Texto Laura del Río
Fotografía Jorge Pariente
Vídeo Rubén Pagán

LA CATEGORIZACIÓN, EL PRIMER PASO HACIA LA PROTECCIÓN

Los datos de calidad sustentan el negocio

"Se debe vigilar igualmente tanto a empresas tradicionales como a los gigantes digitales"

Conjugar datos y negocio se ha convertido en el reto estrella para la empresa moderna. A la hora de encarar este desafío hay que tener en cuenta factores tan importantes como la correcta categorización y protección de los datos, esencial para extraer todo el valor que estos pueden tener para el negocio. En este escenario, la reunión organizada por Computing ha servido como termómetro para valorar el nivel de securización que están aplicando las organizaciones a sus datos y las medidas que están tomando para optimizar su gestión.

La administración pública tiene un doble reto respecto a los datos, ya que tiene que ser cien por cien garantista con la seguridad del ciudadano, arrastra una gran tradición en su gestión, y cuenta con unos recursos limitados. "La cantidad de datos que manejamos, no solo a nivel estatal, sino mundial, es otra de nuestras problemáticas", alegó Julio Perales, coordinador del área de Informática del Instituto de Turismo de España, entidad dependiente del Ministerio de Industria, Comercio y Turismo, y con cuyo departamento de Informática trabajan "codo con codo", aunque, en cuanto a la infraestructura TI, "recibimos soporte de grandes compañías", añadió. Más de un tera de datos estructurados, - "como identidades de turistas que visitan España, gastos, viajes, etc." -, y otros tantos no estructurados, - "como contenido multimedia"-, suponen un desafío no

ALBERTO GONZÁLEZ, ALLIANCES MANAGER DE COMMVAULT

"COMMVAULT FACILITA EL MOVIMIENTO DE CARGAS DE DATOS Y BACKUP ENTRE DISTINTOS PROVEEDORES"

Es providencial que el dato esté protegido desde su extracción hasta su almacenamiento o destrucción. Es por eso que la plataforma de Commvault securiza el dato durante todo su ciclo de vida, solución que se ha completado desde el hardware al software, pasando por los servidores y CPD, gracias a la alianza de la compañía con HPE.

Existe una clara tendencia entre los usuarios de adoptar la nube híbrida y el entorno multicloud, a pesar de que los proveedores cloud no facilitan el paso de uno a otro, ya que buscan salvaguardar su nicho de mercado. Así las cosas, Commvault se integra con más de 60 proveedores cloud para dotar a los clientes de la capacidad de mover sus cargas de datos y back up de una nube a otra, y da asesoramiento a los usuarios para levantar la computación donde ofrezca mayor rendimiento.

tanto en cuanto a su mantenimiento, sino en cuanto a cómo explotarlos: "Aún no sabemos cómo extraer información verdaderamente útil de estos datos", dijo Perales.

Pero si la Administración resulta particularmente sensible de por sí, esto aumenta cuando se trata de sectores como la sanidad pública. "En nuestro caso hablamos de petas de datos, no de teras, además de una alta criticidad", afirmó Ángel Luis Sánchez, jefe de servicio de Arquitectura y Normalización de la Subdirección General de Innovación y Arquitectura Tecnológica del Servicio Madrileño de Salud (Sermas), formado por en torno a 35 hospitales y unos 80.000 profesionales. Para el Sermas es tan importante conservar los datos como tenerlos disponibles 24/7; no obstante, cuenta con distintos niveles de almacenamiento, por ejemplo, "de las imágenes no hacemos backup, tan solo archivado", contó Sánchez, ya que, de otro modo, "conservar tanta cantidad de información sería insostenible".

Esta categorización del dato para su adecuado almacenamiento ayuda a la entidad sanitaria a no perder información, para lo que también se apoya en una sofisticada infraestructura de datacenter "con dos CPD en activo y uno de respaldo". Pero ¿es fácil perder un dato? Ángel Luis Sánchez respondió que "no es fácil, pero tampoco imposible", y arguyó que "los mayores fallos son humanos, por no seguir bien los procedimientos de preservación", aunque a su vez admitió que "a veces es complicado hasta darte cuenta de que lo has perdido". En este sentido, a veces la normativa choca con la viabilidad de los procesos. "La ley dicta que se debe guardar la historia clínica de un paciente durante unos determinados años, sin embargo, esto se hace cada vez más difícil debido, en nuestro caso, a la falta de inversión en infraestructuras que lo permitan", explicó. "Tan solo en torno a un 2% del gasto sanitario va al presupuesto TIC, la menor inversión de todas las administraciones", resaltó Sánchez. A su vez, tecnologías como la nube son muy prácticas en estas circunstancias, aunque "la cloud todavía sufre de la desconfianza de muchos políticos para albergar cierto tipo de datos".

