



Contenido

INTELIGENCIA ARTIFICIAL	2
IMPRESIÓN EN 3D.....	5
SEGURIDAD INFORMÁTICA	6
TENDENCIAS Y PROYECCIONES TIC	12
USO SOCIAL DE LAS TIC	18



Sistema de Vigilancia Tecnológica

Ministerio de Comunicaciones

Julio, 2019



INTELIGENCIA ARTIFICIAL

1. ASÍ ES TRACK AI, LA INTELIGENCIA ARTIFICIAL QUE IDENTIFICA TRASTORNOS VISUALES INFANTILES

Fecha: 29/07/2019

La tecnología cobra todo su sentido cuando está orientada a conseguir un beneficio real sobre la vida de las personas. Track AI es un sistema que utiliza la inteligencia artificial y el machine learning de Huawei para detectar y diagnosticar los signos prematuros de problemas de visión en niños.



La Organización Mundial de la Salud estima que en el mundo hay unos 19 millones de niños con problemas de visión que no han sido tratados, de los cuales entre el 70 al 80 por ciento se pueden prevenir o curar.

Cuando el uso de una tecnología como la inteligencia artificial es capaz de marcar diferencias en la vida de millones de personas, podemos afirmar, sin lugar a dudas, que se ha conseguido un hito para todo el conjunto de la humanidad.

Cuando un diagnóstico a tiempo marca la vida de una persona

Track AI es una de esas tecnologías diferenciales que pueden marcar profundamente la vida de millones de personas en todo el planeta, consiguiendo mejorarla de forma definitiva independientemente de su lugar de origen. No importa si el paciente reside en el centro de Nueva York o en una remota aldea de Etiopía.

Huawei está trabajando con IIS Aragón y DIVE Medical para el co-desarrollo de Track AI, un sistema que, mediante inteligencia artificial es capaz de detectar los patrones de visuales de niños con problemas de visión a los que todavía no se les ha diagnosticado, y que por su corta edad no siempre es posible comunicarse.

Esta falta de diagnóstico eficiente pesa como una losa en la vida de esos niños ya que les influye en su desarrollo general provocándoles problemas de retraso educativos y oportunidades sociales.

Gracias a Track AI se les proporciona un diagnóstico rápido y eficaz para unas enfermedades que, por su naturaleza y el perfil de sus pacientes, resulta complicado realizar una detección temprana. Algo que la inteligencia artificial sí consigue.

Un equipo de diagnóstico DIVE completo bajo el brazo

El proyecto Track AI tiene como misión alcanzar un mundo sin discapacidad visual en los niños, por lo detectar trastornos visuales de forma precoz es una de las piezas clave para tratarlos de forma inmediata y, en muchos de esos casos, conseguir la curación total del paciente.

Para ello se realiza una batería de pruebas específicas mediante software DIVE (Dispositivos Integral para una Visión Examinadora) que presenta una serie de estímulos visuales en la pantalla de un portátil MateBook X Pro de Huawei, un dispositivo portátil que cabe perfectamente en la mochila de cualquier médico oftalmólogo del mundo.

A través del hardware de este dispositivo y de su webcam es posible monitorizar y rastrear la mirada del paciente para determinar su patrón de respuesta a los



estímulos. Todos los datos que recoge el software DIVE se transmiten a un Huawei P30 donde, gracias a la NPU de doble núcleo del procesador Kirin 980, se pueden analizar todos los datos recogidos.

Las dos unidades dedicadas de procesamiento neural integradas en el procesador de los Huawei P30 permiten la ejecución local de algoritmos de inteligencia artificial Huawei HiAI con el fin de detectar patrones del comportamiento en la respuesta a los estímulos visuales generados durante la prueba con el software DIVE.

Esta capacidad de procesamiento de la inteligencia artificial de los Kirin 980 que monta el Huawei P30 evita la necesidad de una transferencia constante de datos permitiendo almacenar los datos en el propio smartphone, por lo que la prueba se puede llevar a cabo incluso cuando no existe una conexión de datos, lo cual facilita la movilidad y supone una garantía para la privacidad de los resultados.

Gracias al uso de esta inteligencia artificial es posible detectar patrones anómalos que indicarían la presencia de un problema visual y tomar las acciones adecuadas para corregir los problemas de visión del paciente.

Lo que Huawei aporta al proyecto Track AI es una base de hardware potente, portátil y accesible en el que solo se necesita un ordenador portátil potente como el Huawei MateBook X Pro y un Huawei P30 para diagnosticar trastornos visuales en niños tan pronto como sea posible y sin límites geográficos.

Un esfuerzo internacional para un beneficio global

Entrenar una inteligencia artificial para que sea capaz de detectar sutiles indicios en el seguimiento de un estímulo que revele la

presencia de un trastorno visual requiere de un gran esfuerzo y la recopilación de datos diagnósticos de cientos de miles de pacientes.

Esta colaboración se ha extendido de forma internacional donde Huawei y Dive han formado un equipo formado por 18 oftalmólogos de cinco instituciones médicas en España, Vietnam, México, los Emiratos Árabes Unidos y China han iniciado la fase de recopilación de datos de mirada con el fin de crear una base de conocimiento sobre la que entrenar a la inteligencia artificial.

En este sentido la proyección internacional de Huawei ha sido clave para lograr la implicación en proyecto de países como Reino Unido, México, España, Rusia, China o Vietnam.

Lograr mejorar la vida de millones de niños con trastornos de visión con un smartphone, un portátil y la inestimable ayuda de la inteligencia artificial Huawei HiAI como únicas herramientas de diagnóstico, supone un hito del que toda la humanidad debería estar orgullosa.

Disponible en:

<https://computerhoy.com/patrocinado/tecnologia/track-ai-inteligencia-artificial-identifica-trastornos-visuales-infantiles-460899>

2. ANTES DE COMPRAR, LA INTELIGENCIA ARTIFICIAL PREDICE SI UN USUARIO DEVOLVERÁ UN PRODUCTO

Fecha: 04/07/2019

Investigadores de Google y la empresa india de comercio electrónico Myntra Designs han desarrollado una inteligencia artificial que puede predecir la probabilidad de que un cliente devuelva un producto antes de la compra.



Con este fin, los investigadores capacitaron un modelo de aprendizaje automático en un conjunto de datos de preferencias, formas corporales y productos vistos por los minoristas. Para identificar qué factores tuvieron un efecto importante en la devolución de un producto, los investigadores analizaron la plataforma de comercio electrónico de Myntra Designs. Contiene alrededor de 600.000 productos y millones de pedidos se procesan cada semana.

Entrenamiento modelo

Los investigadores descubrieron que de todos los productos devueltos, el 4% ocurrió cuando había una cantidad de productos similares en un carrito de compras. El 53% de los productos devueltos son el resultado de problemas con el tamaño y la forma en que un producto se ajusta. La posibilidad de productos devueltos también parece depender en gran medida de cuánto hay en un carrito de compras. Si hay cinco productos, la probabilidad es del 72% en comparación con el 9% de los carritos de la compra con un solo producto.

