DEBATES ciberseguridad TIC

Afrontando la seguridad del dato en las Administraciones Públicas

IR A PÁGINA SIGUIENTE

Afrontando la seguridad del dato en las Administraciones Públicas

Aunque el sector público ha logrado un progreso notable en la resiliencia cibernética, todavía existen brechas significativas. Las soluciones de protección de datos son esenciales y pensar en la copia de seguridad es un buen primer paso, pero igualmente importante es tener en cuenta la continuidad del negocio.

Rosalía Arroyo Olga Romero

TAI Editorial, a través de sus cabeceras Director TIC y Ciberseguridad TIC, ha organizado un encuentro en el que se ha debatido sobre la evolución del *backup* en un mundo híbrido y multinube, la protección de un dato cada vez más disperso y una continuidad de negocio cada vez más compleja. En este debate han participado Ignacio Pérez, CISO, AST – Gobierno de Aragón; Julián Fernández de Heredia González-Chamarro, Responsable IT y Sistemas, Cámara de Comercio, Industria y Servicios de Madrid; Alejandro Plaza Gómez, Centro de Operaciones de Ciberseguridad Madrid Digital; Miguel Ángel Blanco Arribas, Jefe de Área de Planificación y Sistemas Informáticos, Subdirección General de Sistemas y Aplicaciones para la Financiación Territorial, Ministerio de Hacienda y Función Pública; y Francisco Manuel Cortes Jurado, Jefe de Servicio de Explotación de Sistemas Informáticos, Gobierno de Castilla la Mancha. En la moderación del debate participaron Olga Romero, redactora de Director TIC, y Rosalía Arroyo, directora de Ciberseguridad TIC.

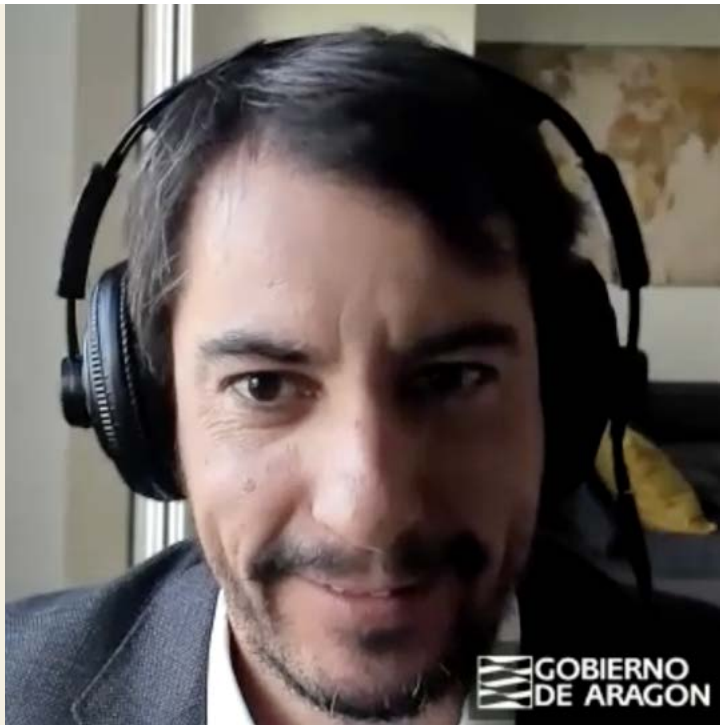
"Ya no basta con tener un *backup*. Ahora necesitamos tener diferentes escenarios de desastre y cómo vamos a actuar ante ellos"

"Si tienes tus activos en la misma nube, no", responde Ignacio Pérez cuando se plantea si la copia de seguridad debe hacerse en la nube o en local. Propone que al menos se cambie de proveedor de nube por si se produce algún "cisne negro", que en seguridad es un suceso o evento imprevisible que puede tener consecuencias significativas y de gran alcance. Explica el CISO que los datos deben cifrarse antes de subirse a la nube, "aunque el paradigma de la computación cuántica tendrá un impacto" y asegura que, en todo caso, "lo que debe hacerse es tener en cuenta el contexto en tu análisis de riesgo" a la hora de optar, o no, por la nube para hacer un *backup*.

Asegura también Ignacio Pérez durante una de sus intervenciones en el debate que "uno es responsable de los activos que tiene", y añade que hay dos activos esenciales: los servicios y la información, "que es donde hay que poner el foco" porque todo lo demás no dejan de ser activos

> “Las nuevas herramientas de *backup* y recuperación te dan unos tiempos de respuesta, de retención y de punto de recuperación objetivo que antes eran impensables”

Ignacio Pérez,
CISO, AST – **Gobierno de Aragón**



relevantes para poder sustentar los anteriores.

