MESA REDONDA

Tecnologías de valor.

El lema del ASTICNET "Avanzando hacia la sociedad digital" nos habla de la sociedad que viene, pero también de la sociedad actual.

NURIA SERRANO BENAVENTE
Jefa de área en el Ministerio de Industria, Turismo y Comercio

La Administración ya trata a día de hoy con una sociedad conectada, acostumbrada a resolver a golpe de teléfono la mayoría de gestiones cotidianas de sus vidas, ha probado los servicios que las nuevas tecnologías son capaces de ofrecer y conoce cuáles son sus ventajas. Por lo tanto, esos son el tipo de servicios que esperan obtener de su Administración.

Así pues, tenemos la obligación de llevar a cabo la tan manida transformación digital de la Administración Pública para ponernos al día; no porque sea la expresión de moda, sino porque debemos buscar la manera de proveer el mejor servicio posible al ciudadano y de aportar el mayor valor añadido posible.

La mesa, titulada "Tecnologías de valor", presentó de forma somera tres tecnologías tratando de presentar en qué proyectos o actuaciones podrían aportar mayor valor para generar servicios innovadores apoyándose en tecnologías o técnicas que suenan futuristas pero que ya son una realidad.

Para ello, la mesa contó con la presencia de tres especialistas de empresas relevantes en su sector, y con Elena Moreno, Técnica Superior de Proyecto Informático en el Ministerio de la Presidencia, para aportar el punto de vista de la Administración sobre la implantación de las mismas.

Con todos ellos compartimos una serie de preguntas destinadas a cubrir los aspectos más relevantes de cada proyecto que dieron lugar a un debate interesante, cuyos aspectos más relevantes transcribimos aquí.

PONENTE/ENTREVISTADO:

DAVID CÁCERES
Solution Director en la Enterprise Business Unit de Huawei

Proyecto VDI

En primer lugar, se contó con la presencia de David Cáceres, Solution Director en Huawei Technologies, para averiguar más sobre un proyecto que podría resultar interesante para muchos organismos de la Administración: La implantación del Escritorio Virtual Digital.

¿Podrías explicarnos a grandes rasgos qué supondría abordar la virtualización de los puestos de trabajo y qué objetivos podríamos alcanzar con este proyecto?

El primer punto es realizar un buen análisis y una buena prueba de concepto, asegurar qué es lo que se quiere cubrir y definir claramente los objetivos del proyecto. Es necesario asegurar que el ROI del mismo es efectivo y medible. Estos objetivos deben incluir una mejora en los procesos relacionados con el puesto de usuario, sistemas más ágiles, menos interrupciones, menos necesidades de soporte y, como objetivo menos tangible, que el usuario sienta el puesto de usuario como una herramienta que realmente le facilita el trabajo y no que le genera problemas.

Algunas de las ventajas obtenidas serían el contar con sistemas de seguridad mejorados, asegurando la continuidad del servicio, disponer de plataformas donde el usuario sea más autónomo en la resolución de problemas, y por último, adaptarse a las nuevas necesidades de mercado y poder explorar la utilización de nuevas herramientas-soluciones sin que esto suponga un proceso tedioso o costoso.

¿Cuáles serían las posibles ventajas del uso de VDI en la AGE frente al uso de los PCs tradicionales?

Principalmente son tres ventajas: ahorro de costes, flexibilidad y seguridad.

1. Ahorro de costes en cuanto a la mejora en la gestión, la reducción de necesidades de soporte local para centros remotos y la reducción de tasa de problemas al disponer de un sistema con altos estándares de servicio y resiliencia que garanticen continuidad de negocio. A estos, hay que añadir los Modelos de pago por uso y por supuesto un sinfín de ahorros indirectos relacionados con la utilización de los recursos de manera más eficiente.

2. Flexibilidad por la posibilidad de disponer de sistemas bajo demanda en minutos, contar con más de un sistema por usuario o utilizar grandes centros de datos para aprovechar sus capacidades en momentos puntuales. Además de la optimización en los procesos de renovación de plataforma, tanto a nivel software como a nivel hardware.

3. Seguridad, al garantizar el no acceso a los datos por personas no deseadas, mejorar el control de acceso de usuarios y poder controlar la información que está disponible en cada momento. Además de poder implantar mecanismos de marchas atrás para recuperación ante desastres, copias de seguridad instantáneas, optimización de la consecución del compliance y la posibilidad de adaptarse y desplegar nuevos mecanismos de seguridad sin que ello suponga un trauma para la organización ni para el usuario.