Con estas ideas, el equipo creó un llamado "modelo doble híbrido" para predecir la posibilidad de devolver carritos de la compra completos, así como algunos

artículos. Un clasificador de IA de nivel superior clasificó los carros retornables. Un segundo clasificador, que se basa en los carritos de la compra clasificados, predice la probabilidad de que un producto individual sea devuelto.

Ambos clasificadores fueron capacitados en un conjunto de datos con muestras de tres

categorías, con información como la marca, la antigüedad del producto, el tamaño del carrito de compras, el día y la hora del pedido, la ciudad a la que debe ir, el método de pago y cómo. a menudo se ordenaba algo.

Resultados

El sistema de IA con mejor rendimiento fue capaz de predecir con una precisión del 74% si un artículo se devolvería o no. Además, el sistema logró un área de 82.3% por debajo de la característica operativa del receptor, que es una forma de determinar la precisión de detección.

En una prueba en vivo con 100.000 usuarios, el número de pedidos se redujo ligeramente (en un 1.7%) en comparación con un conjunto de control. El porcentaje de productos devueltos disminuyó un 3 por ciento.

El equipo argumenta que puede ser útil determinar qué clientes pueden devolver un producto porque un minorista puede actuar de antemano. Esto puede ser, por ejemplo, la personalización de los gastos de envío.

Disponible en:

<https://www.computerworld.es/tendencias/antes-de-comprar-la-inteligencia-artificial-predice-si-un-usuario-devolvera-un-producto>



IMPRESIÓN EN 3D

1. UN RESTAURANTE DE TOKIO IMPRIME SUSHI PERSONALIZADO EN 3D SEGÚN TUS FLUIDOS BIOLÓGICOS

Fecha: 05/07/2019

Por extravagante o surrealista que parezca, esta noticia es real como la vida misma. Un restaurante de Tokio analizará las muestras biológicas de sus clientes para fabricar piezas de sushi personalizado gracias a la impresión 3D.



Mientras que es común entre los restaurantes de alta gama que los comensales hagan reserva previa para conseguir mesa, en Sushi Singularity en Tokio, los requisitos son un poco diferentes. El local nipón solicitará a los potenciales clientes el envío de muestras fecales para personalizar al máximo la experiencia de degustar este manjar tan propio de la cultura japonesa. Según la información del medio designboom, el nuevo restaurante de Open Meals creará recetas de sushi personalizadas para satisfacer las necesidades nutricionales de cada cliente.

Open Meals es harto conocido por sus proyectos de alimentos experimentales, como el concepto de “teletransportación de sushi”, fundamentado en brazos robóticos que sirven sushi en forma de cubos impresos en 3D. Ahora, la concepción futurista de este plato combina el poder de los datos con la creatividad y las posibilidades propiciadas impulsadas por la

poderosa tecnología de impresión 3D.

Los invitados que planean comer en Sushi Singularity recibirán un kit de pruebas de salud por correo, con viales para recolectar materiales biológicos como orina, saliva y heces. Tras el envío se analizará el genoma y el estado nutricional del cliente, teniendo una especie de ID de salud de cada cliente. Con esa información, Sushi Singularity elabora recetas de sushi personalizadas, optimizando los ingredientes con los nutrientes más necesarios para el organismo del comensal. El restaurante utiliza una máquina para inyectar vitaminas y minerales crudos directamente en los alimentos.

Para hacer las cosas aún más distópicas, todo el sushi en Sushi Singularity será producido por una impresora 3D con brazos robóticos gigantes. Los elementos del menú aprovechan al máximo la tecnología. Por ejemplo, cuenta con atún de cultivo celular, láser de CO2 o un modelo altamente detallado de un castillo japonés hecho de calamares congelados.

En lo tocante a la fecha, la compañía planea lanzar Sushi Singularity en Tokio en algún momento del año 2020. No serán los primeros robots de sushi que se lanzarán en Japón: el servicio de entrega de alimentos Ride On Express ya debutó con robots de entrega en el país nipón el pasado año 2017.

Disponible en:

<https://www.ticbeat.com/innovacion/un-restaurante-de-tokio-imprime-sushi-personalizado-en-3d-segun-tus-fluidos-biologicos/>



SEGURIDAD INFORMÁTICA

1. ¿CUÁL ES LA FORMA CORRECTA DE MEDIR LA TEMPERATURA DE LA CPU DE TU ORDENADOR?

Fecha: 18/07/2019

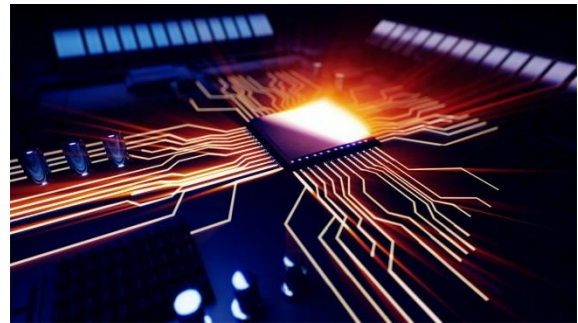
Mantener la temperatura del PC en unos límites seguros es necesario, pero ¿cuál es la forma correcta de medir la temperatura de la CPU de tu ordenador? Te lo contamos al detalle.

Trabajar a una temperatura elevada puede acortar la vida útil de los componentes de tu PC y provocar graves daños a algunos de ellos. Te mostramos cuál es la forma correcta de medir la temperatura de la CPU de tu ordenador para que te puedas asegurar de que tu ordenador está funcionando tal y como debería. Además, esto es algo vital de cara al verano para saber si necesitamos, o no, más ventiladores o mejor refrigeración en el PC.

Componentes como la tarjeta gráfica o la CPU integran mecanismos que hacen que baje su rendimiento si alcanzan temperaturas demasiado altas para evitar que se dañen por un exceso de temperatura, provocando que su rendimiento se sitúe por debajo de lo que realmente permite.

Si tu ordenador comienza a funcionar más lento cuando lleva ya un rato funcionando o sufre reinicios sin motivo aparente, es más que probable que tenga problemas de temperatura, por lo que no está de más que sigas nuestros consejos para monitorizar las temperaturas de la CPU de tu ordenador.

Monitoriza la temperatura desde el propio procesador



Intel y AMD son los dos fabricantes principales de procesadores para ordenadores de escritorio y ordenadores portátiles. Ambos fabricantes cuentan con sus propios softwares de monitorización del funcionamiento de sus procesadores.

Entre los parámetros que monitorizan estos programas también se muestra la temperatura a la que está trabajando el procesador.

Si tienes un procesador Intel, descarga la herramienta Intel XTU (Extreme Tuning Utility) desde su página web oficial. Esta herramienta se utiliza para monitorizar los parámetros de funcionamiento del procesador durante el proceso de Overclocking, por lo que la temperatura del procesador se muestra de forma constante en la parte inferior de la ventana del programa.

Son preocupantes unos valores por encima de los 65 grados, aunque cada procesador soporta una temperatura distinta. Como norma general, si marca 70 grados es que el equipo necesita una revisión de su refrigeración de forma urgente.

Si tu PC monta uno de los nuevos Ryzen de AMD, también puedes monitorizar su funcionamiento y, al igual que en el caso de Intel, mantener bajo control las temperaturas de tu PC.