Menciona también que la Ley Cloud de Aragón “nos empuja a la nube directamente”, lo que requiere de unas certificaciones. No le preocupa tanto a Ignacio Pérez el tema normativo como el *“vendor locking”* por varios motivos, desde el económico, debido a una posible modificación de tarifas; como de gestión por si hay cisne negro importante y el proveedor te arrastre.

Apuesta el CISO de AST por entornos híbridos y recuerda que el mayor riesgo de un plan de continuidad de negocio no es el incendio o inundación, sino “un ataque lógico que nos inutilice el servicio”. Asegura también que ya no basta con tener un *backup*, “ahora necesitamos tener en cuenta diferentes escenarios de desastre y cómo vamos a actuar ante ellos”.

En opinión de Ignacio Pérez, la evolución y adopción de nuevas herramientas de *backup* y recuperación te dan unos tiempos de respuesta, de retención y de punto de recuperación objetivo “que antes era impensable”. Habla también de un aumento de la concienciación, “ya que antes no tantas organizaciones tenían la costumbre de tener un *backup*”.

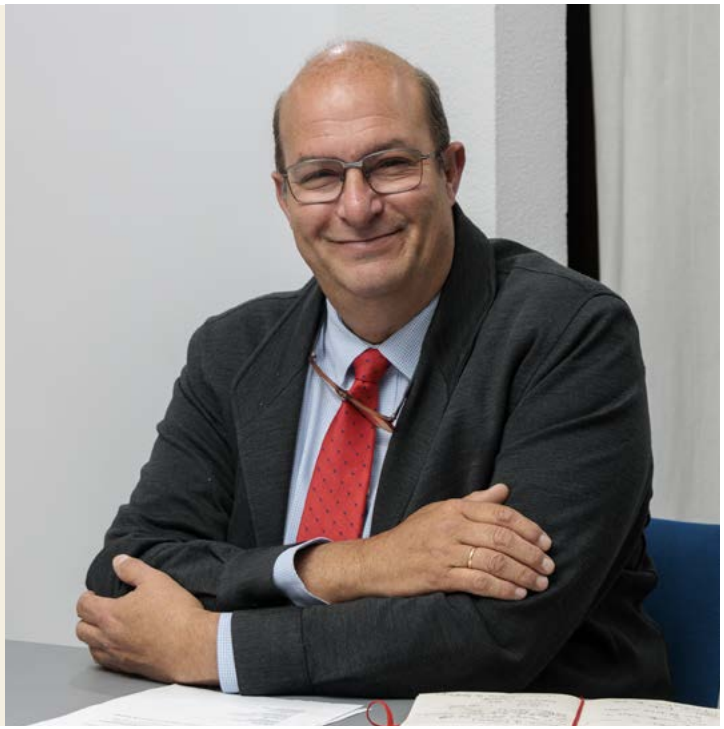
Para el CISO de Aragonesa de Servicios Telemáticos, “la ventaja que tenemos ahora es el poder hacer copias en poco tiempo y muy continuas, que antes era inviable” y que “los entornos *legacy* probablemente sean el gran hándicap”. Añade que “a pesar de que la nube tiene sus riesgos, creo que todos somos conscientes de que, por lo menos con respecto a los grandes fabricantes, las medidas que pueden poner están a años luz de lo que nosotros generalmente ponemos, y eso es algo a tener muy en cuenta”.

Frente a la pregunta de si se está desplazando todo el tema de *backup* y recuperación a los departamentos de ciberseguridad, comenta Ignacio Pérez que el responsable de ciberseguridad no tiene que hacer el *backup*, sino que “damos un marco común a todos los actores que tienen que hacer *backup*. Tenemos que hacer una función de auditor, de comprobar que todo está bien, que se han hecho las pruebas”.

A la hora de responder a la pregunta ¿existe una estimación de cuántos datos pueden per-

mitirse perder?, habla Ignacio Pérez de hacer un BIA, o análisis de impacto de negocio, por cada modelo de negocio que se tenga. Comenta que, aunque la respuesta a esa pregunta se tiene, no se da "porque produce un daño en la imagen" y asegura que ninguna organización, pública o privada, deja de tener pérdida de datos "porque los recursos son finitos".