¿Cuáles serían los principales inconvenientes o dificultades para su implantación en la AGE?

Pensamos que el cambio de paradigma en el modelo tecnológico del usuario final y la adaptación a las necesidades más concretas y específicas de la AGE pueden ser los puntos más complejos a resolver, que no imposibles. Otro punto que suele generar conflicto es la utilización de diversos dispositivos que no se han utilizado previamente en soluciones VDI, pero con nuestros protocolos y desarrollos propios estos problemas se suelen solventar de manera ágil.

Desde el punto de vista de la Administración, ¿cuáles serían los principales inconvenientes/dificultades para su implantación en la AGE?

Las principales reticencias/inconvenientes serían:

a. Seguridad: se podría reforzar con comunicaciones cifradas, uso de un proveedor de Cloud certificado ENS, sistemas de identificación extensibles: certificado, doble factor... Se deben revisar de forma exhaustiva la viabilidad, sobre todo desde el punto de vista legal, de realizar transferencias de datos entre "nubes" de distintos países.

b. Aspectos legislativos: se podría hacer uso de cualquier servicio en la nube que respete la legislación comunitaria y nacional, que ya los hay. En concreto hay varios proveedores ENS certificados. No obstante, se podría contar con el asesoramiento de la AEPD y el CCN, por citar algunos ejemplos.

AsticNet 2018

c. Cautividad de un proveedor de cloud. Para evitarlo, es fundamental elegir un proveedor que disponga de una nube estandarizada. Existen varios organismos internacionales que han dedicado grupos de trabajo específicos en los últimos años a la estandarización de estas tecnologías, por ejemplo:

i. IEEE, con los grupos de trabajo, P2301 (estandarización de la gestión y la portabilidad en cloud computing mediante diferentes interfaces y formatos) y P2302 (federación e interoperabilidad entre clouds, como el intercambio de datos entre nubes).

ii. ITU-T, que estudia la computación en nube, hay un grupo de trabajo SG13 que dirige la actividad de normalización de Cloud Computing; además el grupo SG17 cubre la seguridad en la nube.

iii. ISO e IEC a través de la JTC (Joint Technical Commission) y el subcomité 38 DAPS (Distributed application platforms and services).

d. Costes de migración vs mantener lo existente. Se debe evaluar para cada organización en función de varios factores: número de usuarios, centralizado/distribuido, perfil de usuarios.

e. Resistencia al cambio e impacto de adaptación al nuevo paradigma: es imprescindible apoyo de la dirección para superarlo.

Visto desde dentro de la Administración, ¿cómo crees que podría contratarse un servicio VDI de acuerdo a la Ley de Contratos del Sector Público?

Se requiere un modelo contractual lo suficientemente flexible para ajustarse a la casuística del servicio y su escalabilidad.

En la actualidad, y de conformidad con la legislación vigente, sería posible la contratación de este tipo de servicio a través de un procedimiento abierto donde el pago se produjera en función de indicadores cuantificables para el servicio; por ejemplo: número de usuarios, número de escritorios/perfiles distintos; igualmente sería necesario incluir en los PPTs unos acuerdos de nivel de servicio adecuados. Igual que se definen unidades de trabajo en un abierto que cubre la asistencia técnica de ciertos servicios, podrían definirse "unidades de aten-

ción básica al usuario" en las que se incluirían un mínimo de prestaciones incluidas. El Gobierno Vasco ha licitado ya trabajos similares mediante procedimientos abiertos.

¿A qué tipo de organismo crees que se adaptaría mejor un parque virtual de puestos de usuario?

Las soluciones cloud tradicionalmente se han visto con mayor beneficio para las Administraciones más pequeñas, pero esto no tiene porqué seguir siendo así. En organizaciones distribuidas geográficamente o con competencias muy descentralizadas también podrían aportar valor.

¿Crees que es posible implantarlo en sedes u organismos en los que el número de empleados es elevado?

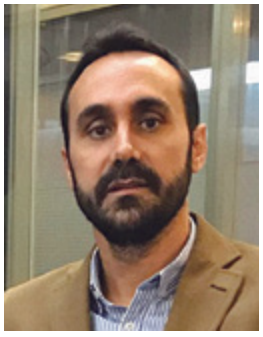
Sin duda. Actualmente el departamento de I+D de Huawei cuenta con 100.000 ingenieros que trabajan en modo VDI sobre Cloud y tienen a su disposición más de 170.000 escritorios virtuales. Este es el core de la compañía y el número de perfiles es muy variado: diseño, pruebas, implantación, ingeniería, análisis...