En el caso de los AMD la herramienta que necesitas es AMD Ryzen Master que también puedes descargar desde la propia web de AMD. El propósito de la herramienta es exactamente el mismo que veíamos en el caso de Intel XTU, monitorizar el funcionamiento del procesador durante el proceso de Overclocking.

En este caso la temperatura del procesador Ryzen se muestra en la parte superior izquierda de la ventana de AMD Ryzen Master.

Cómo medir la temperatura de tu PC con software de terceros

Si el procesador de tu PC ya tiene un cierto tiempo y no es compatible con las herramientas que te hemos propuesto para medir la temperatura de la CPU de tu ordenador, necesitarás usar un software de terceros para hacerlo.

Este tipo de software ofrece un soporte para procesadores mucho más extenso y utiliza los sensores de la placa base para realizar la lectura de los valores de temperatura de los componentes.

Uno de los programas para medir la temperatura del PC más sencillos de usar es HWMonitor que puedes descargar gratis desde su página web.

Este programa está disponible en formato instalable, de forma que se descarga un archivo .exe, o en formato no instalable descargando un archivo Zip que incluye los ejecutables para 32 y 64 bits. Cualquiera de los dos formatos funciona de forma idéntica.

HWMonitor realiza una lectura más extensa, aunque como decimos, sus datos están basados en las lecturas de los sensores de la placa base, por lo que la cantidad de información que será capaz de mostrar dependerá en gran medida de la disponibilidad y precisión de esos sensores.

De cualquier modo, sus lecturas te mostrarán de forma muy aproximada si el procesador de tu ordenador está sufriendo un exceso de temperatura.

En la ventana de HWMonitor se listan los componentes principales que forman tu PC: placa base, CPU, memoria RAM y el sistema de almacenamiento. Cada uno de ellos ofrece una lectura de su temperatura, por lo que para conocer la temperatura a la que está trabajando el procesador de tu PC solo tienes que desplegar los datos del apartado Temperatures del procesador.

Lo interesante de este programa es que no solo te muestra la temperatura actual del procesador (o de cualquier otro componente), sino que también te muestra los valores mínimos y máximos que ha registrado.

Este rango te da una idea más fiable de las temperaturas a las que trabaja el procesador, sobre todo cuando debe enfrentarse a mucha carga de trabajo.

Sondas para medir la temperatura del procesador

Medir la temperatura mediante herramientas por software es una forma rápida, sencilla y barata para medir la temperatura de la CPU de tu ordenador, pero no es la única.

También puedes utilizar la sonda de temperatura que integran algunos sistemas de control de ventiladores o rehubos.

Algunos de estos sistemas de control de ventiladores, además de graduar la velocidad de rotación de los ventiladores instalados adecuando el nivel de ruido a la carga del equipo, también vienen equipados con sondas de temperatura para mostrar ese dato en las pantallas del propio controlador.



Control de temperatura desde el corazón de tu PC

Podríamos considerar a la BIOS o UEFI de tu PC como el corazón mismo de tu ordenador ya que es aquí donde se hace posible que todos los componentes funcionen de forma conjunta.

Tal y como comentábamos en el apartado en el que hablábamos de HWMonitor, la placa base cuenta con una serie de sensores que permiten obtener una lectura de los valores de temperatura de los componentes de tu PC.

La BIOS o UEFI de tu PC también puede acceder a esos valores y mostrarlos en pantalla, por lo que también puedes usarlos para hacerte una idea de su temperatura.

Obviamente esta función es muy limitada ya que mientras se encuentra ejecutando la BIOS o UEFI el sistema operativo todavía no se ha cargado, por lo que solo se dispone de la temperatura del procesador en reposo o con un uso muy reducido, y no bajo una carga de trabajo normal que es como debe medirse la temperatura de la CPU de tu ordenador.

Así que, una vez que sabéis cómo medir la temperatura del PC, solo hay que poner arreglo. Si es una torre, es más sencillo utilizando ventiladores nuevos más potentes o un sistema de refrigeración líquida, que ha bajado de precio estos últimos años. Si es un portátil, una vez limpiados los componentes internos... solo nos queda añadir una base con ventilador, como esta, para intentar disipar el calor.

Disponible en:

<https://computerhoy.com/reportajes/tecnologia/cual-forma-correcta-medir-temperatura-cpu-ordenador-450337>

2. CONSEJOS PARA AUMENTAR LA CONFIANZA DEL CONSUMIDOR EN LA SEGURIDAD Y LA PRIVACIDAD DE LOS DATOS

Fecha: 10/07/2019

Las violaciones de datos de alto perfil y las amenazas de seguridad cada vez más sofisticadas están impulsando a las marcas inteligentes a gestionar mejor las cantidades masivas de datos de consumo que han pasado años recopilando.



Las violaciones de datos de alto perfil y las amenazas de seguridad cada vez más sofisticadas están impulsando a las marcas inteligentes a gestionar mejor las cantidades masivas de datos de consumo que han pasado años recopilando. Para ello, las marcas deben priorizar los intereses de sus clientes y construir una estrategia moderna de seguridad de datos y privacidad donde la confianza del consumidor es fundamental.

Estos son algunos consejos para construir una estrategia exitosa de seguridad y privacidad de los datos de los clientes en la era del consumidor:

1. Cambie el enfoque de la mitigación de riesgos a la protección proactiva de la identidad.

Los líderes en seguridad y privacidad necesitan apoyo multifuncional para implementar una estrategia de gestión de datos exitosa y orientada al cliente. Permita



que otros grupos hagan que la seguridad de los datos y la privacidad sean fundamentales para sus prácticas empresariales, en lugar de mitigar las violaciones de la privacidad y la seguridad de los datos solo cuando se producen. Al adoptar las mejores prácticas de seguridad y privacidad a lo largo del viaje de un cliente, desde el marketing digital hasta el registro y la autenticación online, pasando por la gestión de preferencias, el almacenamiento de datos, etc..., aumentará la confianza de los consumidores.

2. Permita que sus clientes gestionen sus datos.

No hace falta decir que una estrategia de seguridad de datos y privacidad de extremo a extremo implica su techstack (diagrama en el que se representa el flujo de gestión de Marketing Digital y la arquitectura tecnológica que lo soporta). Eche un vistazo a los proveedores de soluciones y a las plataformas internas que utilizan sus equipos de marketing, comercio electrónico, sitio web, servicio al cliente y otros equipos multifuncionales para capturar, gestionar y proteger los datos de los consumidores. Asegúrese de que permiten el cumplimiento de las normativas regionales de privacidad de datos y de que se alinean con su estrategia de gestión de datos prioritaria para el cliente. Un punto de referencia crítico: los clientes deben poder acceder y gestionar sus datos de perfil y preferencias. Esto tiene varios beneficios de marca, incluyendo el cumplimiento de la privacidad de los datos, el aumento de la confianza de los clientes y la mejora de los datos de primera mano.