> "Para la realización de copias de seguridad y restauración de sistemas, el modelo cloud resulta ser muy interesante"
>
> **Julián Fernández de Heredia González-Chamarro,** Responsable IT y Sistemas – **Cámara de Comercio, Industria y Servicios de Madrid**



"La información está muy distribuida y dispersa. El reto es acotarla"

Pone sobre la mesa Julián Fernández el esquema 3-2-1 que ha acompañado al *backup* desde hace años: tres copias de tus datos; dos de las copias de seguridad deben estar almacenadas en diferentes tipos de medios, y al menos una copia de seguridad debe estar almacenada fuera del sitio, para decir que, entendido como un recurso, "la nube puede ser muy interesante y además es una infraestructura deslocalizada."

Menciona el directivo durante el debate que cuando se habla de salvar datos, no solamente estamos hablando de documentos y ficheros, "sino también de imágenes de máquinas virtuales, y todo ese tipo de factores, evidentemente, añaden complejidad a la salvaguarda. Y se complica cuando lo que estamos salvando son aplicaciones", asegura.

Planteado qué retos genera el *backup* y la recuperación en entornos híbridos y *multicloud*, responde Julián Fernández de Heredia que en la Cámara de Comercio, Industria y Servicios de Madrid "nos estamos moviendo en un entorno de *cloud* privada 100 %, con ganas de empezar a hacer cosas con *cloud* híbrida". Dicho esto, añade que la industria está impulsando la adopción de la nube "y que ahora el consumo de aplicaciones es como consumir una *utility*: luz o agua: tú consumes y pagas la factura". La realidad es que la información está dispersa y que el reto es acotarla, algo que no resulta fácil. Un segundo reto es, "en caso de contingencia, cómo continúas dando servicio de sistemas de información a la entidad de la mejor manera y en el menor plazo posible."

¿Cuántos datos pueden permitirse perder? "No es un problema con una solución única", res-

ponde Julián Fernández de Heredia, añadiendo que si un dato puede ser esencial o no depende del entorno o la circunstancia. Asegura también el directivo que la máxima es no perder ningún dato, pero que es evidente que es imposible y que lo que se busca es "minimizar siempre el impacto y los daños".

"El futuro está en las soluciones híbridas"

Más allá de que el *backup* se haga en la nube o en una infraestructura local, habla Miguel Ángel Blanco durante su primera intervención del tiempo de recuperación. Teniendo esto en cuenta, "a lo mejor el *backup* en la nube puede ser muy útil" y, en todo caso, teniendo siempre en cuenta que "como mínimo hay que encriptarlo y tenerlo en un proveedor distinto al que se esté utilizando".

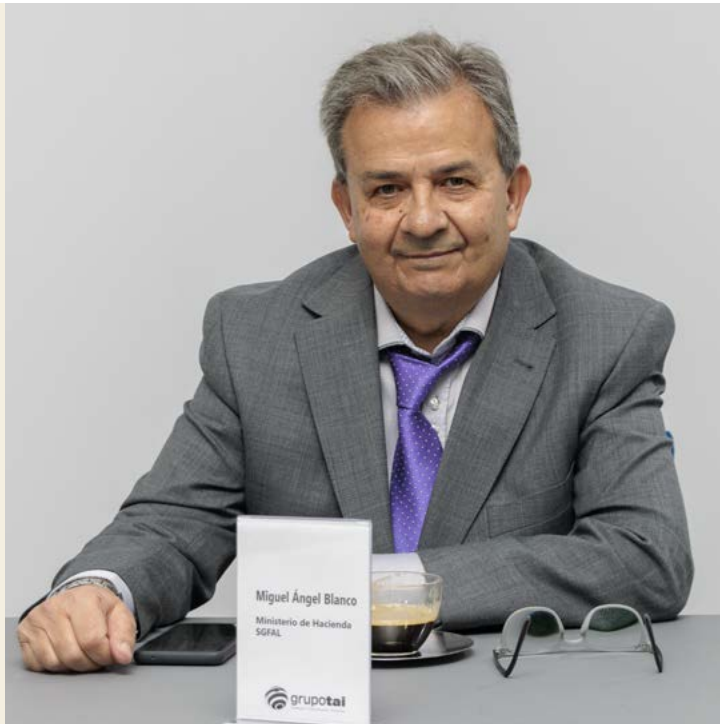
Explica Miguel Ángel Blanco que la Subdirección General de Sistemas y Aplicaciones para la Financiación Territorial está inmersa en una transformación que llevará a la entidad a, en lugar de tener una plataforma primaria y otra de respaldo, poner las dos plataformas de modo activo-activo, que "ofrece indudables ventajas, pero tiene unas restricciones de latencia" que asegura que debe ser inferior a cinco milisegundos. Añade que el futuro está en las soluciones híbridas.

