OPINIÓN

El apocalipsis digital no llegó. Llegó la factura

Por Ernesto Ángeles · 19 de noviembre de 2026 · 5 min de lectura



Oficinas que pierden acceso a sus plataformas de trabajo; aviones que no despegan; bancos que experimentan retrasos en sus operaciones; sistemas digitales que dejan de responder y hasta sistemas de refrigeración comercial afectados por incidentes de ciberseguridad. Todo esto ha sucedido durante las últimas semanas.

Ante semejante acumulación de incidentes, no faltan las voces alarmistas que auguran el fin del dinero, de los vuelos, de la civilización y hasta de la humanidad. Sin embargo, la realidad no es tan simple, fatalista ni inexplicable. ¿Cómo se puede explicar el caos tecnológico de las últimas semanas? ¿Existe alguna relación entre los distintos acontecimientos? Y si no estamos ante un cataclismo tecnológico, ¿qué podemos esperar de esta creciente fragilidad digital?

Para comenzar, no existe una sola razón detrás de los incidentes, sino múltiples causas. En el caso de Microsoft, una combinación de defectos de software, problemas de capacidad y fallos en sus mecanismos de gestión del tráfico provocó una interrupción en cadena. Los problemas de control aéreo en Estados Unidos estuvieron relacionados con la inestabilidad de una infraestructura de telecomunicaciones heredada. El incidente de JPMorgan se debió a un error de software en sus sistemas locales, mientras que United Airlines experimentó una interrupción tecnológica que afectó las aplicaciones utilizadas por sus tripulaciones. La NSA sufrió una degradación temporal de su red interna durante tareas de mantenimiento programado, y Apple experimentó interrupciones en algunos servicios después de una actualización interna.

Como es posible observar, no existe una única razón detrás, sino una serie de incidentes que nada tienen que ver con el fin del mundo; no obstante, sí existen hilos conductores que unen al caos digital que está sucediendo en diversas partes del mundo.

El primero tiene que ver con nuestra creciente dependencia de las infraestructuras digitales y su interconexión. Buena parte de las actividades económicas, gubernamentales y sociales depende hoy de sistemas tecnológicos que operan en línea. Además, muchos de estos servicios se encuentran concentrados en un número relativamente reducido de proveedores y operadores, cuyas plataformas sostienen las actividades de millones de personas y organizaciones. Esto significa que un fallo en un punto estratégico puede propagarse rápidamente y afectar a usuarios que ni siquiera conocen la infraestructura de la que dependen.

Ahora bien, estos sistemas se encuentran en contextos que los someten a condiciones que degradan su seguridad, estabilidad u operatividad; tales variables no son sólo de naturaleza técnica, sino que son el resultado de decisiones políticas y económicas.

Una de estas condiciones tiene que ver con lo que coloquialmente se denomina código espagueti. El concepto describe programas cuya estructura interna es desordenada, difícil de interpretar y complicada de modificar.

Piensa en un sistema bancario con más de dos décadas de existencia: en su primera versión, quizá tenía diez funciones principales; su arquitectura era relativamente sencilla y los programadores originales conocían prácticamente todas sus partes. Sin embargo, después de veinte años, el banco necesita incorporar: pagos mediante dispositivos móviles; sistemas de prevención de fraude, identificación biométrica, inteligencia artificial... Y en vez de rehacer la arquitectura (por sus costos y consecuencias operativas a corto plazo), diversos equipos modifican el código existente.

El resultado puede ser un programa en el que una modificación aparentemente insignificante altera el comportamiento de componentes que, en teoría, no deberían tener relación. Y como el código se ha vuelto intrincado y sus distintas partes son altamente interdependientes, resulta cada vez más difícil prever las consecuencias de una modificación; el problema no es necesariamente que el sistema deje de funcionar, sino que mantenerlo y modificarlo se vuelve progresivamente más complicado.

Una segunda condición es la de las infraestructuras heredadas: sistemas tecnológicos antiguos que continúan utilizándose porque son indispensables para las operaciones de una organización. Y aunque la antigüedad no constituye por sí misma un factor de fallo, el problema aparece cuando las limitaciones técnicas, la falta de compatibilidad o la dificultad para conseguir componentes y personal especializado impiden mantenerlos, protegerlos e integrarlos con tecnologías contemporáneas.

El sistema de control aéreo estadounidense ilustra esta problemática; se ha documentado que 51 de los 138 sistemas de control aéreo en Estados Unidos son insostenibles y otros 54 potencialmente insostenibles[1]. Por tanto, no se trata de una deficiencia que aparezca de un día para otro, sino de un problema político-económico acumulado durante décadas.

En tercer lugar, encontramos la denominada deuda técnica, concepto introducido por Ward Cunningham en 1992. Cunningham utilizó esta metáfora para explicar cómo, cuando un equipo de desarrollo toma atajos técnicos con el propósito de entregar rápidamente un producto, puede obtener beneficios inmediatos, pero adquiere una obligación futura. Si esa deuda no se atiende, los costos de mantenimiento aumentan, las modificaciones posteriores se complican y los problemas se acumulan.

Con el tiempo, esta dinámica puede adquirir una dimensión sistémica: las decisiones técnicas tomadas por diferentes organizaciones, la interdependencia entre sus infraestructuras y la falta de mecanismos de aislamiento pueden crear riesgos adicionales, cuyas consecuencias terminan extendiéndose mucho más allá de la entidad donde se originaron.

Por tanto, el verdadero villano no usa capucha, ni trabaja para ningún gobierno enemigo: es un CEO que prefiere costo sobre seguridad, una empresa que convirtió un atajo técnico en una solución permanente, un directivo que pospuso una modernización costosa, un político que prefirió heredar un problema y un mundo que decidió que la eficiencia importaba más que la resiliencia. Eso no genera titulares tan emocionantes como un ciberataque global; pero es, con mucho, la explicación más probable —y la más incómoda— de por qué todo pareció romperse al mismo tiempo.

La verdadera vulnerabilidad no está en que mañana desaparezca el dinero, dejen de volar los aviones o se apague internet; está en haber construido una civilización que depende de infraestructuras cuya complejidad, concentración, mantenimiento y politización no corresponden con la importancia que tienen para nuestra vida cotidiana.

[1] https://www.gao.gov/products/gao-26-107992

Publicado en Punto de Referencia. Dirección original: https://puntodereferencia.mx/opinion/el-apocalipsis-digital-no-llego-llego-la-factura
Descargado el 21 de noviembre de 2026.