3. Cree una cultura en la que el cliente sea el primero en implementar su estrategia.

Una vez que construya su estrategia de seguridad de datos y privacidad, debe

implementarla de manera efectiva. Cree una cultura empresarial que respete los datos de los clientes permitiendo que sus líderes interfuncionales compartan información y mejores prácticas con sus equipos. Promulgue una política de privacidad y seguridad de datos aplicable y proporcione a sus empleados las herramientas para seguirla. Al crear una cultura en la que el cliente es lo primero, su empresa cosechará las recompensas de forma multifuncional: cumplimiento de la privacidad de los datos, protección frente a las violaciones de datos, mejores datos de primera mano para una mejor personalización, clientes más comprometidos y una mayor lealtad a la marca.

Disponible en:

<https://cso.computerworld.es/tendencias/consejos-para-aumentar-la-confianza-del-consumidor-en-la-seguridad-y-la-privacidad-de-los-datos>

3. LAS IMPLICACIONES DE PSD2 EN CIBERSEGURIDAD

Fecha: 09/07/2019

La nueva directiva quiere garantizar la correcta identificación de los usuarios cuando realizan sus compras, y para ello obliga a la utilización de dos factores de autenticación diferentes.



La consecución del Mercado Único Digital (MUD) europeo pasa, de manera transversal, por contar con una buena estrategia de ciberseguridad en el Viejo Continente tanto a nivel público como



privado. Por eso, el sector de pagos está viviendo una profunda transformación que el próximo mes de septiembre vivirá un nuevo capítulo con la llegada de la segunda Directiva sobre Servicios de Pago (PSD2, de sus siglas inglesas). Con su entrada, será obligatorio utilizar la autenticación de cliente reforzada (SCA, en inglés), término que define las normas de seguridad que regirán el uso de las últimas tecnologías en el ámbito de los pagos digitales, como las soluciones en el ámbito biométrico.

Según Alberto López, responsable de ciberseguridad y soluciones digitales para España y Portugal de Mastercard, “la autenticación reforzada será fundamental en el ecosistema de pagos, que deberá adoptar distintas medidas para implantar el nuevo estándar de seguridad establecido por la legislación europea”.

La nueva directiva quiere garantizar la correcta identificación de los usuarios cuando realizan sus compras, y para ello obliga a la utilización de dos factores de autenticación diferentes entre algo que el usuario tiene, como el teléfono móvil o una tarjeta, algo que el usuario solo conoce (una contraseña) y algo que el usuario es (huella dactilar, reconocimiento facial...).

Según un estudio realizado por la propia Mastercard, el 75% de los comercios electrónicos minoristas de Europa no está al corriente del nuevo estándar de seguridad. A pesar de los cambios legislativos, solo un 14% de esta muestra ha implantado ya la SCA, mientras que un 51% afirma que no lo hará antes de septiembre o, directamente, no tiene planes para hacerlo.

En la actualidad, un 80% de los ciudadanos europeos compra a través de su teléfono móvil (aunque el nivel de abandono de estas operaciones antes de finalizar la transacción es elevado y ronda el 25%). “El

comercio electrónico sigue ganando terreno al físico y es fundamental garantizar que las transacciones digitales sean seguras y cómodas”, ha señalado López.

Disponible en:

<https://cso.computerworld.es/tendencias/las-implicaciones-de-psd2-en-ciberseguridad>

4. PROTEGER LAS APLICACIONES CRÍTICAS; UNA CUESTIÓN DE NEGOCIO

Fecha: 03/07/2019

El 58% de las organizaciones ya ha sufrido durante los dos últimos años pérdidas de información, problemas de integridad o interrupciones del servicio que afectan a sus aplicaciones.



La ciberseguridad muta a velocidades de vértigo. Y, en consecuencia, las estrategias de las empresas deben estar en continuo reciclaje y prestar siempre atención a las nuevas tendencias, procesos y tecnologías para contar con una protección efectiva de sus negocios. En definitiva, la ciberseguridad se ha convertido en un elemento transversal, quizá el más importante, de toda compañía que se haga llamar digital. Para disfrutar de la explotación de los datos o de las bondades del comercio online, por ejemplo, es necesario tener buenos sistemas de detección, prevención y respuesta ante amenazas, asegurar la disponibilidad y contar con el talento técnico imprescindible.



Pero, decíamos, el primer imperativo es saber en qué paradigma estamos, conocer qué es lo que hay que defender y cómo. Ya no nos movemos en un entorno en el que la mayoría de los datos de las empresas se encuentran físicamente en las instalaciones y solo tenían que hacer hincapié en la seguridad de la red y los dispositivos, basándose en un perímetro sólido. Pero el perímetro se ha difuminado y los atacantes pueden entrar a las compañías mediante cualquier vector. Una de esas puertas de entrada la conforman las aplicaciones críticas, muchas de ellas ya en la nube. Más si tenemos en cuenta que en España no se está dando la prioridad necesaria a su seguridad. Según un estudio de Cyberark, el 73% de las empresas locales no le da la importancia suficiente a este aspecto. Una estadística que choca con los casos reales de uso porque más de la mitad de los encuestados reconoce que incluso el menor tiempo de inactividad que afecte a estas herramientas puede suponer graves impactos en el negocio. Además, el 58% de las organizaciones ya ha sufrido durante los dos últimos años pérdidas de información, problemas de integridad o interrupciones del servicio que afectan a sus aplicaciones. A pesar de ello, un 75% de los encuestados piensa que puede detener de manera eficaz los ataques a la seguridad de los datos o infracciones en el perímetro. Los números son peligrosos si tenemos en cuenta que desde los sistemas bancarios, el I+D, hasta el servicio al usuario y la cadena de suministro se ejecutan con aplicaciones críticas.

Obviamente, lo que se considera crítico puede variar en función del sector industrial y de cada empresa: desde Office 365 hasta los sistemas de planificación de recursos empresariales (los llamados ERP). En cualquier caso, explican desde Cyberark, su alteración influye inmediatamente en los resultados económicos y la pérdida de datos comprometidos comporta riesgos

comerciales y fiscales permanentes. Por ejemplo, el coste medio de un ataque a un sistema ERP oscila en torno a los 5,5 millones de dólares. O, una alteración en un software de gestión con el cliente (CRM, de sus siglas inglesas) puede afectar a la continuidad de los procesos de ventas y fidelización de clientes.

Cómo proteger las aplicaciones críticas

Para poder cimentar una estrategia de defensa efectiva, lo primero que hay que tener en cuenta es de dónde vienen los ataques. El 80% de las filtraciones de datos guarda relación con credenciales privilegiadas comprometidas, como contraseñas, tokens, claves y certificados, según la consultora Forrester. Por ello, proteger las aplicaciones comerciales críticas significa que el acceso debe estar reservado a personas o máquinas con las credenciales y permisos adecuados. Este tipo de herramientas ahora operan en entornos locales, en la nube y a través de aplicaciones SaaS y, en muchas ocasiones, mediante una combinación de las tres. En este contexto, hay una gran variedad de usuarios privilegiados que requieren acceso: empleados que trabajan tanto en instalaciones como en puntos finales remotos, socios externos o proveedores y desarrolladores que introducen cambios en dichas aplicaciones. Por otra parte, las credenciales privilegiadas también están integradas en las interacciones máquina a máquina. De este modo, hay que administrar y rastrear de manera efectiva los accesos sin desequilibrar los presupuestos. Pero, ¿cómo operar eficientemente en este paradigma tan complejo? Desde Cyberark han desglosado cinco claves.