El modelo virtual puede ser aplicado a prácticamente cualquier organismo. Las grandes ventajas podrían ser para la gestión de centros remotos con muchos puestos de usuarios u oficinas muy dispersas que requieren de un soporte local. También puede ir enfocado a ciertos tipos de áreas con trabajos muy específicos y que requieren de altas necesidades de computación. Los centros con volatilidad en las cargas por procesos puntuales también pueden ser buenos focos de modernización.

¿Crees que podría suponer un valor añadido para el ciudadano?

Son beneficios más indirectos, pero se ganaría en agilidad en la atención y no disrupción del servicio por problemas locales. Igualmente, tender a "comoditizar" la tecnología permite dedicar recursos, tiempo o dinero a otro tipo de necesidades.

PONENTE/ENTREVISTADO:



CÉSAR TAPIAS HERRANZ
Responsable de la división de datos no estructurados en DELL EMC

Data Lake

El segundo de los participantes en la mesa sobre tecnologías de valor fue César Tapias Herranz, Responsable de la división de datos no estructurados en DELL EMC. Con el tema "Las bases para desbloquear el capital de los datos en la Administración Pública" habló de los datos y del potencial de los data lakes para transformarlos en valor.

El título de la presentación habla del capital de los datos, ¿a qué te refieres?

La base de la transformación digital está en los datos y los datos se están convirtiendo en el principal capital de las compañías. Por ejemplo, IDC, que predice que en 2021 más del 50% del PIB estará digitalizado, u Ocean Tomo, recientemente actualizó un estudio de 2015 donde concluye que el 84% del valor de las 500 compañías del mundo proviene de recursos intangibles.

Estos datos ponen de manifiesto que la información se está convirtiendo en el principal activo de las compañías a día de hoy, más allá de los recursos físicos.

¿Y qué es la Administración Pública, si no datos?

La transformación digital se suele asociar mucho con la compañía privada, centrando sus beneficios en buscar ventajas competitivas, pero no se trata solo de eso, si no también de buscar eficiencias, minimizar riesgos... En la Administración Pública la transformación digital nos puede ayudar a mejorar los servicios, dotarlos de más calidad, reducir costes e incluso desarrollar nuevos servicios.

Los términos big data, inteligencia artificial, internet de las cosas (IoT) que se asocian a la transformación digital, parece que son algo que no aplica a todo el mundo, sólo a aquellos organismos suficientemente grandes. ¿Es así?

Obviamente hay ministerios que pueden verse más favorecidos que otros, pero sin duda muchos más de los que pensamos podrían beneficiarse de la transformación digital. Trabajamos con ministerios del interior y defensa para identificar zonas de conflicto y ajustar patrullas en tiempo real o en resolución de crímenes, con servicios de salud para integrar nuevas fuentes de datos como la genómica, o la patología digital que ayuden a mejorar la prevención el diagnóstico y la curación de enfermedades, con ministerios de industria para optimizar el uso de la energía y control de distribución de aguas, en definitiva, en multitud de ámbitos que van más allá de la ciencia ficción asociada al Big Data.

Tradicionalmente cuando se ponen ejemplos de aplicaciones del Big Data caemos en los típicos asociados a redes sociales, internet, etc. Esto también tiene cabida, por ejemplo podríamos medir el impacto de una

campaña en la población a través del análisis de redes sociales, pero antes de pensar en cómo integrar las fuentes de datos que existen fuera de la Administración Pública, sería interesante integrar y explotar los propios datos de la Administración para optimizar los servicios, y eso no es sólo big data, también es aprovechar la digitalización de la Administración y la constante interacción con el ciudadano.

¿Y cuáles son las barreras o retos que crees que existen en la Administración Pública para abordar esa transformación?

Obviamente existen varios factores:

- Que no partimos de cero, la Administración no es una start-up nativa digital, y tenemos que transformar una IT, unos servicios que actualmente existen, y que tenemos que continuar dando.

- Como toda transformación, requiere una fuerte inversión. En este punto lo ideal sería conseguir una infraestructura que nos pudiese garantizar los servicios actuales al tiempo que nos permite abordar dicha transformación.

- Que hay múltiples fuentes de datos, están dispersas y además manejan contenido no estructurado o no fácilmente analizable.

