El futuro de la tecnología

En los últimos años hemos ido asimilando la tecnología informática en nuestras vidas hasta hacerla más natural que nunca. De la vieja promesa de llevar un PC a cada casa a la realidad de llevar un ordenador en nuestros bolsillos. Estamos en 2017 y el desarrollo tecnológico no se ha parado, continúa y más fuerte que nunca. La ciencia ficción ya había predicho un montón de innovaciones que nunca terminaban de llegar y que ya casi las teníamos descartadas, como el coche autónomo, pero a día de hoy ya no parece una locura como hace unos pocos años.

Llevamos años viviendo lo que es una autentica revolución industrial, posiblemente la última revolución industrial, que llevará varios años y consistirá en la automatización casi completa de la fase de producción de todo lo que usamos. Sin embargo no se limita únicamente al sector industrial todo lo que puede ofrecernos. Tiene grandes efectos en toda la economía y en el comportamiento social de las personas. La tecnología ha cambiado la forma en la que interactuamos como individuos en la sociedad y está planteando dilemas muchas veces interesados pero otras auténticos problemas que podrían devenir.

Un ejemplo es la privacidad, parece que hemos asumido ya la perdida de la privacidad ya sea por no pagar el software que usamos o porque no estamos dispuestos a asumir una supuesta inseguridad ciudadana. Si esto continua por aquí los peligros son grandes y eclipsarán a los beneficios que nos proporcionan tarde o temprano. La informática tiende hacia la estandarización y muchas veces acabamos viendo monopolios en ciertos sectores. Uno de los aspectos que creo que son preocupantes es que empresas como Google monopolicen el acceso a la información, haciéndose tan buenas en su trabajo que jamás vuelvan a tener un competidor digno en estos campos. El peligro de que Google se convierta en el gran hermano de Orwell creo que es muy grande, puesto que controla el acceso a la información y siempre está a la última en desarrollos de Big Data e Inteligencia Artificial.

Necesitaremos legislar para evitar que sucedan todas estas cosas, pero más importante aun creo que es estar concienciados de su importancia y exigir que se apliquen dichas normas. Los peligros de un mal uso de la tecnología no solo vienen de su uso armamentístico como en el pasado, sino asimilamos correctamente la tecnología en nuestras vidas puede por intereses privados causar graves daños en nuestra sociedad. Todo cambio tecnológico debe de ir acompañado de un cambio social y tecnología y sociedad deben de avanzar juntas buscando hacer nuestras vidas más sencillas y simplificar nuestro trabajo. ¿Que nos depara la tecnología en el futuro? Nadie lo sabe a ciencia cierta pero creo que todos estamos de acuerdo en que tiene que ser para hacer un mundo mejor y no para dañar más el que ya tenemos.

La distancia entre nosotros es lo que nos está destrozando

Somos más que nunca antes en la historia de la humanidad, tenemos más lujos que nunca y a pesar de ello estamos más distanciados entre nosotros que en cualquier otro momento de la historia.

El distanciamiento entre las personas es tan brutal que se puede percibir en la cantidad de gente que padece de problemas emocionales. Cada vez hacen falta más psicólogos y cada vez se toman más fármacos y drogas para solucionar los síntomas de nuestra infelicidad. Esto no soluciona nada, se ataca el síntoma y la realidad es que esa persona sigue jodida porque lo que lo causaba sigue presente.

Se proporcionan para que esta persona pueda seguir trabajando y rindiendo hasta que reviente. Una vez ha reventado, muy simple contratamos a otra persona para su mismo puesto. Por este motivo la mayor parte de la gente va infeliz al trabajo, solo es una forma de ganar dinero y salir corriendo de allí lo más rápido posible. Es evidente que el trabajador feliz es más eficiente a largo plazo, en una sociedad donde se busca ante todo la eficiencia algunos se dan cuenta y lo ponen en práctica. Menos mal que es así, pero no es motivo suficiente para tratar con decencia y humanidad a los empleados. Se que es difícil de entender en una sociedad tan podrida pero los dividendos a fin de mes no lo son todo. A veces el crecer por crecer no lo es todo aumentando ganancias e ingresos hasta el infinito, ¿De que sirve mi actividad empresarial si solo crea miseria en mis empleados y en mi sociedad con tal de crecer?

A la infelicidad en el trabajo hay que sumarle los graves problemas emocionales que suele padecer la gente por un simple motivo, distancia con la familia y los amigos. Muchos construyen sus corazas y se distancian de la gente cercana, el hablar de los sentimientos y emociones es tabú en nuestra sociedad que se centra en lo banal y lo irrelevante.