La primera es identificar qué aplicaciones son verdaderamente críticas para la empresa. El responsable de ciberseguridad debe saber las funciones clave de finanzas,



marketing y recursos humanos. Así, estará mejor posicionado para identificar las aplicaciones comerciales más relevantes para su negocio. En segundo lugar, y en un mundo en el que el término cloud es más que una tendencia, familiarizarse con la nube y protegerla es un imperativo. El Ciso debe entender cuál es su estrategia en este ámbito, su plan de migración y lo que se está desplazando hacia la nube. Asociarse con los interlocutores multifuncionales para garantizar que la seguridad de acceso privilegiado es una consideración prioritaria a la hora de migrar aplicaciones a la nube o de adoptar nuevas.

Asimismo, hay que proteger el acceso de los administradores que gestionan las aplicaciones comerciales críticas. Es necesario almacenar y rotar todas las contraseñas relacionadas con estas aplicaciones, incluida la infraestructura subyacente. También es necesario realizar

un seguimiento de auditoría completo de todas las actividades privilegiadas que involucren a estas herramientas. Por supuesto, no hay que olvidarse de las máquinas. El uso de credenciales de codificación fija comporta un riesgo de seguridad importante y debería erradicarse.

Por último, se vuelve imprescindible limitar el riesgo derivado de las estaciones de trabajo de usuarios finales no administradas. Para ello, hay que eliminar los derechos de administrador local para evitar la descarga de virus. Hay que invertir también en protección contra el phishing y en formación y concienciación para que los usuarios sean capaces de reconocer este tipo de amenazas.

Disponible en:

<https://cso.computerworld.es/tendencias/las-implicaciones-de-psd2-en-ciberseguridad>

TENDENCIAS Y PROYECCIONES TIC

1. EL ORIGEN DE NOMBRES DE LA INFORMÁTICA QUE NUNCA HUBIERAS IMAGINADO

Fecha: 20/07/2019



¿Por qué decimos "voy a rípear un CD" o a un fallo se le llama "bug"? Usamos muchas palabras curiosas en informática, y algunas de ellas tienen orígenes inesperados. Vamos a echar un vistazo al origen de nombres de la informática que nunca hubieras imaginado.

La informática lleva con nosotros apenas 80 años. Cuando nació, era un mundo completamente nuevo y no existían las palabras para llamar a las cosas. ¿Quién las inventó? ¿Por qué usamos términos como "ratón" o "spam" con un significado muy diferente a la palabra original? Vamos a descubrir el origen de nombres de la informática que nunca hubieras imaginado.

Cuando nació la informática, a principios del siglo XX, solo estaba al alcance de algunos privilegiados. Los primeros informáticos eran académicos, investigadores, militares y profesores universitarios. No brillaban por su originalidad a la hora de poner los nombres a la cosas, así que los primeros tecnicismos de la informática eran muy aburridos.

Un programa se llama así porque es una



lista de tareas redactada con antelación (programadas), y un lenguaje de programación recibe el nombre porque, bueno, sirve para comunicarse con el ordenador. Un ordenador es una máquina que ordena datos. Todo muy lógico, pero también muy obvio y aburrido.

Aún peor son los acrónimos, que también abundan en la informática. Un PC es un Personal Computer (computadora personal) y una LAN es una Local Area Network o Red Local. La memoria RAM es Random Access Memory o Memoria de Acceso Aleatorio. Y así podríamos seguir hasta dormirnos.

Por suerte, la informática llegó a la gente de la calle en los años 70 del pasado siglo, con el nacimiento de los ordenadores domésticos. Los usuarios comenzaron a darles nuevos usos que sus creadores ni habían imaginado, y se inventaron palabras mucho más originales y divertidas.

Los variados orígenes de la informática

- ✓ Los anglicismos
- ✓ Acrónimos curiosos
- ✓ Una cuestión de modas
- ✓ Siglos de antigüedad
- ✓ Palabras divertidas

Los anglicismos

Una fuente muy importante de nombres de informática que usamos en español proviene de los anglicismos, es decir, la adopción directa de palabras en inglés. Ocurre en todos los ámbitos, no solo en informática, y se ha acentuado desde que existe Internet.

Ripear

Ripear un CD u otro contenedor de datos,

es extraer su contenido para usarlo en otro lugar. Su uso más común es extraer las canciones de un CD para convertirlas a un formato digital, como el MP3. También se usa con un DVD para extraer la película y convertir al formato MP4, por ejemplo.

En contra de lo que mucha gente cree, no proviene de la palabra RIP (descanse en paz), relativo a extraer todo el contenido de un CD o DVD y así pierde su utilidad (muere, o lo dejamos en paz). Proviene del verbo rip, o ripping, que significa desgarrar, o hacer trizas, en el sentido de que se rompe la resistencia de ese CD o DVD y se desgarran para extraer su contenido, y así convertirlo a otro formato.

Banear

Decimos que alguien o algo ha sido baneado, cuando ha sido expulsado, o se le impide la entrada. Por ejemplo banear a alguien de un foro, o banear un vídeo en YouTube.

Proviene del verbo inglés to ban, que se usa para lo mismo. Es una palabra muy antigua cuyo origen está en la expresión germánica bannen, que significa desterrar o expulsar. En el siglo XIV ya se usaba como sinónimo de prohibir.

Meme

Esta palabra es la misma que se usa en inglés, no se ha adaptado.

Un meme es una idea, concepto o chiste que se expresa de forma visual (con una imagen o vídeo) y está pensado para hacerse viral, es decir, distribuirse rápidamente por foros y redes sociales.

La palabra la inventó el científico y zoólogo Richard Dawkins para su libro El Gen Egoísta, publicado en 1976. En él explica que al igual que los genes transmiten características físicas de unos individuos a



otros, existen genes culturales, que transmiten las mismas ideas y conceptos entre individuos. A la mínima cantidad de información transmisible a través de estos genes culturales la llamó meme.

Este concepto de transmitir cultura pop de forma rápida e inmediata se trasladó a Internet, y así nacieron los memes que todos conocemos.

Acrónimos curiosos

En la introducción del artículo hemos mencionado algunos acrónimos aburridos (la mayoría). Pero también existen otros mucho más originales y populares, provenientes de Internet en general, y las redes sociales en particular. ¡Vamos a verlos!

WTF

Este acrónimo de la expresión inglesa What the Fuck? tiene una traducción literal bastante grosera, pero también se usa en formas más suaves como ¿Qué demonios? o ¿Qué narices? Básicamente se utiliza como una forma vulgar para expresar frustración o sorpresa.

LOL

Otra palabra muy repetida en redes sociales es LOL o LoL, que proviene de la expresión inglesa Laughing Out Loud. Y ésta sí la podemos traducir sin ruborizarnos. Significa reírse a carcajada limpia.

GIYF

Esta palabra tiene una traducción directa, pero exige una explicación.