Planteado cómo ha sido la evolución que ha experimentado la adopción de las herramientas de *backup*, recuperación y continuidad de negocio en las Administraciones Públicas, recuerda Miguel Ángel Blanco que al principio se trataba de "salvar ficheros y poco más"; la llegada de la virtualización requirió la necesidad de "salvar inteligentemente esas cajas oscuras (máquinas virtuales) de una manera compatible para que luego se pudiera recuperar", a lo que siguió la llegada de las *snapshots*... "pero lo que no debemos olvidarnos es tener una copia al menos en un lugar no accesible en línea, por ejemplo, una caja ignífuga". Menciona el peligro del *ransomware* y el correo electrónico como principal vector de ataque.

El *backup* en disco, considerado como una copia de seguridad intermedia, se realiza en dife-

> "El *backup* en la nube debe estar encriptado y colocado en un proveedor distinto al que se esté utilizando"

Miguel Ángel Blanco Arribas,
Jefe de Área de Planificación y Sistemas Informáticos, Subdirección General de Sistemas y Aplicaciones para la Financiación Territorial – **Ministerio de Hacienda y Función Pública**



rentes intervalos del día; además, cada día se hace un *backup* en cinta, unas cintas que cada cierto tiempo se llevan a otro desplazamiento. ¿El problema? "Que recuperar tus operaciones desde una cinta lleva su tiempo".

Respecto a cómo los aspectos relacionados con las copias de seguridad y recuperación se están desplazando a los departamentos de ciberseguridad, coincide Miguel Ángel Blanco en que "somos una especie de auditores para que las normas se cumplan" y resalta que es importante que las funciones entre los responsables de ciberseguridad y el responsable de sistemas, que son quienes tienen que operar los *backup*, estén diferenciados para detectar posibles problemas.

A la hora de hablar de pérdida de datos, menciona Miguel Ángel Blanco dos tipos de datos. Los relacionados con las operaciones estadísticas son consistentes y lo siguen siendo a pesar de que haya alguna pérdida. Que se pierda o degrade la información relativa al procedimiento de pago puede generar más problemas, pero también en función del día. "Podríamos tener apagado nuestro CPD un día entero, pero si es el día que se hacen las transferencias, entonces hay un problema", explica, añadiendo que se tienen que hacer análisis y planes de recuperación de manera continuada.

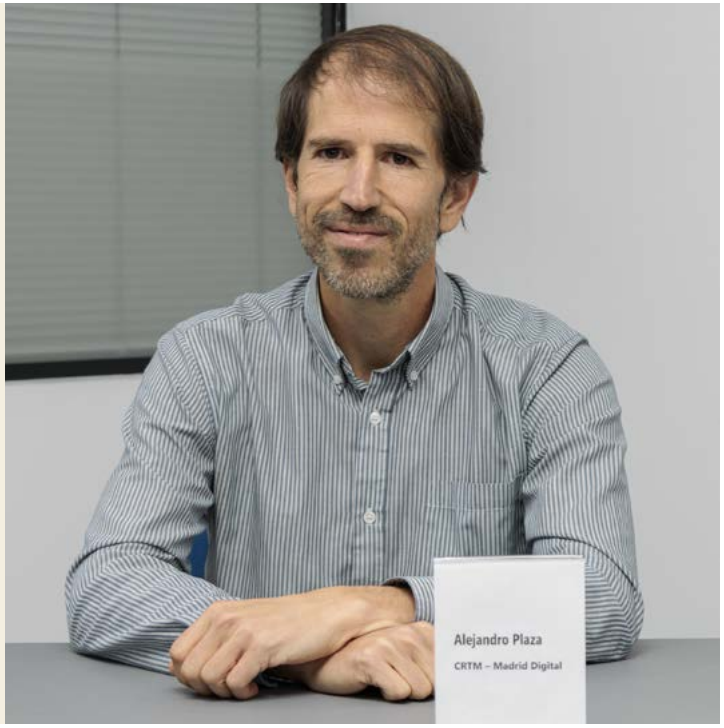
"Las cintas son la última salvaguarda"

"Dentro de poco la pregunta será irrelevante", dice Alejandro Plaza Gómez cuando planteamos *¿backup* en la nube o no?, porque "la industria te lleva todo a la nube", asegura. Explica que, aunque son muchas las administraciones que siguen teniendo infraestructura propia, muchas no y, cumpliendo todas las normativas, tendrán todo en el *cloud*.

Hablando de los retos del *backup* y recuperación en entornos híbridos y *multicloud*, menciona Alejandro Plaza Gómez lo complicado que es cambiar de proveedor o la dificultad que hay de entendimiento entre los diferentes proveedores. Aboga por soluciones que puedan ser lo más simples posible y se integren con la mayoría de sistemas.