- Que estamos hablando de muchos datos de naturaleza y estructura muy diversa, y cuyo valor varía en función del momento, por lo que necesitamos arquitecturas muy escalables e hiperflexibles.

- Que hay muchas aplicaciones que transformar, muchas nuevas herramientas con las que integrarse que fomentan las arquitecturas autocontenidas para dar libertad al desarrollador, pero por otro lado necesitamos entornos estables con garantías, y por supuesto como administradores de IT, se necesita control. Y todo ello a la vez.

Y desde el punto de vista de la Administración, ¿algún factor más que añadir?

Otra característica de estos proyectos a comentar sería la descentralización de competencias, puesto que existen diferentes niveles de AP con competencias distintas sobre las mismas colecciones de datos. Se requiere consenso institucional para el tratamiento de los mismos.

Igualmente, se requeriría un modelo de contratación flexible; además, como César ya ha comentado, la inversión inicial puede ser muy significativa; quizá podría pensarse en modelos cofinanciados entre distintos niveles de AP.

¿Y cuál sería el rol de las unidades TI? ¿Deben asumir el papel de DPO? ¿El CDO debe tener perfil TIC?

Las instrucciones de la AEPD sobre el perfil que debe poseer el DPO no dejan lugar a dudas: este perfil no debe recaer en unidades encargadas del tratamiento de los datos, que es precisamente el rol de las unidades TI.

El Chief Data Officer (CDO) es uno de los principales ejecutivos de una organización, el cual asume la responsabilidad de la estrategia relacionada con los datos y la información, el gobierno de datos, el control y desarrollo de políticas y la explotación efectiva de los mismos, junto con la explotación de los activos de datos para crear valor de negocio.

Comparándolo con el CIO, el CDO desempeña una función más relacionada con riesgos, cumplimientos, gestión de políticas y funciones de negocio. Se trata de un rol que impulsa estrategias de información y análisis con propósito de negocio. El CDO podría incluso reportar al CIO, o bien funcionar en una posición paralela. En esencia, el CDO de una organización hace las veces de pegamento entre la estrategia de datos y las métricas.

Viendo todos los retos que conlleva, ¿cuáles crees que son las bases para transformar el IT pensando en las posibilidades que nos ofrece la transformación digital?

En primer lugar, crear un Data Lake, esto es un repositorio capaz de interactuar con fuentes de datos, usuarios y aplicaciones, independientemente de los formatos que se utilicen. Esto nos permitirá consolidar los innumerables silos de información, integrarnos con cualquier fuente de datos y trabajar con diferentes estructuras: Archivo, Objeto, Stream. Obviamente antes de analizar cualquier información necesitamos tener toda esa información.

Pero esta, a su vez, debe cumplir con los criterios/garantías que necesitamos para seguir dando servicio (alta disponibilidad, continuidad de servicios, seguridad, etc.), no olvidemos que todo esto no puede impactar negativamente al ciudadano.

El objetivo es invertir en una arquitectura que nos permita continuar dando servicio al tiempo que se crean los nuevos servicios digitales.

En segundo lugar, se deberá diseñar una arquitectura escalable que permita alinear el coste con el valor del dato. Escalabilidad es un término que en ocasiones no se utiliza correctamente. Un sistema escalable es aquel que mantiene su nivel de servicio a pesar del crecimiento, no es sólo un tema de capacidad. Asimismo, pensemos que esa escalabilidad va más allá del datacenter, para poder llegar a cualquier ámbito, ya sea una consejería o la propia nube. Esto es importante porque no solo hablamos de integrarnos con la nube a nivel de preservación de datos, sino para abordar incluso servicios (por ejemplo, imaginemos que no tenemos conocimiento

para crear el servicio, ni siquiera para crear un PaaS).

Dentro de esta definición de escalabilidad, cualquier arquitectura de nueva generación debe poder definir políticas para automatizarlo todo que nos facilite crear un catálogo de servicio. No debemos administrar infraestructura, debemos administrar servicios. Al final, el objetivo es crear un IaaS que facilite la transformación de datos en valor

a. Que se integre con múltiples herramientas de analíticas sin transformar el dato.

b. Que facilite la implementación de entornos autocontenidos.

c. Que permita integrar analíticas en tiempo real con analítcas batch.

¿Por dónde empezamos, cómo se puede contratar?

Como cualquier transformación, no sólo implica un HW o un SW, y eso afecta a las personas, ese expertise nos marcará el camino.

