



EL GOVERN TIENE DESPLEGADOS MÁS DE 100 PROYECTOS (DATO, IOT, NUBE...)

Valencia pone rumbo a la digitalización

« Valencia es la siguiente etapa de nuestro tour por la geografía española para conocer de primera mano cómo está evolucionando la digitalización dentro de nuestras instituciones públicas: ¿Qué proyectos tienen en marcha y qué nivel de madurez están alcanzando? ¿Cuáles son los inhibidores y los reactivos para su modernización? Estas y otras cuestiones han sido debatidas en este encuentro presencial de Computing.



Los contertulios, representantes de las diferentes instancias administrativas de esta Comunidad, se muestran un tanto críticos por factores estructurales que entorpecen una transformación más fluida, pero reconocen que los avances han sido muchos, y que la pandemia, de nuevo, ha servido de acicate para establecer unas nuevas reglas de juego. Muchos trámites que antes se realizaban de forma presencial ahora se realizan de forma telemática, la nube se presenta como el escenario ineludible (el correo y otras aplicaciones ya viven en el cloud) y la ciberseguridad se ha convertido en la principal trinchera de las instituciones, tanto en presupuesto como en atención prioritaria. Quedan retos organizativos, de gestión de identidades, de reciclaje

de personal, de liderazgo, de captación de talento... como quedó expresado en esta interesante jornada en la que Computing contó con la colaboración de Commvault, IPM y Okta (a través de Ingecom).

El Gobierno de la Generalitat Valenciana está subido a esta ola de transformación merced a un plan estratégico que lanzó en el mes de junio pasado, como continuidad de uno anterior al que le pilló la pandemia y que fue algo criticado por no haberse concentrado en la transformación. Un nuevo plan de transformación digital liderado por el President de la Comunitat Valenciana dotado de 1.000 millones de euros y que se compone de seis ejes: Infraestructuras, comunicaciones y movilidad imprescindibles y críticas; Gobierno inteligente; Gobierno sostenible; Educación Digital;

ENRIQUE MARTÍN, OKTA PRODUCT MANAGER DE INGECOM

“OFRECEMOS UN PORTFOLIO COMPLETO DE GESTIÓN DE IDENTIDADES”



Los organismos públicos se han digitalizado, han conseguido subir muchos servicios a la nube y esto hace que la identidad de las personas que tienen que acceder se vea vulnerada. Desde OKTA, podemos ofrecer soluciones para que todas las aplicaciones que pueden estar tanto en on premise como en el cloud para las diferentes administraciones puedan ser accedidas de una forma segura identificando que la persona que está accediendo es quien dice ser. OKTA ofrece un portfolio completo de la gestión de identidades y la gestión de acceso a las

aplicaciones desde una funcionalidad básica de SSO, diferentes soluciones de MFA adaptativo en función de quién accede, cómo accede y dónde accede, así como poder trazar todo el ciclo de vida de la identidad dentro de las organizaciones. Otro punto crítico es el acceso a los servidores, ofrecemos un pool de herramientas de acceso privilegiado a ellos. Asimismo, vemos una mezcla de aplicaciones en cloud y on premise, donde OKTA también aporta Access Gateway para ofrecer esa integración en ambos mundos.

NURIA BRUNAT, TERRITORY ACCOUNT MANAGER DE COMMVAULT

“HAY QUE SEGUIR AVANZANDO EN LA CONFIANZA DIGITAL”



Las AAPP ya han iniciado su proyecto de digitalización, camino hacia el cloud, habilitando trámites y gestiones de forma telemática que anteriormente se hacían de forma presencial en las oficinas. También están implantando aplicaciones en la nube como es el caso del correo electrónico. Este camino iniciado nos debe servir para seguir avanzando, pero sin perder de vista la seguridad de los datos al ciudadano. Es lo que denominamos la confianza digital. No hay que

olvidar que en el mundo, cada pocos segundos, se produce un ataque de ransomware, lo cual pone en riesgo la garantía y la disponibilidad de la información. En Commvault contamos con una suite de productos que se gestionan de forma unificada desde una plataforma y que básicamente nos permite garantizar la seguridad de la información y la disponibilidad de los datos. Una función que permite a las Administraciones Públicas ofrecer un mejor servicio al ciudadano.