La realidad es muy sencilla, el dinero es fácil de medir y la empresa no tiene emociones. Al ser una agrupación, se consigue distanciar a nivel individual de los actos que causa y de su responsabilidad individual, creando una responsabilidad colectiva. La empresa no tiene emociones y sus accionistas y empleados aunque la tienen la ven diluida por la distancia entre el cargo y las consecuencias. Una empresa es un ente social, si existe es para generar un beneficio, como ente social se compone de personas y las personas deben de tener un trato cercano y afectivo para que la empresa funcione y merezca la pena que siga existiendo. Ese y no otro es el motivo por el que es necesario replantear las relaciones sociales en una empresa, no por el dinero sino para acercar a la gente y que se enriquezcan personalmente entre si y al mismo tiempo generen valor para la sociedad que se retorne en forma de beneficios económicos y autosatisfacción en los empleados.

Yo no elegí mi carrera porque pensase en el dinero, si quisiese eso hubiese

elegido otra carrera muy probablemente. Que suerte que somos muy jóvenes e inocentes cuando tenemos que elegir una carrera si fuésemos más mayores a lo mejor tomaríamos muchos otra decisión porque la sociedad nos ha enfermado mentalmente hasta el punto de no entender lo que importa en la vida.

Cada uno tomamos nuestras decisiones de que hacemos con nuestra vida, yo personalmente he aprendido a saber que valorar y a darme cuenta cuando no estoy feliz con algo y tratar de poner remedio. Miro a la sociedad y no me gusta lo que veo pero eso no es motivo para no levantarme cada día y pelear por poder ver el lado oculto de las cosas, eso que no es tan visible pero que compone la esencia de la vida.

IoT y su implementación en la empresa

El futuro del IoT no se limita solo a las Smart Homes y Smart Cities, también puede tener su futuro en la empresa. Pero una empresa puede tener unas necesidades diferentes a las de una ciudad donde es un entorno público o una casa donde su entorno es privado. La empresa puede tener una serie de características especiales, datos que no solo son privados sino que son especialmente delicados, muchas veces no solo vulnerando nuestra privacidad, sino también la del cliente, pudiendo asumir responsabilidades legales en caso de que se produzca alguna filtración. Es por este motivo que se considera una de las 5 prioridades en la encuesta de capacidades y necesidades de auditoría interna de 2014 de Protiviti. De cara a unos años podría suponer en algunos ámbitos una diferencia competitiva con respecto a sus competidores. Para tener unos controles de los riesgos que supone esta nueva tecnología deberíamos responder a las siguientes preguntas.

Para empezar como se implanta el IoT en la organización y quien posee los componentes respectivos del IoT. Es decir en donde vamos a implementarlo y con que objetivos y quien será el responsable de ello. También sería necesario hacer un análisis de riesgos asociados a la implementación de cada componente del IoT. Por ejemplo no es lo mismo una cámara de seguridad que un termostato inteligente. Es decir es necesario cuantificar y controlar esos riesgos. Con ello analizamos que datos se recogen, almacenan y analizan y sus implicaciones legales. También es necesario tener en cuenta una política de contingencia en caso de una vulneración de la seguridad de dichos dispositivos, tanto activa como pasiva. Así mismo analizar el riesgo de no implementar el IoT y si se puede maximizar el efecto con un análisis de los datos. Estos son los aspectos a tener en cuenta para la realización de una correcta auditoría de seguridad del IoT, ¿Pero cuales son sus principales riesgos y como nos podemos enfrentar a ellos?

Para empezar pueden ser vulnerables a un ataque de denegación de servicio, garantizar su disponibilidad continua es un aspecto importante para evitar

fallos en la actividad y servicios de la empresa. Esto se podría solventar en aquellos sistemas que sean más críticos garantizando una política de acceso de dispositivos autorizados o de dentro del perímetro de seguridad.

Otro aspecto es comprender la complejidad de las vulnerabilidades, por ejemplo un termostato de un sistema crítico en una industria que puede tener graves consecuencias si proporciona datos erróneos o falsos. Es necesario entender que ese termostato en un sistema crítico y en una auditoría de seguridad debería de estar presente. También es necesario gestionarlas correctamente, tanto en la instalación de los sistemas como en su actualización para garantizar que realmente estamos configurando realmente bien la red y actuando a tiempo en caso de tener un problema, identificándolo y solventándolo. Algunas formas de solucionar las intrusiones podrían ser el uso de VLANs para garantizar la separación de componentes dentro de una red y aislarlos. El crear un sistema de IoT en la empresa supone la generación de nueva información y conocimiento que puede tener nuevas necesidades de seguridad y con ello nuevos riesgos. Detectar los riesgos a tiempo y una actividad malintencionada puede suponer una diferencia fundamental.