Podemos, por ejemplo, realizar una inversión en infraestructura para crear un IaaS (esto supone Inversión en tecnología (HW/SW) y el desarrollo de un portal de provisión,. Podemos ir más allá y crear un PaaS (supone incorporar herramientas) o podemos subir la abstracción y crear un portal de Servicios o un AaaS.

Y no todo tiene que ser onpremise, para todo ello tenemos también la nube, en la cual podemos crear un PaaS como pago por uso por ejemplo.

En la Administración, ¿crees que podría ofrecerse como un servicio horizontal?

Por supuesto, aunque por la inversión inicial que supone y la gestión del paradigma sería demasiado para un solo organismo, habría que pensar en modelos cooperativos.

PONENTE/ENTREVISTADO:

RAFAEL CUENCA CARMONA
Territory Manager Iberia en Rohde & Schwarz Cybersecurity

Seguridad

Los dos casos anteriores proponen proyectos que suponen grandes cambios frente a la infraestructura tradicional. No podemos olvidar un aspecto indispensable a la hora de afrontarlo: la seguridad. Rafael Cuenca Carmona, Territory Manager Iberia en Rohde & Schwarz trató varios aspectos clave a la hora de gestionarla.

¿Qué percepción de la ciberseguridad existe en la Administración? ¿Cuál es el grado de conciencia sobre seguridad?

En general, el principal problema de la seguridad no está relacionado con la tecnología, sino con la percepción en sí de la realidad digital de nuestra sociedad, de nuestras instituciones.

Pensamos que nuestras organizaciones están viviendo una transformación digital, y yo creo que el concepto ya de base es erróneo, ya que transformación tiene que ver con cambio radical, de crisálida a mariposa; mientras que evolución habla más de mejora progresiva, competitividad, optimización... y esa es la situación en la que nos encontramos.

Creemos que la Administración sigue siendo analógica, pero la realidad es que nuestra Administración es un sistema híbrido en evolución hacia un plano digital, siendo la base de ese sistema, las interacciones entre subsistemas, digitales desde hace mucho tiempo.

Esta falsa percepción de realidad hace que en muchos casos, al desconocer el riesgo, este no se tenga en consideración, y esto es lo que la "Industria del mal" utiliza para realizar sus actos delictivos.

Esta falta de percepción igualmente hace que descuidemos o confiemos en planteamientos preconcebidos sobre los sistemas de información que ya no son válidos, como por ejemplo el concepto de "user": pensamos en un user como una persona que se conecta a internet, pero hoy en día un user puede ser un algoritmo, una cosa, una api/aplicación, un bot haciendo web scraping... De hecho, los humanos en el tráfico de internet ya somos minoría.

Otro concepto es el relacionado con aplicaciones y seguridad. En primer lugar, hoy en día el concepto que tenemos de aplicación ya no es correcto, ya que la mayoría de las aplicaciones, (las aplicaciones son las que conforman internet) están basadas en Web services, y estas aplicaciones están sujetas siempre a una urgencia de un mercado y a una demanda de servicios cada vez mayor... ¿Realmente estamos invirtiendo los recursos adecuados tanto en desarrollo como en seguridad? ¿En qué factores me baso yo para evaluar la seguridad de la aplicación de un banco, por ejemplo? Ésta se basa en un sistema operativo, protocolo, subsistemas... que envía correcciones de su código cada cierto tiempo. Entonces, ¿puede ser que estemos asumiendo "by default" la calidad de las aplicaciones, y que de esta manera, esa falsa percepción de seguridad nos esté tapando el bosque?

Creo que el asunto de la ciberseguridad se basa en la percepción

AsticNet 2018

que tenemos y quizás la solución al problema comenzaría únicamente poniendo calidad en las aplicaciones, utilizadas pero desconocidas en muchos casos.

Dado que el estado de avance en temas de seguridad es tan desigual entre diferentes organismos, ¿cómo podríamos implementar perímetros de seguridad internos en la AGE para evitar la propagación de malware desde otros organismos?

Es complejo hablar de perímetros en un mundo que está eliminando lo físico en una evolución al plano digital hiper interconectado. Yo creo que más que hablar de perímetros deberíamos hablar de identidad digital, de seguridad en el dato, de seguridad en aplicaciones... Creo que son las claves.

