SERVICIOS DIGITALES BAJO EVALUACIÓN

Falla del Reniec abre debate sobre quién responde

Especialista explica qué exige la ley ante interrupciones y daños.

Cristina Luna del Pozo
cristina.luna@expreso.com.pe

La interrupción de los servicios del Reniec plantea una pregunta que va más allá de la recuperación de sus sistemas: ¿quién responde si la paralización ocasiona pérdidas económicas a ciudadanos o empresas? La responsabilidad no es automática, pero la legislación permite evaluar reparación cuando se acreditan daños vinculados con el servicio público.

Daniela Chávez, asociada del área de Protección de Datos y Seguridad de la Información del Estudio Olaechea, explicó que el perjuicio debe ser efectivo, cuantificable e individualizado, y tener una relación directa e inmediata con el servicio. La normativa contempla excepciones, como el caso fortuito y la fuerza mayor. Sin embargo, sostuvo que un incendio no exonera por si solo al Reniec.

La entidad atribuye la interrupción a una sobrecarga eléctrica y un incendio en sus servidores. Según la abogada, las instituciones públicas tienen obligaciones de prevención y recuperación. La Ley 29664 y su reglamento exigen planes de continuidad operativa, mientras que las normas de gobierno digital y confianza digital establecen deberes de seguridad y gestión de incidentes.



Interrupción a servicios de Reniec afectó a los sistemas interoperados de otras instituciones.

Cabe precisar que, el problema también alcanza a otras entidades públicas y privadas que dependen de todo los servicios interoperados.

Tras ser consultada, la especialista señala afectaciones a los bancos y también trámites migratorios. Chavez explicó que la interoperabilidad facilita el intercambio, pero también crea dependencias.

Por ello, cada entidad debe identificar sus funciones críticas y prepararse para la indisponibilidad de servicios de terceros. Las responsabilidades dependerán de las reglas de cada servicio.

La especialista advirtió que no existe una ausencia total de normas. Se debe determinar si se aplicaron y supervisaron y si previeron efectos en cadena.

También podrían investigarse responsabilidades de funcionarios si se detectan incumplimientos. No obstante, la sola interrupción no demuestra una infracción ni da lugar automáticamente a una indemnización. Para establecer responsabilidades se requiere conocer los resultados de la investigación técnica y la evaluación de las autoridades competentes.

PROTECCIÓN DE DATOS PERSONALES

Copias de datos bajo examen

Daniela Chávez indicó que la normativa exige copias de respaldo seguras y verificar su integridad. Deben hacerse, como mínimo, cada semana, salvo que no se actualicen los datos personales. La autoridad también tendría que revisar las medidas frente a fallas eléctricas, el documento de seguridad y la recuperación de información. La caída del servicio no demuestra por sí sola una filtración de datos.

48

HORAS es el plazo máximo para notificar a la autoridad y a los titulares cuando un incidente de datos personales cumple los supuestos previstos, según indicó Daniela Chávez.