En el ámbito legal no se quedan atrás en lo referente a manejo de datos sensibles; de hecho, en su caso tienen que tratar también con datos sanitarios y de otra naturaleza en muchas ocasiones. Así lo explicó César Mejías, CIO de Garrigues, quien dijo que en su base de datos contaban con hasta "180 millones de documentos, entre los que guardamos hasta los correos electrónicos con nuestros clientes de forma obligatoria". De este modo, Mejías afirmó que "al precio que está el giga, nos podemos permitir este almacenamiento masivo de datos y, así, crear un histórico". Para albergar todos estos datos, cuentan con tres CPD en activo, uno en Latinoamérica y dos en España, además de numerosas cintas y discos duros a la vieja usanza. "Nos da miedo alojar ciertos datos de clientes en la nube", admitió Mejías, ya que "ahora estos deben estar alojados en países que cumplan con el marco legal europeo". Así las cosas, si guardas tus datos, por ejemplo, en la nube de HP, un proveedor americano, "la Patriot Act (ley similar al GDPR europeo), puede bloquear tus datos en un momento determinado", comentó. El rol del Data Protection Officer (DPO) salió a relucir en el discurso de Mejías como alguien que han incorporado a la empresa para "garantizar la calidad e integridad del dato", al-

Agencia Tributaria,
José Borja Tomé

Commvault,
Luis López

Deloitte,
Jesús Rojas

Eulen,
Alejandro Las Heras

Garrigues,
César Mejías

HPE,
Javier Esteban

Instituto de Turismo de España,
Julio Perales

guien que, en el caso de Garrigues, también ha asumido las funciones del Chief Data Officer (CDO).

¿Dónde están nuestros datos?

Las personas nos preocupamos por la privacidad y destrucción de nuestros datos más de lo que parece, incluso, según señalaron en el encuentro, somos más reticentes a dar información a la AAPP o a otro organismo similar que a cualquier página de Internet o a las redes sociales. En este sentido, la aprobación de GDPR ha configurado un nuevo paradigma que ha hecho remover conciencias y responsabilidades, sobre todo "por el miedo a las elevadas multas a las que se pueden enfrentar quienes no cumplan con la normativa", admitió María Jesús Casado, responsable de Seguridad de la Información de la Intervención General del Estado. La Agencia de Protección de Datos le da especial importancia a los consentimientos y a la destrucción de cierta clase de datos privados, por lo que "si deseas conservar estos datos debes justificar por qué de manera legítima y contar con el consentimiento de las personas a las que pertenecen". Nuevas medidas que exigen una mayor inversión, que se ha producido según Casado: "No ha habido antes una dotación de recursos superior a la que se ha realizado para cumplir con GDPR", sentenció.

Respecto a la normativa, el auge del cloud juega un papel fundamental y que preocupa especialmente a Casado: "Es inevitable que todos vayamos a la nube tarde o temprano", dijo, "pero hay que hacer un estudio exhaustivo sobre qué datos son aptos para subirse al cloud y de qué manera, es decir, si cifrados o no". No en vano, actualmente los proveedores cloud precisan de certificación para trabajar con la Administración, algo a lo que Luis López, account manager del sector público de Commvault, contestó que, a pesar de su obligatoriedad, no les suelen pedir certificado alguno, "sea cual sea el partido que esté en el poder". Por el contrario, proveedores como Eulen aseguraron que a ellos siempre les ha sido requerido el certificado de seguridad cuando ha colaborado con algún organismo del sector público.

No obstante, en el encuentro lamentaron que, a la hora de firmar un contrato con la Administración, primen factores como los costes antes que las certificaciones de seguridad o la calidad de ciertos servicios. "Es cierto que los presupuestos son ajustados, pero por unos céntimos que te pases ya se cambia a otro proveedor más barato, aunque sea menos seguro", contó Javier Esteban, account manager de Hewlett Packard Enterprise (HPE). "Nosotros como proveedores no podemos hacer más que estar cualificados, certificados y cumplir las normas, pero hay márgenes que no podemos pasar y servicios que no podemos abaratar", sentenció Esteban; a lo que Casado añadió que en la AAPP son los primeros que sufren las consecuencias de unos presupuestos acotados "que no dependen de nosotros", dijo, "y que se reflejan además en la falta de otro tipo de recursos como el capital humano". También le sorprende a Javier Esteban el desconocimiento que a veces manifiesta la Administración sobre qué datos pueden y no pueden borrar, "lo que les impide establecer una estrategia clara de protección del dato".