Incluso si decidiésemos generar un perímetro, éste estaría supeditado a la fortaleza de los sistemas de identificación de los usuarios que accederían a la información con distintos niveles de clasificación, a través de aplicaciones. Por tanto, dependemos del usuario, de su cultura digital (no necesariamente mala), de sus intereses, situaciones, circunstancias... de lo que quiera hacer con la información, dentro o fuera, de una manera lícita, ilícita o quizás accidental (algún malware)... y, finalmente, de si las aplicaciones que provean esa información tienen vulnerabilidades, de si las API´s que se conectan con mis sistemas son seguros, etc.

La clave estaría en tener la información protegida, permitiendo su acceso a los usuarios habilitados dentro de los entornos reconocidos, permitiendo al usuario que ya tiene una cultura digital que utilice esa tecnología de manera segura, haciendo que esa información esté cifrada by default y que solo pueda ser leída descifrada por los sistemas autorizados basados en una identidad digital, todo soportado por aplicaciones seguras.

Igual que ha evolucionado el concepto de desarrollo vs sistemas/explotación al nuevo paradigma de devops, ¿de qué manera ha evolucionado el paradigma de la seguridad? ¿Cómo se integra la pata de la seguridad con las metodologías y herramientas ágiles?

La seguridad está evolucionando continuamente para adaptarse a los requerimientos de la sociedad y del negocio que exige inmediatez y agilidad.

El nuevo paradigma devops habla de esto, pero en el mundo real nos encontramos con una disrupción entre lo que tiene que ser y la realidad. En lo referente a seguridad, metodología choca con plazos, costes, etc. La realidad es, que hoy en día, la seguridad en el desarrollo de aplicaciones queda relegada a un plano secundario: si hay tiempo y dinero se hace, en caso contrario se asume el riesgo.

Sí es cierto que existe una evolución, y yo creo que todo va en esa dirección, pero aún queda camino por recorrer.

Hemos estado hablando sobre proyectos que implican trabajar en la nube (los otros dos temas son VDI y Data Lake), ¿es posible ofrecer servicios de seguridad integral en la nube a un organismo AGE?

La pregunta ya no es si es posible, sino si realmente hay alternativa... En un mundo basado en entornos virtuales en los que los usuarios se conectan a sus aplicaciones desde múltiples dispositivos, entornos, ¿hay alternativa? Es decir, yo me conecto a mis aplicaciones desde el móvil, pc, cibercafé... independientemente de que ponga controles en mis dispositivos, ¿dónde tiene más sentido establecer esa protección? Hoy en día... ¿y mañana?

Creo que efectivamente no es una opción, lógicamente dotado de las medidas de seguridad adecuadas, regulaciones que garanticen la protección de datos, etc. pero va a ser así.

¿Cómo se evita la percepción de la seguridad como un freno a la revolución digital? ¿Hace falta un cambio de mentalidad en las organizaciones?

Yo creo que más que de freno tendríamos que hablar de temor, ya que la evolución es imparable, y en muchos casos ya no solo no se dispone de los recursos, sino que adicionalmente, tampoco se dispone de la percepción y el conocimiento adecuado para poder incluso realizar un análisis de situación. Precisamente el freno no es la percepción de seguridad sino la percepción de inseguridad ante un entorno en evolución constante.

Los sistemas están evolucionando de tal manera, que en entornos en los que antes era posible separar sistemas, comunicaciones, seguridad... ahora todo se está mezclando en una interacción automatizada, y la realidad es que las empresas, organizaciones están tendiendo a soluciones basadas en servicios que garanticen esa disponibilidad y accesibilidad requerida para poder evolucionar.

¿Qué implicaciones del nuevo RGPD podemos destacar?

Pues únicamente decir que el RGPD es algo mucho más interesante, a pesar de parecer una norma destinada a martirizar a los administradores de sistemas CIO, CSO...

El RGPD trata de proteger a los usuarios, de protegernos a todos en un mundo digital gobernado por datos en forma de números de tarjeta de crédito, números de seguridad social, compras, expedientes médicos, etc. Por desgracia, la única manera de que esto se aplique, es a través de regulaciones, y esto ya está aquí.

Los que trabajamos en esta área ya desde hace demasiado tiempo hemos visto cómo este asunto, la seguridad, siempre ha sido relegado a un segundo plano. Hemos conocido problemas de seguridad, los hemos sufrido y, aun así, el asunto de las sanciones se ve como algo exagerado, cuando la realidad es que si no se sanciona no se hace.

Yo estoy de acuerdo con que el señor que guarde información mía en su sistema y que haga negocio con ella, si no la custodia, si tiene algún problema, que pague. Es la única manera en la que esto funciona en el mundo real. ✱