los Estados miembros amplíen esto a tres nuevos ámbitos del historial médico: pruebas de laboratorio, informes de alta médica e imágenes e imaginería médicas.

La iniciativa facilita también la elaboración de las especificaciones técnicas que deberán utilizarse para intercambiar historiales médicos en cada caso.

Para seguir fomentando este intercambio de información, se establecerá un proceso conjunto de coordinación entre la Comisión y los Estados miembros. Esto permitirá recibir contribuciones y opiniones de las partes interesadas, tales como representantes del sector, profesionales de la salud y representantes de los pacientes, tanto a nivel nacional como de la UE.

Disponible en:
https://www.computerworld.es/tecnologia/bruselas-promueve-el-intercambio-de-historiales-medicos-electronicos-en-la-ue?fbclid=IwAR0TpBesOB2o30iT29K_zZpF-GcI26ome9Q6uII10jg0xZ54ORQUNFxYIIY

REPÚBLICA DE CUBA
MINISTERIO DE COMUNICACIONES

Sistema de Vigilancia Tecnológica