Por último con la generación de nuevas cantidades de información y en ello el IoT interviene, se genera un crecimiento de la demanda de ancho de banda. Esto si no se gestiona correctamente puede empeorar gravemente el servicio que ofrece la compañía o perjudicar el conjunto de sus actividades. Una correcta gestión del tráfico de red de la empresa es necesaria para garantizar que cada sector recibe el ancho de banda necesario para cumplir correctamente con sus actividades y con ello también anticiparse a al crecimiento de dicha demanda.

En resumen, las posibilidades que puede ofrecer a una empresa el Internet of Things son enormes y puede suponer la diferencia entre una empresa prospera y una en decadencia. Sin embargo también abre la puerta a nuevas prácticas para gestionar los nuevos riesgos que emergen, así empresas que no estaban acostumbradas a trabajar con unos niveles de seguridad tan altos deberán de aprender y realizar nuevos tipos de auditorias para atacar el problema y con ello seguir ofreciendo un servicio o producto a sus clientes de máxima calidad sin estar en un riesgo constante por no haberlos previsto y gestionado.

IOT Seven Enterprise Risk to Consider, IoT Agenda, http://internetofthingsagenda.techtarget.com/tip/Internet-of-Things-IOT-Seven-enterprise-risks-to-consider

KnowledgeLeader, INTERNAL AUDIT AND THE INTERNET OF THINGS, https://www.knowledgeleader.com/KnowledgeLeader/Resources.nsf/Description/HIInternalAuditandtheInternetofThings/$FILE/HI%20Internal%20Audit%20and%20the%20Internet%20of%20Things.pdf

Riesgos en el Smart Car

El IoT es la gran promesa de la tecnología para los próximos años, un ejemplo claro que empezamos ya a ver son los conocidos como Smart Cars. Coches inteligentes que serán capaces tanto de llevarnos de un sitio a otro solos como de asistirnos con información durante la conducción para cumplir mejor con dicha tarea. Se estima que para 2020 habrá 250 millones de automóviles conectados a IoT por las calles. Esto permitirá reducir el número de accidentes y reducir la congestión del trafico entre otras muchas cosas. Con la incorporación del coche autónomo se espera acabar con el principal causante de los accidentes, que en el 90% de los casos es el factor humano.

Sin embargo esta incipiente tecnología tiene sus consecuencias inmediatas. Los fabricantes de coches tienen que adentrarse en terreno desconocido en muchos casos. Los expertos en seguridad comparan los coches inteligentes con la protección que tenían los ordenadores de escritorio de los 80 y 90. Un ejemplo es una vulnerabilidad encontrada en el protocolo MirrorLink que permitiría afectar a sistemas críticos del vehículo. La vulnerabilidad de los automóviles a la piratería se considera problemática por la Agencia de Proyectos de Investigación Avanzada de Defensa o DARPA. Considera que actualmente no supone un gran riesgo puesto que este tipo de ataques está solo al alcance de unos pocos, pero conforme vaya generalizandose el IoT, el riesgo irá creciendo y que los sistemas deberán de tener un nivel de protección a la altura del riesgo. Algunos investigadores afirman que aunque se han tomado medidas para mejorar la seguridad de redes a bordo de los vehículos, sigue sin ser suficiente para la amenaza que supone.

No solo hay problemas en el desarrollo de la seguridad de los Smart Cars, también hay riesgos inherentes a la incorporación nuevas tecnologías a la labor de conducción. Por ejemplo un gran problema que se puede considerar es una mala implementación de tecnologías que puede suponer un elemento de distracción para el conductor. La NHTSA ha publicado una serie de pautas para alentar a los fabricantes de automóviles a limitar la distracción de los dispositivos electrónicos dentro del vehículo. Entre algunas de las recomendaciones proponen bloquear el uso visual-manual de mensajería por texto, búsqueda por internet, redes sociales o la introducción manual del número de teléfono. Los objetivos son reducir la complejidad y duración de la tarea a realizar con un dispositivo, reduciendo así las miradas fuera de la carretera y la información innecesaria para la labor de conducción.