Proviene de Google is Your Friend, que significa Google es tu amigo. Un frase cada vez más discutible hoy en día, pero que concretamente significa que cuando necesitas información, uses el buscador de

Google....

XOXO

Es una de las expresiones más curiosas que se emplean en redes sociales, porque no es una palabra en sí misma. XOXO se usa en inglés como una firma de despedida para expresar besos y abrazos, pero nadie tiene muy claro de dónde proviene.

Unos dicen que la X representa a una persona abriendo los brazos, y la O, a los labios en círculo para besar. Otros, que la X son dos bocas besándose y la O, dos personas abrazándose. Una tercera corriente de opinión asegura que en realidad representan sonidos, ya que la X suena muy parecido a beso (Kiss) en inglés, y la O a Hugh (abrazo).

La realidad es que estamos, posiblemente, ante el primer emoticono de la historia, pues existen cartas del siglo XVIII en donde XXXXX significa muchos besos, y el mismísimo Winston Churchill lo usaba en las cartas a su madre, en 1894.

Una cuestión de modas

En ocasiones los nombres de la informática se crean mezclando palabras, conceptos, o incluso objetos y dispositivos físicos que están de moda en ese momento.

Podcast

Los podcast se gestaron alrededor del año 2000, cuando el desarrollador Dave Winer añadió una especificación al formato RSS (utilizado para notificar actualizaciones de noticias) con la que se podía incluir un archivo multimedia a esas notificaciones.

En 2004, el presentador de la MTV Adam Curry creó un programa llamado iPodder con el que podías leer las notificaciones RSS, descargar los archivos de audio a iTunes, y reproducirlos en su iPod. La



estructura básica del podcast había nacido.

La palabra podcasting (crear o hacer un podcast) viene de juntar iPod y broadcasting. Fue acuñada en el año 2004 por el periodista inglés Ben Hammersley, cuando escribió un artículo en The Guardian explicando cómo crear tu propia radio online en Internet.

Como vemos, en 2004 el reproductor musical iPod estaba de moda, y su nombre se usaba para reflejar la posibilidad de reproducir contenido de audio en un dispositivo portátil. El iPhone y los smartphones aún no habían nacido.

Trol

Un trol o troll es una persona que molesta a los demás en redes sociales o foros, por diversión o aburrimiento. No hay que confundir con los haters, que son personas que odian a algo o a alguien concreto, y se pasan el día atacándolo.

Hasta hace unos años un trol era una palabra poco conocida en España, pero se volvió popular gracias a las películas de El Señor de los Anillos y los videojuegos y libros de fantasía épica.

Un troll es un monstruo con bastante mal humor que ataca a todo el que se pone por delante. Proviene de las leyendas nórdicas y el folclore escandinavo, y aparece en historias orales y escritas con miles de años de antigüedad.

Spam

Muchos han intentado inventarse un acrónimo para Spam, el correo publicitario que se envía a millones de usuarios de forma no solicitada. Algunos dicen que significa Stupid Pointless Annoying Messages, o Mensajes Estúpidos sin sentido. Otros, Sending and Posting Advertisement in Mass o Enviar Publicidad

en Masa.

Pero la historia más creíble es la que afirma que un grupo de chat famoso en los años 80 se obsesionó con un sketch del grupo cómico Monty Python, en donde repetían continuamente la palabra Spam (carne enlatada). Así que comenzaron a llamar Spam a las frases repetitivas que se usaban en los chats. Más tarde, cuando llegaron los envíos publicitarios masivos a través de Internet, les adjudicaron esta palabra, por su carácter repetitivo y molesto.

Siglos de antigüedad

Existen nombres de la informática que llevan siglos, incluso milenios usándose. La mayoría provienen del latín, que es un idioma cuyas raíces comparten buena parte de las lenguas europeas, incluido el inglés, la cuna de la informática. Aunque también hay palabras que provienen del japonés, el ruso, y otras lenguas no latinas.

Computadora

Uno de los ejemplos más obvios de palabra con un origen milenario, es el computador o computadora. En inglés es computer, que viene del latín, pues deriva de la palabra putare, que significa pensar. Así que un ordenador es una máquina que piensa. Pero en realidad su origen completo es Com-putare, otra palabra latina que significa calcular. Por tanto, un computador es una máquina para hacer cálculos.

La palabra Compute lleva en la lengua inglesa al menos desde el siglo XVII, y también la usaban los romanos hace más de mil años. Computer era una persona que hace muchos cálculos, y ya aparece en un periódico escocés del año 1731, según la BBC.

Se asoció rápidamente a los ordenadores, y ya se usaba en los años 30 del pasado siglo.



Hacker

De forma similar a la computadora, la palabra hacker se remonta siglos atrás en el tiempo. En el siglo XIII se usaba el verbo hack para denotar la acción de corta algo bruscamente, o golpear de forma tosca. También se utilizaba como sinónimo de trucos ingeniosos.

En 1955 el MIT empleaba el verbo hack para describir la acción de acceder a un sistema eléctrico. En los años 70 se utilizaba la palabra hacker para describir a las personas que intentaban penetrar en los sistemas informáticos para realizar acciones maliciosas.

Como vemos su origen era negativo, y así se ha mantenido durante décadas, usado a menudo como sinónimo de ciberdelincuente. Ahora hay un mayor conocimiento del mundo hacker, y existen muchos hackers éticos respetados y admirados.

Palabras divertidas

Tenemos también palabras coloquiales que se hicieron populares porque eran frescas, originales y divertidas. A veces no tienen relación con lo que definen, o se trata de simples bromas y juegos de palabras, pero se impusieron a otras que parecían más apropiadas.

Matamarcianos y comecocos

En los años 80 del pasado siglo poca gente hablaba inglés en España. Así que cuando llegaban las novedades tecnológicas de Estados Unidos o Reino Unido, sus nombres se castellanizaban. Y como la mayoría no sabía lo que significaban, pues esos nombres eran una simple descripción.

Los casos más míticos son, posiblemente los matamarcianos y el comecocos, palabras que hoy ya no se usan, pero que

fueron muy populares en el siglo XX.

Los primeros videojuegos que llegaron a España era las máquinas recreativas que había en los bares, y las más populares eran los juegos de naves en donde había que disparar a invasores extraterrestres, como Space Invaders (1978), Galaxian (1979) o Galaga (1981).

La gente llamaba a estos juegos matamarcianos (una descripción literal), y así se usó durante años para describir a los shoot'em up o juegos de naves y disparos.

Otro juego mítico, Pac-Man (1980), aquí se bautizó con el apodo de el comecocos, porque había gamers que se enganchaban y se obsesionaban con él. Se hizo tan popular que mucha gente (profana) lo usaba para llamar así a cualquier videojuego, e incluso a una consola. Había padres que les decían a sus hijos "deja de jugar al comecocos", cuando en realidad estaba jugando con la consola NES...

Hoy en día la mayoría de la gente sabe inglés, o está acostumbrada su uso, y los nombres de los juegos ya no se traducen.

Magufo

Aunque no es un término informático, nació en Internet. Y al contrario que el resto, es un palabra nacida en España. Más concretamente, en la lista de correo Excépticos, creada por Xoan Carreira.