"El plan de *backup* y recuperación debe estar alineado con la política de seguridad de la información"

Alejandro Plaza Gómez,
Centro de Operaciones de Ciberseguridad
Madrid Digital



En opinión de Alejandro Plaza, las cintas son la última salvaguarda. Y eso a pesar de reconocer que las cabinas de discos son ahora mucho más económicas, y que los discos tienen más capacidad. Añade que debe tenerse en cuenta que hay que amortizar las inversiones y que, si las cabinas de cintas siguen funcionando, ¿por qué no utilizarlas?

Tradicionalmente el *backup* ha sido asunto de los departamentos de sistemas, de la parte de TI, pero cada vez está más cerca de los departamentos de ciberseguridad. En opinión de Alejandro Plaza "no puede ser de otra manera", y explica que en Madrid Digital el plan de *backup* y recuperación sí que está alineado con la política de seguridad de la información, porque "no deja de ser el último seguro cuando todo falla".

Explicando que Madrid Digital funciona como un integrador de diferentes consejerías que consideran que lo suyo es lo más importante, "el trabajo es mucho más complejo porque efectivamente el dinero y los recursos son finitos y es difícil valorar en cuál de ellas tienen que poner más foco".

"Las tecnologías de copia inmutable son un avance importante"

Tomando como referencia la Ley de Protección de datos, así como el Esquema Nacional de Seguridad, y recordando que las administraciones han sido un poco reacias a la adopción de la nube, "esto ha dejado de ser un problema hace bastante tiempo", afirma Francisco Manuel Cortes que "no debería de suponer un problema, porque además nos hace ser más resilientes".

Francisco Manuel Cortés habla durante su intervención del *"vendor locking"* mencionado por otros compañeros de mesa para decir que es algo en lo que normalmente se piensa poco, "pero en lo que nosotros debemos estar obligados a pensar, porque los que trabajamos en protección del dato, de alguna forma vivimos en un mundo distópico en el que cualquier amenaza sobre nuestra organización ya se ha materializado".

En un escenario marcado por los fondos MRR, recuerda que estamos "en un momento dulce para la contratación en tecnologías de la infor-

> "Aunque no es fácil, debe preverse qué pasa si nuestro proveedor de sistemas de *backup* o protección de datos en la nube nos falla"

Francisco Manuel Cortes Jurado,
Jefe de Servicio de Explotación de Sistemas Informáticos – **Gobierno de Castilla la Mancha**

mación” y que, aunque no es fácil, debe preverse qué pasa si nuestro proveedor de sistemas de copias de seguridad o de protección de datos en la nube nos falla. Al respecto recomienda que debe preverse disponer de recursos, tiempo y esfuerzo para llevar a cabo un proyecto de migración de un proveedor a otro, “algo que no siempre es fácil”.

La restauración de un fichero pequeño se puede hacer fácilmente, “el problema varía si somos víctimas de un ataque exitoso que nos causa un auténtico desastre”, ahí los tiempos de recuperación se manejan en días o más, dice el Jefe de Servicio de Explotación de Sistemas Informáticos del Gobierno de Castilla la Mancha.

Está de acuerdo Francisco Manuel Cortes en que la librería de cintas cumple su función como seguro de vida y califica de “avance importante” las tecnologías de copia inmutable, que ni siquiera el administrador puede borrar. “Esos ficheros de imágenes de copia no los puede modificar nadie, ni un atacante al intentar cifrar, ni tú como administrador puedes modificarlo, ni puedes borrarlo. Esa copia permanece ahí”. Añade que es una tecnología que poco a poco se va adoptando “porque, obviamente, la restauración de disco es infinitamente más rápida que la restauración desde cinta”.

Insiste el directivo que no se va a renunciar a la librería de cintas “porque en caso de desastre, aunque tardes semanas, tienes tus datos a tu disposición y bajo tu control” y que la nube es el siguiente paso en la evolución.

Francisco Manuel Cortés asegura que una buena estrategia de *backup* y recuperación frente a desastres tiene necesariamente que formar parte de una estrategia de ciberseguridad en general, “porque hay que ser consciente de que muy probablemente suframos en algún momento un ataque que tenga éxito”.

¿Existe una estimación de cuántos datos pueden permitirse perder? Francisco Manuel Cortes responde a la pregunta recordando primero que la Administración Autonómica cubre un amplio abanico de ámbitos como, por ejemplo, sanidad o educación y afirma que “un desastre en cualquiera de estos ámbitos es suficiente para infligirte un enorme daño reputacional, aun cuando el resto no esté afectado en absoluto”.