Todos estos sistemas que incorporan los Smart Cars están pensados para participar activamente o pasivamente en la conducción. Pero ninguno más que la tecnología de la conducción autónoma. Aquí se plantea un dilema. Si se produce un accidente con un vehículo autónomo la responsabilidad pasa a ser del conductor, que debería de ser considera un pasajero del vehículo o una parte activa en la conducción, o del fabricante, siendo un accidente industrial por ejemplo. El principal problema puede estar en la falta de un criterio y una regulación que asigne responsabilidades.

Otro de los riesgos a tener en cuenta es la información generada por un Smart Car. Existen muchos sistemas de información que tienen un nivel de privacidad alto, como pueden ser las transacciones bancarias pero actualmente no se puede considerar que los generados por los automóviles tengan el nivel de privacidad en el tratamiento de la información que deberían de tener. Esta información puede ser útil para alertar automáticamente de accidentes, localizar vehículos robados o detección de infracciones. La pregunta es donde está la linea entre respetar la privacidad y detectar las infracciones y delitos fácilmente mediante esta información. Según la Vehicle Infrastructure Integration Coalition existe un esfuerzo cooperativo entre departamentos para buscar el anonimato del conductor. El riesgo además no siempre está en los sistemas que trae el coche una vez comprado sino que podría estar en accesorios comprados e instalados en el mismo por el conductor como pueden ser GPS, transpondedores de pago en peajes… Un ejemplo de esto podría ser las compañías de seguros que instalen sistemas para identificar y premiar a conductores seguros con evidentes problemas de privacidad o también las conocidas como cajas negras que se instalan a día de hoy en la mayoría de los vehículos y se están empezando a usarse en juicios como pruebas del accidente, aunque técnicamente el propietario del vehículo debería de ser también propietario de esa información. Como se puede considerar que sea una prueba una caja negra sino está demostrado que esta funcione correctamente por ejemplo ciñéndose a algún estándar y a una auditoría de sus sistemas de registro de información.

En esta transición hacia los Smart Cars y la conducción autónoma los fabricantes de vehículos van a tener que adentrarse en una serie de tecnologías y buenas prácticas a las que no están habituados. Supondrá un periodo de adaptación que llevará varios años y que muy posiblemente no todos sean capaces de alcanzar los mínimos que deberemos de exigir en cuanto a seguridad y privacidad para nuestros coches del futuro.

IoT And Smart Cars: Changing The World For The Better, Iona Sima, http://www.digitalistmag.com/iot/2016/08/30/iot-smart-connected-cars-will-change-world-04422640

SMART CARS AND SECURITY – THE GAME OF RISKS, MARTIN BELTOV, http://bestsecuritysearch.com/smart-cars-security-game-risks/

Smart cars and connected vehicles Privacy, security and safety considerations – Zurich

U.S. Departament of Transportation Proposes ‘Distraction’ Guidelines for Automakers, http://www.nhtsa.gov/About-NHTSA/Press-Releases/2012/U.S.-Department-of-Transportation-Proposes-‘Distraction’-Guidelines-for-Automakers

Xataka, ¿Quien tiene la culpa si un coche autónomo tiene un accidente? En Volvo lo tienen claro: es de ellos, http://www.xataka.com/automovil/quien-tiene-la-culpa-si-un-coche-autonomo-tiene-un-accidente-en-volvo-lo-tienen-claro-es-de-ellos

USAToday, Your car may be invading your privacy, Chrish Woodyard and Jayne O’Donnell, http://www.usatoday.com/story/money/cars/2013/03/24/car-spying-edr-data-privacy/1991751/

La llegada inminente del coche autónomo

En los últimos años estamos viendo el surgimiento de los coches autónomos. Algunos son prototipos que aun no están disponibles para comprar, como el coche de Google con un nivel de autonomía alto y otros modelos como el Tesla Model S tienen un importante nivel de autonomía, aunque no completa y están ya andando por nuestras calles.

Sin embargo, esta nueva tecnología supone un cambio importante en las leyes de circulación vial. En España por ejemplo tenemos que la DGT está autorizando pruebas de conducción autónoma en algunas ciudades.