Magufo es la fusión de dos palabras: mago y UFO (un OVNI, en alusión a los extraterrestres). Un magufo es una persona que defiende las pseudociencias, y todo aquello que no está demostrado científicamente: los astrólogos, ufólogos, echadores de cartas, adivinos, terraplanistas, negacionistas del cambio climático, la homeopatía, etc.

Al contrario que los crédulos, que creen en



las pseudociencias, un magufo no tiene por qué creérselas, pero las defiende o las usa en su beneficio, en ocasiones para sacarles el dinero a los crédulos.

Bug

¿Por qué a los errores informáticos se les llama bugs? Aunque ya lo usó para definir un fallo en un fonógrafo el mismísimo Tomas Alva Edison en el siglo XIX, cuenta la leyenda que se empezó a usar en informática gracias a una programadora llamada Grace Hopper.

Mientras trabajaba en un ordenador Mark II en 1957, tuvo que apagarlo porque una polilla se había introducido en su interior. Comentó a sus compañeros que está debuggeando el sistema (en inglés bug significa bicho o insecto) y desde entonces se usa tanto el término bug para describir un fallo informático, como debug para arreglarlo.

Hemos repasado el origen de nombres de la informática que nunca hubieras imaginado. ¡Seguro que más de un significado te ha sorprendido!

Disponible en:

<https://computerhoy.com/listas/tecnologia/origen-nombres-informatica-nunca-hubieras-imaginado-449567>

2. ESTE FÍSICO TE DICE DÓNDE PONER EL ROUTER PARA MEJORAR TU WIFI

Fecha: 17/07/2019

En torno al router es preciso tomar una serie de decisiones y medidas: conocer si tus vecinos re roban el WiFi, extremar las claves de seguridad, no dejar la contraseña por defecto sino incluir una robusta y fuerte, cambiar el nombre de usuario o colocar las antenas adecuadamente. Además de los pertinentes ajustes de fábrica, es

fundamental colocar el enrutador en un lugar característico.



Para ello, ya no es preciso recurrir al método de ensayo y error y conocer qué lugar puede proporcionarte una mejor señal WiFi, sino que las matemáticas tienen mucho que decir al respecto. El físico Jason Cole ha descubierto una fórmula que puede determinar el mejor lugar para colocar tu enrutador inalámbrico y, en última instancia, depende del plano de la casa.

Cole comenzó a investigar la ciencia detrás de la colocación del router en un intento por optimizar su propia señal WiFi. Para lograrlo, optó por mapear el plano de la planta de su hogar, asignando valores de refracción a las paredes. El científico se sirvió de la ecuación de Helmholtz para modelar las ondas electromagnéticas que emite el aparato.

Inicialmente, se le ocurrió la sorprendente solución de que poner el enrutador justo en el medio de su hogar da como resultado la mejor señal WiFi posible. Sin embargo, a nivel estético es complicado e incluso muchas veces no resulta posible dados los puntos de alimentación o la ubicación de las diferentes partes de la casa.

Para investigar más a fondo, Cole modificó su modelo para tener en cuenta la absorción en los materiales de las paredes, como el hormigón, así como para detener los reflejos perfectos que forman una onda estacionaria.



La investigación de Jason Cole revela que es posible colocar el router en un lugar desde el que sea posible que la señal WiFi llegue a todas las habitaciones, como se refleja en el vídeo a continuación.

Cole incluso ha creado una aplicación de Android que te permitirá asignar su propia

señal WiFi en tu hogar.

Disponible en:

<https://computerhoy.com/noticias/tecnologia/fisi-co-te-dice-donde-poner-router-mejorar-wifi-457407>

USO SOCIAL DE LAS TIC

1. EL CEREBRO HUMANO YA ESTÁ EN LA NUBE

Fecha: 13/07/2019

Comprender el cerebro humano es uno de los mayores desafíos a los que se enfrenta la ciencia en el siglo XXI. Y así lo ha entendido la Unión Europea, que ha definido como Proyectos Emblemáticos (FET, por sus siglas en inglés) las iniciativas “The Human Brain Project” (HBP) y “Graphene”.



La iniciativa Grapheneexplora, se basa, entre otros usos del grafeno, en su potencial como interfaz cerebral, mientras el Proyecto Cerebro Humano (HBP) aspira a comprender cómo funciona el cerebro humano y lograr, algún día, emular sus capacidades.

El HBP, que se lanzó en 2013, reúne a 120 organizaciones europeas y cuenta con la participación de investigadores que son líderes en este ámbito en el mundo. Se trata de un consorcio multidisciplinar que incluye expertos en neurociencias, informática,

robótica, microelectrónica, así como en innovación, ética, educación, gestión de programas y comunicación.

Entre ellos se encuentra Mavi Sánchez Vives, doctora en neurociencias, que ha coordinado el proyecto SloW-Dyn sobre dinámica de la corteza cerebral.

Su trabajo tiene el propósito de reunir información sobre la composición del sueño, las oscilaciones neuronales y la sincronización de la actividad cerebral, así como las anomalías que pueden surgir como consecuencia del envejecimiento o de enfermedades concretas como el Alzheimer.

¿Se atreve a describir el mundo en que vivimos?

Desde el punto de vista de la neurociencia, vivimos en un mundo en el que se ha desarrollado un enorme interés por el conocimiento del cerebro.

Esto se ha traducido, por ejemplo, en la aparición en la última década de grandes iniciativas gubernamentales y también privadas -como el Allen Institute-. Europa es líder con el Human Brain Project, del que forma parte, pero también hay proyectos similares en Estados Unidos –Brain Initiative-; en China, en Japón, en Corea o en Australia...



He visto crecer ese interés en la sociedad y todo lo que empieza hoy por “neuro” interesa.

¿Por qué interesa tanto?

Interesa porque nuestro cerebro es lo que nos define. El cerebro es el ser humano. Además, es bien conocido por todos que muchas patologías neurológicas, como la enfermedad de Alzheimer, pueden ser devastadoras.

En las últimas dos décadas se ha extendido la idea del cerebro como un órgano con plasticidad, con capacidad de transformación y mejora, lo que abre la puerta a que podamos cuidarlo.

A medida que aumenta la esperanza de vida, aumenta el interés por cuidar del propio cerebro con la alimentación, con el ejercicio, con estimulación cognitiva, con el aprendizaje...

Hay un interés en la mejora del cerebro, en la mejora de las funciones cognitivas. Sí, el cerebro está de moda.

Además está el aspecto tecnológico, la voluntad de desentrañar cómo funciona el cerebro y llegar a establecer relaciones directas con las máquinas.

La interacción del cerebro con la tecnología deriva del hecho de que el cerebro funciona mediante actividad eléctrica y por tanto puede establecerse una interacción con la máquina.

Conocemos cada día más el funcionamiento del cerebro humano y veremos llegar una creciente interacción con la tecnología. Esta interacción es bidireccional: cada vez hay más recursos computacionales para leer la actividad cerebral y, a la vez, podemos interaccionar con esta actividad cerebral mediante

campos eléctricos, magnéticos, luz, etcétera.

