Ecosistema de una sociedad digital frágil y dependiente

Mario Alguacil

El desarrollo del ecosistema digital ha traído avances indiscutibles en numerosos sectores. Sin embargo, con estos avances también han surgido nuevos retos y riesgos. Las interrupciones en infraestructuras críticas como la energía, las telecomunicaciones o los sistemas de datos han evidenciado lo vulnerable que es una sociedad cada vez más dependiente de la tecnología

A lo largo de la historia reciente son diversos los casos en los que determinados incidentes en algún componente del ecosistema digital han puesto en jaque la continuidad de servicios fundamentales y, por tanto, han tenido impacto en la vida normal de las personas, ya sea en movilidad, transporte, sanidad, energía, logística y otros tantos sectores clave.

Uno de los primeros síntomas de esta debilidad, se manifestó alrededor de las incidencias en el sector energético cuyo impacto ya se sufrió hace un par de décadas. Este mismo episodio de madurez y consistencia de las redes de transporte de energía hoy día causarían importantes afectaciones en los sistemas que almacenan, mueven y computan datos.

En tiempos de despliegue de las soluciones de movilidad, y más aún en el momento del despegue de los teléfonos inteligentes, nos vienen a la mente determinadas incidencias en el sistema de telecomunicaciones y en los servicios en la nube que provocan un desconcierto importante en una sociedad altamente dependiente de esta capacidad e inmediatez.

En momentos de nuestra historia, el terrorismo ha provocado afectaciones importantes en los sistemas que gobiernan las operaciones y el conocimiento de las compañías afectadas, que en determinadas ocasiones ha supuesto su desaparición total.

Los fenómenos naturales como los volcanes, los incendios, los terremotos, las tormentas, la sequía, tienen impacto en las infraestructuras digitales que operan nuestras actividades tanto laborales como de entretenimiento, ya sea directamente limitando un servicio o como efecto colateral de los cambios de comportamiento de la población que reordena las capacidades de los sistemas en función de las nuevas necesidades.

En tiempos más recientes, nos viene a la mente el resultado impactante de los ataques cibernéticos a todo tipo de grandes empresas y servicios públicos de los cuales se ha tardado un tiempo elevado en restituir la situación y, en ocasiones, ni siquiera toda la integridad anterior al incidente.

Si nos alejamos de estos grandes episodios de crisis del ecosistema global y nos centramos en las organizaciones tanto públicas como privadas, en muchas ocasiones construidas en su modo digital mediante una acumulación de capas de digitalización de procesos anteriormente manuales, posteriormente optimizados y tal vez robotizados, nos daremos cuenta de que en estos sistemas confluyen un conjunto importante de componentes software, hardware, datos, procesos, dispositivos, interfaces, etc. que todos ellos, a partir de la construcción y escalado progresivo, funcionan correctamente porque su ensamblaje persigue su funcionamiento en condiciones normales.

¿Pero qué ocurre cuando las relaciones entre cliente proveedor o administración ciudadanía colapsan a raíz de cualquiera de los incidentes mencionados anteriormente? Pues que se desencadena la crisis, el análisis de la situación, la restitución de los sistemas, la recuperación de operaciones pendientes o transacciones inacabadas... En principio nada debería pasar, pero el problema puede ser mayúsculo si el proceso de recuperación se prolonga por fugas de información o por volumen/tamaño a recuperar (con lo cual la ventana de recuperación se alarga), o porque no hay seguridad de si lo que se estaba procesando en el momento de la caída se ha consolidado en la BBDD (representa que las BBDD tienen esas capacidades ya resueltas) debido a que el sistema de recogida de datos no es consistente, etc.

La contingencia es la estrategia que nos permite diseñar sistemas operacionales fuera de lo normal que permitan continuar la actividad afectada durante un tiempo prudencial, en ocasiones con claras restricciones funcionales, pero sin la pérdida de la confianza de que todo se restituirá a la situación original. Esta estrategia será la

que permita no desatender los servicios y eludir el caos general.

Esta contingencia (que en demasiadas ocasiones no tiene en cuenta suficientemente a las personas), acompañada de la conveniente resiliencia (entendida como la capacidad de la organización para enfrentarse a la situación y superarla), serán las características más relevantes del proceso de recuperación del ecosistema afectado por las incidencias que actualmente, y a futuro, se irán presentando en la agenda de los responsables de las organizaciones.

Considerar la cultura, las capacidades, las competencias digitales de cualquier organización, forman parte de las estrategias más avanzadas en materia de transformación digital de los actuales ecosistemas que gobiernan los servicios críticos de nuestras vidas. Conocer las conductas relacionadas con la escasez de recursos, las limitaciones operacionales, la falta de movilidad, la incomunicación, la información falsa, la pérdida de privacidad, o las amenazas y consumaciones de actos de delincuencia cibernética serán aspectos clave para diseñar una buena estrategia de contingencia y resiliencia. Será necesario también ensayar las crisis operacionales con el debido interés, calcular las cargas de los sistemas en situaciones límite, pensar los procesos de extremo a extremo con contingencia en cada punto crítico y, sobre todo, interaccionar sistemáticamente con la ciudadanía, los clientes, los proveedores, los operadores, los consumidores, etc., porque es en ese punto dónde el sistema puede aprender para reaccionar convenientemente en casos de incidencia.

Finalmente, tratándose de ecosistemas complejos dónde concurren múltiples disciplinas (como ocurría en la fase de implementación de los mismos), será conveniente armar los correspondientes instrumentos organizativos de gobernanza de las situaciones de crisis que, en este mundo cada vez más ciberfísico, combinen experiencia tanto en la dimensión física como en la digital, considerando que las incidencias pueden comenzar en el mundo digital y acabar afectando al mundo físico o a la inversa.

Hasta aquí todo lo relacionado con incidencias sobrevenidas, pero no planificadas, con lo cual disponer de una modelización de escenarios posibles es clave, pero más clave es planificar todo lo relativo a la introducción de mejoras, cambios o evoluciones en los sistemas con las suficientes ventanas de recuperación en caso de desastre, fallo o funcionamiento inadecuado, que eviten resultados inesperados como en los últimos incidentes vividos. En este sentido, la utilización de la filosofía de los gemelos digitales pueda aportar otra visión a la gestión operacional y escalado de los ecosistemas digitales, aportando un conocimiento nuevo hasta ahora no disponible en tanto que algunos de los incidentes y sus consecuencias posteriores no han podido simularse previamente.■