Actualmente se discute la necesidad de que los sistemas autónomos sean más tolerantes a fallos en función de las limitaciones humanas y a los diversos factores ambientales. Se trata de una tecnología emergente y es necesario tener un correcto equilibrio entre la visión optimista y la pesimista. Un ejemplo sería si el coche es funcional en condiciones de baja visibilidad como niebla o de si es capaz de enfrentarse a problemas complejos como un guardia de tráfico guiando a los coches. Es previsible que esta tecnología irá avanzando y poco a poco podrá enfrentarse a más situaciones por si solo, por lo que por el momento es posible que solo se autorice legalmente la circulación de los vehículos autónomos como una asistencia a la conducción y no concebido como completamente autónomo.

Esta tecnología tiene un gran potencial, en aspectos como la mejora del tráfico, reducción de accidentes y muertes y la accesibilidad de viajes en coche para todos… La automatización completa llegará algún día pero será una transición paulatina y compleja. Por el momento veremos vehículos que requieran de un conductor que supervise y a veces intervenga. La NHTSA formalizó los grados de automatización de los vehículos en 4 niveles,

- Nivel 0: Conducción manual
- Nivel 1: Automatización de funciones especificas, por ejemplo los frenos antibloqueo o la asistencia de frenado.
- Nivel 2: Automatización de funciones combinadas, sirve para sistemas que permiten mantener en el carril un tiempo limitado a vehículos.
- Nivel 3: Sistema de autoconducción limitado, que permite a los coches controlar todos los aspectos de la conducción durante tiempo prolongados y el sistema pide la intervención de la persona cuando no puede actuar.
- Nivel 4: Automatización completa.

La normativa de circulación internacional tiene su base en la convención de Viena de 1968 y en ella se especifica que todo vehículo a motor deberá de tener un conductor. Sin embargo España no tiene ratificado el acuerdo. El objetivo debería de ser regular este sector y no limitarlo, pero sin llegar a reducir la seguridad. Ya se aprobó unas enmiendas para la convención de los

Viena en 2016 para regular los vehículos autónomos siempre que los dispositivos cumplan los reglamentos sobre vehículos de la ONU o que puedan ser invalidados o desconectados por el conductor.

Para terminar también mencionar que los coches autónomos y los llamados Smart Cars tendrán un futuro en nuestras ciudades del futuro, gracias a la generalización del Internet of Things. Por ejemplo en el carsharing los coches podrían ir a recoger a las personas que lo necesiten y repostar ellos solos. Sobre todo teniendo en cuenta que se está promoviendo un modelo de vehículo eléctrico para este tipo de negocio. Además para 2025 se espera que Navigant Research tenga un total de 1.2 millones de vehículos a nivel mundial intercambiando información de seguridad y tráfico en tiempo real que servirá para mejorar los sistemas de conducción autónoma.

Una de las claves para la ciudad del siglo XXI es que el vehículo sea autónomo, eléctrico y bajo demanda, esto supondría un cambio drástico en el modelo de movilidad urbana. El futuro se aproxima y es necesario adaptarnos a el para estar a la cabeza de la innovación y la implementación de estas tecnologías que tanto nos tienen que ofrecer.

ACM,
http://cacm.acm.org/magazines/2016/5/201592-the-challenges-of-partially-automated-driving/fulltext

Expansion,
http://www.expansion.com/juridico/actualidad-tendencias/2016/10/11/57fd2cec46163f3c558b4696.html

Forbes,
http://www.forbes.com/sites/pikeresearch/2016/06/13/the-future-is-now-smart-cars/#212da4e048c9

La seguridad en el Internet Of Things

El IoT es el siguiente paso en la tecnología, asimilar esta en la sociedad proporcionando servicios puntuales allí donde se necesitan. Esto requeriría de una masificación de los dispositivos conectados a internet, directamente conectado al wifi, con zigbee, usando bluetooth, beacons o de otras muchas formas.

Pero tenemos un problema al respecto de esta masificación. Si ya hay graves fallos de seguridad a día de hoy en empresas cuya responsabilidad es cuidar de esos datos y que no se divulguen, hasta que punto puede llegar si creamos un montón de dispositivos, sin garantía de calidad y los conectamos a lo largo de toda nuestra ciudad. El ejemplo más reciente del riesgo que supone lo tenemos con Yahoo y la filtración masiva de las cuentas de sus usuarios. Ahora supongamos que una persona, empresa o institución pública decide

ahorrar dinero a la hora de comprar estos aparatos para su entorno comprando productos de un precio muy bajo y sin garantía de seguridad. La amenaza puede ser importante, cualquier dispositivo que no tenga una correcta implementación puede ser susceptible de ser atacado ya no solo por hackers malintencionados profesionales, sino por cualquiera que estando un poco metido dentro del mundillo siga los defectos de los diversos productos.