Jesús Rojas, socio de Sector Público TIC de Deloitte, aludió a "la falta de categorización de los datos y de planificación" como uno de los principales errores que se cometen a la hora de

DAVID CAMINO, STORAGE PRESALES DE HEWLETT PACKARD ENTERPRISE (HPE)

"HPE OFRECE LA GESTIÓN DE UN MODELO DE BACKUP AS A SERVICE"

HPE es una compañía de infraestructura y servicios con una oferta end to end, actualmente muy focalizada en la seguridad y confidencialidad de los datos de sus clientes. Por este motivo, la empresa ha efectuado una alianza con Commvault que le permite brindar un modelo de backup as a service gestionado en una factura única de pago por uso, ya sea para los datos almacenados on premise o en la nube pública.

Para definir los SLA o (Service Level Agreement) con un proveedor de seguridad, lo primero que deben hacer las empresas es catalogar los datos y determinar una estrategia de recuperación de los mismos que garantice la continuidad del negocio en caso de que se produzca cualquier incidente. Después de establecer los pasos del disaster recovery, se decide qué datos merece la pena subir al cloud y cuáles no.

almacenar los mismos. "No diseñar una estrategia lleva a que muchas compañías se lancen a adquirir tecnología sin antes siquiera saber para qué la van a emplear", afirmó Rojas, "y esto afecta, además, a las personas y a los procesos". Rojas también incidió en que "la pérdida de calidad del dato a la hora de clasificarlo y guardarlo hace que no podamos sacar de él 'insight' de negocio".

El que parece tener cada vez más clara su estrategia es el sector de la Banca, y esta es "sin duda, data centric", señaló Daniel Martínez Batanero, director de Proyectos Estratégicos de Rural Servicios Informáticos (RSI). Para unificar los pasos a dar en torno al dato, RSI ha incorporado la figura del CDO bajo cuya supervisión y control están todos los data awareness y gestores de datos tradicionales. También ha implantado una plataforma scale out de la mano de Commvault que les permite securizar las capas superiores. Con todo, Martínez Batanero espera que la rigurosidad con que están siendo vigiladas las empresas tradicionales se aplique también a los gigantes digitales, ya que parece que para ellos "no es tan específico el uso que deben hacer de los datos".

Volviendo a las particularidades del sector público, la Agencia Tributaria se caracteriza por consumir "muchos más datos que otras administraciones monetarias internacionales", según José Borja Tomé, subdirector general de Tecnologías de Análisis de la Información e Investigación de la Agencia Tributaria. Porque recibe datos de muy diversas fuentes y por el compromiso que tiene con los ciudadanos de hacer un buen uso de los mismos, cada vez tiene más extendida la auditoría informática, que "les ayuda a detectar errores y a fortalecer el acceso a los datos, así como a potenciar su capacidad de análisis".

La nube a debate

El controvertido tema de la cloud nunca falta como elemento de debate. Mientras que algunos como Jesús Rojas desde Deloitte afirmaron que todos los fabricantes de software van encaminados hacia la cloud y, por lo tanto, "en unos años el modelo on premise dejará de existir inevitablemente", otros como Luis López de Commvault defendieron que el cliente enterprise "siempre tendrá un alto porcentaje de infraestructura on premise". En todo caso, ventajas como la capacidad de almacenamiento de la nube son innegables, no así la latencia, la disponibilidad o el ahorro de costes ya que, según dijeron, "muchas veces la nube se cae", y tiene "costes ocultos". Al mismo tiempo, la idea de que contratar un servicio de hosting no es estar en cloud fue expuesta por Ángel Luis Sánchez para rebatir la creencia que tienen algunos de que "sacar tus datos a un CPD externo es subir al cloud".

Estamos en un escenario cambiante para el que es muy difícil estar preparado, ya que "quizá va más rápido de lo que las organizaciones y usuarios somos capaces de asimilar", incidió Alejandro Las Heras, director de Tecnología de Eulen. Las organizaciones se ven muchas veces desbordadas por los datos, que además son muy dispersos, por lo que Las Heras aconseja dar pasos cautelosos como almacenar los datos según su criticidad, no subir a la nube sin hacer antes pequeñas pruebas con los datos menos sensibles o tomar las nuevas normativas como GDPR como oportunidades para mejorar la seguridad, ya que "la empresa que verdaderamente se equivoca es la que no se transforma". ■

IGAE,
María Jesús Casado

Rural Servicios Informáticos,
Daniel Martínez

Servicio Madrileño de Salud,
Ángel Luis Sánchez