Sanidad y servicios digitales sociales eficientes; y Justicia moderna. La misión de GEN Digital 2025 es culminar la transformación digital de la Administración del Consell y sus organismos autónomos, digitalizando la forma de trabajar, racionalizando y simplificando la gestión y los procesos internos y transformando la cultura organizativa de la Generalitat.

Este ambicioso plan, como detalla José Manuel García, director general TIC de la Conselleria d'Hisenda i Model Econòmic, cuenta con más de 100 proyectos como es el caso de AMURA, un plan de comunicaciones valorado en 35 millones al año, que

incluye 5G y servicios de banda ancha de muy alta capacidad. Otro proyecto destacado es ÁNIMA, dirigido a la gobernanza de datos, cuya idea es conseguir la homogeneización del dato en la Generalitat. Esta institución está embarcada en la reducción de sus tres centros de datos actuales a dos, e ir avanzando hacia un modelo de nube privada para toda la organización. “Vamos a ir a la nube con diferentes sabores y la idea es que el legacy vaya desapareciendo”. El directivo también menciona la iniciativa PICA, que se basa en la gestión de la calidad del aire a través de un modelo de Internet de las Cosas.

JOSÉ CARLOS MORÁN, HEAD OF STRATEGIC ACCOUNTS DE IPM

“LA SEGURIDAD DEBE CONFIGURARSE EXTREMO A EXTREMO”



Estamos en un momento ideal para impulsar la digitalización de los organismos públicos, porque el entorno de pandemia ha generado unas necesidades que hacen que se tenga que acelerar esta transformación de las organizaciones. Desde IPM creemos que uno de los ejes importantes va a ser el acceso a las aplicaciones y a la información y en particular la parte de virtualización de aplicaciones y del puesto de trabajo, combinado todo ello con el ámbito de la analítica de datos y de seguridad. La necesidad

de tener que acceder a la información y poder trabajar en cualquier ubicación hace que todo ello se convierta en una necesidad imperiosa. Con el teletrabajo, lo que atañe a ciberseguridad se traslada al hogar y no solo hay que tener en cuenta los problemas de acceso. En IPM contamos con una solución vertical dedicada al puesto de trabajo que incorporamos además de manera horizontal con todo lo relacionado con la seguridad. Y todo ello debe configurarse de extremo a extremo.

Muchos trámites que antes se realizaban de forma presencial ahora se realizan de forma telemática, la nube se presenta como el escenario ineludible

Dos ámbitos de la Administración Pública

José Benedito, jefe de Servicio de Informática y Administración Electrónica de la Diputación de Valencia, distingue entre dos ámbitos diferenciados: prestación de servicios al ciudadano y funcionamiento interno de las instituciones. En relación con el primero, “la pandemia ha supuesto un impulso para servicios electrónicos mejores, un largo camino de años que ha llevado consigo muchas dificultades. Es necesario garantizar los derechos de los ciudadanos y acercarnos a su lenguaje y a los canales que utilizan. En cualquier caso, considero que hemos avanzado y ahora son los aspectos de ciberseguridad los que más nos impactan”.

Por lo que respecta al funcionamiento interno, “somos instituciones presenciales que en dos días pasamos al teletrabajo con éxito. Pero no hemos modificado la organización: ¿qué hacemos con los ordenanzas, con los conductores y auxiliares administrativos que se cuentan por miles y cuya labor pierde sentido fuera del centro de trabajo?”. Desde su punto de vista, “no sabemos cómo aplicar el teletrabajo en unas organizaciones que no miden la productividad ni tienen productos tangibles. Con esta falta de indicadores, corremos el riesgo de una vuelta atrás”.

Manuel David Serrat, técnico de Organización y Coordinación de Sistemas y TI de la Sindicatura de Comptes de la Generalitat Valenciana, completa este argumento: “Históricamente lo que se ha hecho para reducir el tamaño de la Administración ha sido no reponer las bajas, y se ha perdido la oportunidad de reponer una parte de

personal que puede realizar esas funciones, pero ya utilizando tecnología y ya habiéndola mamado desde la cuna. Es muy complicado que el funcionario a partir de una determinada edad se recicle en sus tareas, se requiere muchísima formación y algún que otro incentivo (que brillan por su ausencia), por lo que necesitas una vía a través de la reposición de personal para incorporar talento, no necesariamente en funciones muy tecnológicas, sino que sepan utilizar bien sin apoyo de nadie el uso de las aplicaciones informáticas, utilizar certificados, dobles factores de autenticación en determinados sistemas y entender la ciberseguridad en el correo electrónico”.