La pregunta que surge es como podemos garantizar la seguridad. Bueno pues la responsabilidad no va a ser solo del que hace el producto, también es nuestra responsabilidad a la hora de comprar un dispositivo que vamos a conectar a la red asegurarnos que tiene unas correctas garantías de seguridad y pensar en si confiamos de verdad en el. ¿Confiamos en esa cámara de seguridad conectada a internet comprada en Alliexpress? Yo personalmente no.

Como desarrolladores de estos dispositivos tenemos una responsabilidad con nuestros clientes. Tenemos que garantizar que sus dispositivos no sean vulnerables. Una forma de garantizar las comunicaciones seguras es implementar un cifrado en dichas comunicaciones. Entre los algoritmos de cifrado tenemos el PRESENT, que es un algoritmo ligero de cifrado, se considera que no hace falta en el IoT el cifrado de grandes masas de datos. Otro ejemplo es TRIVIUM, también un algoritmo de cifrado ligero. En este caso se basa en un registro de desplazamiento cíclico para su funcionamiento, tiene el propósito de ser eficiente y de dar un buen resultado de seguridad.

La seguridad de nuestro sistema también se puede ver vulnerada por el hardware que adquirimos, en un artículo interesante de IEEE se analiza un caso en el que se reemplazo una pieza por otra no autorizada para detección de hielo en un avión P-8 Poseidon. Analizando el problema se descubrió que esta pieza provenía de China. Este caso es especialmente interesante porque se centra en la seguridad en el ámbito militar donde la incorporación de una pieza no autorizada puede provocar fallos de seguridad y brechas que pueden ser aprovechadas por el enemigo.

Pero este es un ejemplo orientado a la industria militar con una serie de requisitos que no todos tenemos, aunque no es la primera vez que en nuestro día a día podemos tener brechas de seguridad que desconozcamos por culpa de haber adquirido un producto cuyas medidas de seguridad no eran lo suficientemente estrictas. Un ejemplo es el caso de los primeros lectores de huellas para móviles samsung que tenían una brecha de seguridad que permitían a otras aplicaciones acceder a ellas.

Homekit

Por último vamos a volver al foco del IoT y la seguridad, pero en el ámbito domestico. Personalmente, una de las apuestas que me resulta más interesante en el IoT es Apple Homekit, sin embargo, este parece estar retrasándose a la hora de surgir productos compatibles con el estándar por un motivo. Según se dice tiene unos requisitos de seguridad tan fuertes que está dificultando el desarrollo de fabricantes no acostumbrados a estos niveles de seguridad.

Homekit hace uso de unas claves de cifrado de 3072 bits, curve25519, firmas digitales e intercambio de claves cifradas. Tanto para su conexión por WiFi como por Bluetooth LE. Según parece el problema surge en algunos dispositivos Bluetooth LE que genera un retardo demasiado grande, esto se ha conseguido solucionar incorporando más RAM, pero encareciendo el producto. Sin embargo en un mundo tan inseguro, la existencia de un protocolo que nos de estas garantías y sustentado por un gigante como apple es evidentemente una buena noticia.

IEEE, Pass-IoT: A Platform for Studying Security, Privacy and Trust in IoT, 25/10/2016

IEEE, Defense Systems and IoT: Security Issues in an Era of Distributed Command and Control, 25/10/2016

Xataka, http://www.xatakandroid.com/seguridad/se-encuentra-un-bug-con-el-que-se-pueden-clonar-las-huellas-dactilares-en-los-galaxy-s5, 25/10/2016

Ipadizate, http://www.ipadizate.es/2015/07/26/homekit-fabricantes-accesorios-quejan-seguridad-apple/, 25/10/2016

GTD y planificación a largo plazo

En el ámbito de la planificación y organización personal, siempre he hecho uso de tecnología para poder acceder a mis listas de tareas. Bueno, exceptuando cuando iba al colegio y usaba una agenda la cual jamás conseguí usar correctamente. Esta agenda es igual que el mejor programa para gestionar tareas, sino estás convencido de aplicar un método, de revisarlo regularmente, no servirá de nada. Al empezar la universidad, con el Smartphone y una serie de programas aprendí a planificarme mediante listas de tareas digitales y un cierto compromiso de revisión, actualización y organización de las mismas. Haciendo uso de Wunderlist, creaba una lista de tareas para cada asignatura, creaba las tareas, les asignaba jerarquía, fechas, importancias y mediante una revisión regular conseguí una importante mejora de mi productividad personal.