En esa interacción hay también un nuevo interés orientado a la posibilidad de estimular la capacidad cerebral y también a usar principios del funcionamiento cerebral para el aprendizaje de las máquinas.

Eso explica que hayan entrado grandes corporaciones en el estudio del cerebro, como Elon Musk con NeuraLink, o Google, Facebook y otras. Además del interés científico y médico, hay interés a todos los niveles: en la ciudadanía, en las empresas y en los gobiernos.

¿Cuál es el objetivo final del estudio del cerebro?

Siempre se empieza por las patologías. Se trata de prevenir o tratar las enfermedades degenerativas y las patologías que afectan al cerebro, que causan graves daños a las personas que las sufren y a su entorno.

El coste es altísimo social y económicamente. Sabemos, por ejemplo, que este tipo de enfermedades degenerativas del cerebro tienen un coste de 5.000 euros (unos US\$5.600) al año para cada europeo.

El objetivo prioritario es evitar las enfermedades, problemas muy concretos. Pero para ello es fundamental comprender el funcionamiento, los procesos fisiológicos subyacentes.

Comprender la fisiología es fundamental para entender la patología. Es posible también que los resultados de las investigaciones sobre el cerebro terminen por aplicarse a mejoras en el funcionamiento cerebral de personas sanas.



¿Llegará a estar el cerebro humano en la nube, en un servidor externo?

No creo que lleguemos a verlo, pero se podría. Hay ya muchas cosas que se pueden hacer. Si lo que quieres decir es que tu actividad cerebral puede estar en la nube, ya te confirmo que eso es posible hoy día.

Pero con esto nos referimos a registros de electroencefalograma, imagen cerebral, etcétera. Lo que están haciendo muchos de estos grandes proyectos de estudio del cerebro son enormes bases de datos de imagen cerebral, de actividad eléctrica, de mapas de todas las células cerebrales...

En ese sentido, sí podemos decir que nuestro cerebro humano ya está en la nube en estos momentos. Ahora bien, que tus ideas, tus pensamientos, tu consciencia, tu razonamiento, tu creatividad o tus sentimientos..., en definitiva, que tu "yo" íntegro se llegue a volcar en un ordenador, eso está aún por ver.

¿Debemos temer al progreso tecnológico y científico acelerado?

No hay que tener miedo pero hay que estar alerta. Todos estos avances tecnológicos están entrando en nuestra vida de una forma progresiva, casi sin darnos cuenta.

Creo que los avances en ciencia y en tecnología buscan el bien y nos proveen de herramientas para que nuestra vida sea mejor. Los avances en ciencia, en genética, en robótica, en realidad virtual, en energía, en materiales... son positivos. Hacen que nuestra vida sea más larga y mejor.

El problema es que la humanidad es capaz de hacer cosas maravillosas, pero también es capaz de desviarse y proponerse usos perversos.

Eso es posible con la realidad virtual o la interfaz cerebro-ordenador, pero también con un cuchillo de cocina. Tenemos que estar alerta, considerar las consecuencias y el doble uso que se puede hacer con cada innovación, pero sin que los temores nos detengan.

No hay que olvidar tampoco que siempre hay consecuencias no previstas. Como ha advertido Jaron Lanier, internet y las redes sociales se crearon de una forma -gratuita y abierta- que ha acabado volviéndose en nuestra contra por el uso que se hace de los datos de los usuarios.

Debemos estar muy alerta para evitar desviaciones que terminen perjudicando a la humanidad.

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.tynmagazine.com/el-cerebro-humano-ya-esta-en-la-nube/>

2. BLINDATUTARJETA.COM, NUEVO SERVICIO BIOMÉTRICO DE PAGO SEGURO PARA TARJETAS Y MÓVILES

Fecha: 05/07/2019

Blindatutarjeta-com es una nueva plataforma tecnológica que permitirá pagar en tiendas físicas y de comercio electrónico de forma rápida y segura en apenas dos pasos con todo tipo de tarjetas y de móviles con reconocimiento biométrico.

La biometría en sus diversas vertientes - huella dactilar, reconocimiento del iris, escáner facial, etc- cada vez experimenta mayor acogida y penetración en el mercado con respecto a las formas convencionales de autenticación digital. Ahora, la alianza de la compañía europea de tecnología Biocryptology con la fintech KíneoX (otrora IMSolutions), ha dado como resultado una solución para poder identificarse, realizar compras y pagar de forma segura ahorrando tiempo y evitando fraudes.



Para ello, los usuarios solamente deberán tener la app de Biocryptology y registrar su

tarjeta bancaria en blindatutarjeta.com. De esta manera, su tarjeta -tanto de débito como de crédito- quedará blindada completamente y sus datos encriptados. Podrán pagar con cualquier smartphone con tecnología de huella dactilar o tarjeta - el resto están limitadas por los acuerdos que las marcas de teléfonos alcancen con cada banco-.

Cabe destacar que Blindatutarjeta.com cuenta con la certificación más alta en seguridad para pagos con tarjeta, PCI DSS Nivel 1. Es un estándar de seguridad de las principales compañías emisoras de tarjetas de pago para ayudar a comercios, proveedores de servicios y bancos a reducir el riesgo de fraude con tarjetas de crédito protegiendo las infraestructuras que procesan, transmiten o almacenan datos de tarjetas de crédito.

En un comercio físico la persona se identifica desde la aplicación, donde previamente ha cargado sus datos, y confirma la compra con la huella biométrica, mientras que una tienda online podrá identificarse con un código QR generado al entrar en la tienda para confirmar con la huella la compra.

Con una facturación de 28.423 millones de euros en los nueve primeros meses del año pasado (+29,9%), según los últimos datos de la Comisión Nacional de los Mercados y la Competencia (CNMC), el comercio electrónico atraviesa una época dorada en España. El único dato negativo es el del 30% de internautas que abandonan el carrito de compra por problemas de login y formularios, según datos de Google Pay.

Soluciones como esta lograrán que “las ventas de las tiendas crecerán de forma exponencial y la experiencia de los usuarios será mucho más grata”, tal y como estima Raúl Legaz, director de Biocryptology. La solución que brindan con KíneoX es gratos



para los particulares y la previsión es alcanzar la cifra de 50.000 usuarios en tres meses.

Por otro lado con esta plataforma se podrán cumplir los requisitos de doble autenticación que establece la nueva Directiva europea de Medios de Pago (conocida como PSD2) que entra en vigor el 14 de septiembre y convierte el teléfono móvil en el medio de pago más rápido, efectivo y seguro. Esta normativa sustituye a la de 2007 e implementará lo que se conoce como SCA (Strong Customer Authentication) para garantizar que realmente es el usuario quien está dando permiso para acceder a dichos datos.

Además de eliminar el riesgo de fraude se evita el tedio del proceso para los usuarios, la exposición de datos sensibles como información bancaria o dirección y reconfirmar la operación al realizar compras físicas y digitales.

Disponible en:

<https://www.ticbeat.com/seguridad/blindatutarjeta-pago-seguro-moviles-tarjetas/>



REPÚBLICA DE CUBA
MINISTERIO DE COMUNICACIONES



Sistema de Vigilancia Tecnológica