Javier Mateo, subdirector de Emprendimiento Valencia Activa del Ayuntamiento, añade una incógnita más a esta ecuación. “Cuando hablamos de digitalización con el ciudadano nos olvidamos de la automatización y la aplicación de la inteligencia artificial. Tenemos muchas tecnologías que pueden automatizar los procesos y tarde o temprano tienen que llegar. Las administraciones públicas tienen que ver esa gestión del cambio. Tenemos pilotos en Valencia que ya van incorporando estas tecnologías, no se trata de eliminar puestos de trabajo sino de aportar valor. Es necesaria una transformación continua de talento, abordar cursos de tecnología avanzada, más allá de Excel. Corremos el riesgo de que nos estalle en las manos, y esta gestión del cambio tiene que venir desde arriba. Los tiempos son vitales”.

Policía local, una Administración especial
Capítulo aparte merece la Policía Local de

ASISTENTES

1 Javier Mateo, Ayuntamiento de Valencia | **2** José Benedito, Diputación de Valencia |
3 José Manuel García, Conselleria d'Hisenda i Model Econòmic - Generalitat Valenciana |
4 Jesús Mandingorra, Conselleria de Sanitat Universal i Salut Pública - Generalitat Valenciana
5 Manuel David Serrat, Sindicatura de Comptes - Generalitat Valenciana | **6** Eladio Barber,
 Policía Local de Valencia | **7** Manuel Esteve, Universitat Politècnica de Valencia



Valencia, como bien describe Eladio Barber, Comisario Principal y Responsable de la Unidad de Logística: “Nuestro problema reside en que somos Administración especial, resulta complicado comunicarte con los servicios del Ayuntamiento, la inmediatez tiene que ser total al tomar decisiones. Hay que tener gente cualificada y hacer análisis de decisiones en el servicio público de la calle. Desarrollamos nuestras propias aplicaciones y nos cuesta encontrar en el mercado herramientas que nos sean útiles; nuestros servicios no son los habituales y los proveedores no nos entienden”. Sus programadores son policías que disponen de los conocimientos técnicos para sistematizar las funciones de la institución. La ciberseguridad es, por añadidura, otra prioridad de su servicio, “trabajamos con información muy sensible de los ciudadanos (como es el documento nacional de identidad) y hay que garantizar que no puedan ser hackeados. Tenemos un centro de datos propio”.

De diferente índole son las circunstancias de la Conselleria de Sanitat Universal i Salut Pública, como describe Jesús Mandingorra, jefe de Área de Sistemas de Información del Consorcio Hospital General Valencia: “Tenemos médicos que se creen informáticos y eso nos crea muchos problemas. En el ámbito interno hemos avanzado, está completa la historia electrónica digital del paciente, aunque hay personas que todavía traen papeles. Antes había 10 celadores que entregaban a mano los expedientes, ahora escanean y gestionan

expedientes electrónicos. Hemos desplegado un portafirmas electrónico y hemos superado los problemas de la facturación. En la atención al ciudadano, no hemos avanzado tanto por problemas de identificación. Es complejo mantener la seguridad de los derechos de los ciudadanos al mismo tiempo con principios de transparencia y accesibilidad”. La ciberseguridad es una espada de Damocles, “el 16 de julio sufrimos un ataque de ransomware y hubo que mandar a los pacientes a casa. Pudimos parar el ataque y recuperar la información, con la ayuda de Commvault”.

Manuel Esteve, Catedrático de Universidad de Ingeniería Telemática de la Universitat de Valencia y Director del Máster de Ciberseguridad y Ciberdelincuencia, considera que la concienciación es el elemento fundamental. “La mayor parte de la seguridad de las organizaciones no depende de los técnicos, sino que está en manos de los usuarios. El pasado año empezamos un máster en ciberinteligencia y conseguimos poner de acuerdo a las áreas de Informática y Telecomunicaciones, algo inaudito”.

El segundo aspecto que Esteve considera vital es la preparación: “La preparación en el ciclo de gestión de incidentes es más importante que la propia respuesta. Cuando tomas las medidas reactivas estás vendido, pero lo que te garantiza que saldrás con éxito es la preparación. Esta guerra no se resuelve en la batalla sino en el entrenamiento. La preparación tecnológica, personal y de procedimiento vale para todo tipo de organizaciones”. ■