Fue un amigo quien me recomendó leerme Gettings Things Done, de David Allen, un libro que trata de una forma de planificación personal que es la que he usado hasta ahora, o al menos es la técnica de la que he tratado de aprender más. Este libro me lo leí dos veces, con paciencia y tomando notas de lo más relevante y remarcando lo que no había entendido.

De esas dos lecturas saqué unas conclusiones interesantes. Una de las más

valiosas es que es necesario almacenar las ideas, no solo las tareas que tenemos que hacer. David Allen propone un método de registro lo más veloz posible que nos evite una pérdida de tiempo, o la pereza de registrarlo. Así que fue lo primero que puse en práctica. Con aplicaciones sincronizadas entre todos los dispositivos, sincronizo bandejas de entrada tanto de Todoist como OneNote. Así no solo registro las tareas que tengo que hacer sino también registro las ideas a desarrollar, películas y series que quiero ver, libros que leer, cosas que comprar… Esta técnica me ha permitido organizar mejor mis ideas y perder mucha menos información relevante de la que perdía antes. Esta es la fase de recopilación.

Otro aspecto relevante del libro de David Allen es la organización mediante el uso de contextos. Como ya he dicho antes, usaba Wunderlist y solo para las asignaturas de la universidad. Con los contextos he podido elevar mi sistema de planificación a toda mi vida, categorizando las tareas en función de donde estoy o lo que uso en ese momento, por ejemplo, casa, universidad, internet, pc, tienda… También he intensificado el uso del calendario para los eventos que tienen una hora o día determinados y son inamovibles, o eventos regulares.

Aun me queda por aprender bastante de GTD y cómo adaptarlo a mí de la mejor forma posible. GTD requiere de compromiso en su aplicación, no es bajarte una app y solucionar tu vida. Los aspectos en los que menos he avanzado es en la fase de procesamiento de la bandeja de entrada, muchas veces los proceso directamente cuando meto las tareas y no debería hacerse así. Si he conseguido tras bastante esfuerzo gestionarme con el concepto de proyectos de GTD y creo que me ha permitido mejorar mi organización.

GTD también habla de planificación a futuro usando una metáfora de la distancia a la pista de aterrizaje pero en mi opinión aunque es un concepto valido para planificación del futuro de tu vida es completamente insuficiente para poder elaborar una planificación de tu vida. En este aspecto prefiero otro enfoque al meramente formal. El enfoque del que suelo hacer uso para decidir que decisiones tomar en mi vida, en lo que sería el ámbito de la planificación estratégica se basa en algo que aprendí en filosofía. El concepto de Platón de la búsqueda de la felicidad mediante el equilibrio de todas las partes de la mente. Esto, junto con una aptitud crítica ante mi vida y con el objetivo de la autorrealización me ha permitido dar bruscos giros para alcanzar ese anhelado equilibrio que me permita tener en mente que quiero hacer en todos los aspectos de mi vida, como llegar a esos objetivos y mantenerme en pie en el proceso.

GTD me ha proporcionado unos elementos de planificación personal importantes, sin embargo, en cuanto a planificación estratégica y la búsqueda de mi propia felicidad, es algo en lo cual llevo ya tiempo buscando como alcanzarla de la mejor forma posible y me doy cuenta de que aún me queda mucho por entender, pero humildemente creo haber conseguido hacer grandes progresos con respecto a la persona que era, la que soy y me ha proporcionado una visión de lo que quiero ser que me permite seguir adelante con ilusión.

El gran hermano te vigila

Big brother is watching you

Recuerdo claramente uno de los mejores libros que he leído, aquellos que lo hayan leído lo habrán identificado al momento por el título de este artículo. Hablo de **1984**. Y porque esta referencia a esta gran novela distópica que recomiendo a todo aquel que no la conozca. El motivo es las oportunidades y peligros del Internet de las Cosas.

En estos últimos 10 años hemos asistido a una **perdida de nuestra privacidad** que ni el propio Orwell podría haber imaginado. Cualquier persona que sepa indagar un poco en las redes sociales puede extraer información de otras personas, ya sea explicita o implícita. Internet se ha convertido en un lugar peligroso. Pero no podemos pensar que por esta perdida de la privacidad que a la mayoría de los usuarios parece no importarles, se vaya a detener, va a ir a más.

Prediction of IoT

Las **posibilidades del internet de las cosas** son incontables, me atrevería a decir que será la gran **promesa de la próxima década**. Nos permitirá tener casas interconectadas que se anticipen a nuestras necesidades o ciudades inteligentes que ayuden a los invidentes y nos proporcionen información adicional de nuestro entorno que nos pueda interesar.

El numero de datos generados van a seguir creciendo y más si incorporamos más y más dispositivos a las redes que recopilen información del entorno, la transfieran y luego esta sea almacenada, analizada y utilizada.

Una vez asumido este futuro y comprendido el presente la pregunta es si es necesario renunciar a nuestra privacidad por las comodidades de estas nuevas tecnologías. El IoT ya está asomando, empezamos a tener televisores conectados, accesorios para crear las llamadas SmarthHomes, pulseras cuantificadoras como las Fitbit y ya se han producido polémicas al respecto de todos estos dispositivos. Sin ir más lejos Samsung recomienda que no hablemos de información sensible delante de nuestro televisor porque esta sería enviada a sus servidores para el reconocimiento de voz y almacenada. Que símil más terrorífico con las telepantallas de la novela anteriormente citada.

Por supuesto no tiene buena pinta el futuro al que avanzamos. Si existen buenas prácticas al respecto de como tratar la información privada, sin embargo es necesario que sean las empresas las que lo implementen, y si su negocio se basa en esta información van a ser reacias a hacerlo.

He leído un interesante artículo de ISACA Journal donde se habla claramente de distintos Frameworks de buenas prácticas a la hora de tratar información privada relacionado con el Internet of things, esto se conoce como FIPPs. Proporciona un marco de referencia para el diseño de programas y tecnologías basadas en el Internet of things. Existen dos modelos inspirados en el **FIPPs**, para empezar el GAPP y también el NIST. **GAPP** se centra más en cumplir con buenas prácticas internacionales, luego solo son necesarias pequeñas modificaciones para las leyes locales. En cambio **NIST** se centra en garantizar el cumplimiento de las leyes federales en este ámbito.

Cambiando un poco de técnicas, ahora voy a hablar de la **privacidad diferencial**, una técnica que busca proteger a la gente a la hora de llegar a conclusiones a partir de sus datos. Esto supone extraer conclusiones de los usuarios como conjunto o subgrupos y no como individuos. No es la técnica de agregación que ha demostrado ser vulnerable permitiendo sacar información de individuos anonimizados. Esta técnica usa cifrado, inserciones de ruido y procura garantizar que matemáticamente no se pueda asociar los datos con tu identidad. Dicha técnica ha sido desarrollada por Microsoft y tanto Apple como Google afirman que la utilizan.

El negocio del futuro es la información, con ella se puede prever los comportamientos sociales de grandes grupos y anticipar las necesidades del usuario. Yo veo un futuro en el que esta información se utilice para ayudar a curar enfermedades no como un mecanismo de control en el que no puedas hablar ni en tu casa. Los peligros son reales, la amenaza del terrorismo está más presente que nunca y muchos políticos tratarán de solucionar el problema de la única manera que saben, controlando y espiando de manera masiva. La promesa de solucionar este problema mediante el espionaje ha seducido a muchos, pero si abrimos la veda para perseguir con una policía del pensamiento quien nos garantiza que su baremo en el futuro no cambiará en cuanto a lo que considera que es una amenaza.

En mi opinión la solución a este problema pasa por la implantación de **estándares** que garanticen la privacidad, **supervisiones** regulares obligadas por parte del estado y unas **normas** claras de que se puede hacer y que no con esa información. Lo que me gustaría ver cuando compro una SmarthTV o accedo a Google Photos es un organismo internacional que ha dado su **sello de aprobación** a la plataforma o producto y que me garantice que esos datos son míos y que no se van a utilizar para cosas que no se me ha dicho que se usan así como que no va a ser un peligro para mi en el futuro, sea yo un político importante o una persona común.

<<Gizmodo>>, Polemica por las SmartTV de Samsung, http://es.gizmodo.com/polemica-por-las-smarttv-de-samsung-pueden-oirte-y-en-1684622232

<<Panda Security blog>>, Panda Security, acceso el 8 de octubre de 2016 http://www.pandasecurity.com/spain/mediacenter/seguridad/privacidad-diferencial/
Doron Rotman, Chris Krypreos, Sarah Pipes <<Back to the Future in Device Security>>, ISACA Journal (2015) http://www.isaca.org/Journal/archives/2015/volume-6/Pages/back-to-the-future-in-device-security.aspx